UNIVERSITY OF PIRAEUS

DEPARTMENT OF INFORMATICS

PhD DISSERTATION

Clinical Decision Support Systems – Diagnostic and Prognostic Attribute-based Access Control In Acute Care

Συστήματα Υποστήριξης Κλινικών Αποφάσεων – Διαγνωστικός και Προγνωστικός Μηχανισμός Ελέγχου Έκτακτης Πρόσβασης Προσωπικών Κλινικών Δεδομένων

Evgenia Psarra

Supervisor Professor

Dimitrios Apostolou

Piraeus, July 2023

UNIVERSITY OF PIRAEUS

DEPARTMENT OF INFORMATICS

PhD DISSERTATION

Evgenia Psarra

Advisory Committee: *Dimitrios Apostolou, Professor (supervisor)*

Panagiotis Kotzanikolaou, Associate Professor

Maria Virvou, Professor

Approved by seven-member examination committee on 3 July 2023

Dimitrios Apostolou *Professor* *University of Piraeus*	Panagiotis Kotzanikolaou *Associate Professor* *University of Piraeus*	Maria Virvou *Professor* *University of Piraeus*
Konstantinos Metaxiotis *Professor* *University of Piraeus*	*Dionisios Sotiropoulos* *Assistant Professor* *University of Piraeus*	Aggelos Pikrakis *Assistant Professor* *University of Piraeus*
	Ioannis Verginadis *Assistant Professor* *Athens University of Economics and Business*	

Piraeus, July 2023

Evgenia Psarra

Doctor of Department of Informatics, University of Piraeus

The views and conclusions contained in this document express the author and should not be interpreted as representing the official positions of the University of Piraeus.

Περίληψη

Το Σύστημα Υποστήριξης Κλινικών Αποφάσεων (CDSS) είναι μια τεχνολογία πληροφοριών στον τομέα της υγείας, η οποία παρέχει στο ιατρικό προσωπικό, πληροφορίες για τα δεδομένα των ασθενών, για τη βελτίωση της υγειονομικής περίθαλψης. Τα CDSSs αποτελούν ένα σημαντικό τομέα της τεχνητής νοημοσύνης στην ιατρική. Επιπλέον, η ανάγκη αξιόπιστων μέσων για τον έλεγχο της πρόσβασης σε ιατρικά δεδομένα αυξάνεται συνεχώς, καθώς ένας αυξανόμενος αριθμός υπηρεσιών υγειονομικής περίθαλψης παρέχονται ηλεκτρονικά. Σε κρίσιμες καταστάσεις όπου η ζωή του ασθενούς βρίσκεται σε κίνδυνο, πολλοί παράγοντες οι οποίες συμμετέχουν στις υπηρεσίες έκτακτης ανάγκης, θα πρέπει να έχουν δικαίωμα πρόσβασης στα Ηλεκτρονικά Μητρώα Υγείας (EHRs) των ασθενών.

i) Να ενισχύσει το μηχανισμό ABAC με προηγμένους και εξατομικευμένους χειριστές περιεχομένου. Ως εκ τούτου, αυτή η διδακτορική διατριβή επεκτείνει την προαναφερθείσα έρευνα σε σχέση με την ενσωμάτωση ασαφών κανόνων σχετικά με τις μετρήσεις υγείας των ασθενών σε έναν μηχανισμό ABAC ο οποίος παρέχει πρόσβαση σε EHRs εισάγοντας εξατομικευμένους χειριστές περιεχομένου για την καλύτερη αντιμετώπιση καταστάσεων έκτακτης ανάγκης. Πιο συγκεκριμένα, αυτή η έρευνα στοχεύει πρώτον στην εύρεση πιθανών συνδυαστικών μετρήσεων υγείας οι οποίες μπορούν να χαρακτηρίσουν κρίσιμες καταστάσεις. Επιπλέον, στόχος αυτής της έρευνας είναι η αξιολόγηση αυτής της προσέγγισης χρησιμοποιώντας μια διαδικτυακή εφαρμογή ώστε να συγκριθεί με υπάρχοντες απλούστερους μηχανισμούς που μελετήθηκαν σε αυτή τη διατριβή.

ii) Να αναπτύξει και να εφαρμόσει τεχνικές μηχανικής μάθησης, βάσει των ιατρικών μετρήσεων των ασθενών και να τις ενσωματώσει στο μηχανισμό ABAC. Αυτός ο μηχανισμός μπορεί να παραχωρήσει πρόσβαση σε ένα σύστημα ευαίσθητων EHRs εφαρμόζοντας εξατομικευμένους χειριστές περιεχομένου βασισμένοι στη μηχανική μάθηση, οι οποίοι μπορούν να αξιοποιήσουν ακατέργαστη σημασιολογική πληροφορία, π.χ. δεδομένα από συσκευές IoT, έτσι ώστε να εντοπιστούν κρίσιμες ιατρικές καταστάσεις και να παραχωρηθεί πρόσβαση σε ευαίσθητα ιατρικά δεδομένα. Πιο συγκεκριμένα, αυτή η προσέγγιση χρησιμοποιεί το ιστορικό υγείας του ασθενούς προκειμένου να προβλέψει τις

ιατρικές μετρήσεις των επόμενων δύο ωρών εφαρμόζοντας Νευρωνικά Δίκτυα Μακροπρόθεσμης Μνήμης (LSTM). Οι τιμές των προβλεπόμενων μετρήσεων υγείας πρέπει να αξιολογηθούν από τους εξατομικευμένους ασαφείς χειριστές περιεχομένου της διατριβής, έτσι ώστε να εκτιμηθεί η κρίσιμη κατάσταση της υγείας του ασθενούς. Επιπρόσθετα, στόχος είναι να αναπτυχθεί μία επαρκής διαδικτυακή εφαρμογή ώστε να αξιολογηθεί αυτή η προσέγγιση και να συγκριθεί με διαφορετικές προηγούμενες προσεγγίσεις της παρούσας διδακτορικής διατριβής.

iii) Τέλος, για να ενεργοποιηθεί ο μηχανισμός προληπτικής δράσης, εφαρμόζονται LSTM νευρωνικά δίκτυα τα οποία χρησιμοποιούν το πρόσφατο ιστορικό υγείας του ασθενούς για να προβλέψουν τις τιμές ιατρικών μετρήσεων εντός των επόμενων δύο ωρών. Η ασαφής λογική χρησιμοποιείται για την αξιολόγηση της κρισιμότητας της κατάστασης της υγείας του ασθενούς. Αυτές οι τεχνικές ενσωματώνονται σε ένα ιδιωτικό και αδειοδοτημένο δίκτυο αλυσίδας συστοιχιών (blockchain) αξιοποιώντας την πλατφόρμα Hyperledger-Fabric, ικανό να διασφαλίζει τις ευαίσθητες πληροφορίες του ασθενούς. Συνολικά, η ενσωμάτωση αυτού του προγνωστικού μηχανισμού στο δίκτυο αλυσίδας συστοιχιών blockchain αποδείχθηκε ένα ισχυρό εργαλείο για τη βελτίωση της απόδοσης του μηχανισμού ελέγχου πρόσβασης. Επιπλέον, το εν λόγω δίκτυο αλυσίδας συστοιχιών blockchain μπορεί να καταγράψει το ιστορικό του ποιος και πότε είχε πρόσβαση στα ευαίσθητα EHRs ενός συγκεκριμένου ασθενούς, διασφαλίζοντας την ακεραιότητα και την ασφάλεια των ιατρικών δεδομένων. Ο προτεινόμενος μηχανισμός ενημερώνει προληπτικά την ομάδα έκτακτης ανάγκης σχετικά κρίσιμες ιατρικές καταστάσεις των ασθενών συνδυάζοντας ασαφείς και προγνωστικές τεχνικές και εκμεταλλεύεται τα κατανεμημένα δεδομένα του δικτύου αλυσίδας συστοιχιών blockchain, διασφαλίζοντας την ακεραιότητα και την ασφάλεια των δεδομένων και ενισχύοντας την εμπιστοσύνη των χρηστών στον εν λόγω μηχανισμό.

vi) Τελευταίο αλλά εξίσου σημαντικό, αυτή η διατριβή αξιοποιεί χειριστές περιεχομένου που βασίζονται σε νευρωνικά δίκτυα για την επίτευξη διαγνωστικού ελέγχου σε ευαίσθητες ιατρικές πληροφορίες και για την εκτίμηση ασθενειών των ασθενών, όπως υπέρταση ή εγκεφαλοαγγειακές παθήσεις, με βάση τις ιατρικές μετρήσεις τους.

Abstract

A Clinical Decision Support System (CDSS) is a health information technology, which provides clinicians and staff, with patients person-specific information, intelligently filtered or presented at appropriate times, to enhance healthcare. CDSSs constitute a major topic in artificial intelligence in medicine. In addition, the demand of robust means to control access to healthcare data is constantly growing as an increasing number of healthcare services are provided electronically. In critical situations where the patient's life is in danger, several subjects participating in emergency services should be entitled to retrieve critical data concerning the patients' Electronic Health Records (EHRs).

The focus of the current research is:

i) To enhance the ABAC paradigm with advanced and personalized context handlers. Therefore, this Ph.D. dissertation extends the aforementioned work with respect to the integration of fuzzy rules concerning patients' health metrics to an ABAC mechanism that grants access to EHRs by introducing personalized context handlers that can better cope with emergency situations. More precisely, this work aims firstly at finding possible conjunctive combinations of health metrics that result in the consideration of critical conditions (e.g., hypertension) during the access control process, and secondly, at forming complex fuzzy rules that can realistically assess critical situations. Additionally, our objective is to evaluate this approach by using a web application and compare it with the existing simpler implementations studied in this dissertation.

ii) To develop and apply machine learning techniques, based on patients' health metrics and integrate them with an ABAC paradigm. This mechanism can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers in which raw contextual information e.g., data from IoT devices, can be used in order to identify acute care conditions and grant access to sensitive medical information. More specifically, this approach uses the patient's health history in order to predict the health metrics of the next couple of hours by implementing Long Short Term Memory (LSTM) Neural Networks (NNs). The prognosed health metrics' values are to be evaluated by the dissertation's personalized fuzzy context handlers, so as to estimate the criticality of the health condition of patient. Additionally, our objective is to develop a sufficient web application so as to evaluate this approach and compare with different ones of this current dissertation.

iii) Finally, to enable proactivity, we apply LSTM NNs that utilize patient’s recent health history to prognose the next two-hour health metrics values. Fuzzy logic is used to evaluate the severity of the patient’s health state. These techniques are incorporated in a private and permissioned Hyperledger-Fabric blockchain network, capable of securing patient’s sensitive information in the blockchain network. Overall, integrating this predictive mechanism within the blockchain network proved to be a robust tool to enhance the performance of the access control mechanism. Furthermore, our blockchain network can record the history of who and when had access to a specific patient’s sensitive EHRs, guaranteeing the integrity and security of the data. Our proposed mechanism informs proactively the emergency team about patients’ critical situations by combining fuzzy and predictive techniques, and it exploits the distributed data of the blockchain network, guaranteeing the integrity and security of the data, and enhancing the users’ trust to the mechanism.

iv) Last but not least, this dissertation leverages neural network-based context handlers for achieving diagnostic control in sensitive health information, and for estimating patients’ diseases, such hypertension or cerebrovascular diseases, based on their health metrics.

Keywords: Attribute-based access control, Healthcare data security, Cloud, Context-aware security policies, Context-aware services, Decision making, Electronic health records, Emergency services, Fuzzy logic, Health information management, Medical diagnosis, Medical information systems, Acute care, Data privacy, Cloud storage, Context handling, Complex fuzzy rules, Personalized access control, Descriptive analytics, Descriptive synthesis, Body mass index, Blood pressure, Smoking, Hypertension, Sequential health data, Health records, Long short term memory, Machine learning, Neural networks, Medical diagnosis, Medical prognosis, Private and permissioned blockchain, Hyperledger fabric blockchain technology, Smart contacts, Personalized policies, Proactive access control, Artificial neural networks.

Table of Contents

List of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 12

List of Tables

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 12

List of Acronyms

Acronym	Full Term
ABE	Attribute-based Encryption
ABAC	Attribute-based Access Control
LSTM	Long Short Term Memory
ASCLEPIOS	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare
AMPLE	ASCLEPIOS Model PoLicies Editor
EHRs	Electronic Health Records
EMRs	Electronic Medical Records
LSTM	Long Short Term Memory
NNs	Neural Networks
RBAC	Role-Based Access Control
DAC	Discretionary Access Control
DBP	Diastolic Blood Pressure
SBP	Systolic Blood Pressure
HR	Heart Rate
BMI	Body Mass Index
IPFS	InterPlanetary File System
API	Application Programming Interface
PSO	Particle Swarm Optimization
GA	Genetic Algorithms

Acknowledgments

First of all, I would like first of all to express my warmest thanks to the supervisor of the Doctoral Dissertation, Professor of University of Piraeus Dimitrios Apostolou for the trust he showed me in the first place, giving me the opportunity to cooperate with him and work under his instractions, but also the continuous and systematic scientific guidance throughout my research. His contribution was determinative and without his help this dissertation would have never been completed. His knowledge and experience were provided to me without hesitation, while the very frequent discussions with him, resulted in the generation of new ideas about the subject of my doctoral dissertation. Additionally, as he is the head of the laboratory of Decision Support Systems, gave me the opportunity to be in a fully organized scientific environment, the surrounding knowledge of which, played a very important role in the development of my scientific research.

I must also warmly thank i) Professor of National Technical University of Athens Gregoris Mentzas, ii) Assistant Professor of Athens University of Economics and Business Yiannis Verginadis, and iii) Dr. Ioannis Patiniotakis for the ongoing valuable tips, instructions and key discussions throughout my research endeavor. Their help and contribution has been invaluable and their suggestions on individual issues were essential.

I must also warmly thank i) Professor University of Piraeus M. Virvou, ii) Associate Professor of University of Piraeus P. Kotzanikolaou, iii) Professor of University of Piraeus K. Metaxiotis, iv) Assistant Professor of University of Piraeus D. Sotiropoulos, and v) Assistant Professor University of Piraeus A. Pikrakis for their supervision.

I also thank my family for the support they showed me during my research.

Chapter 1

1. Introduction

A. Research Area of Dissertation

The need of a trusted environment in which only authorized users are permitted to access a system was of imperative importance since the early days of cloud computing. Even nowadays, a lot of users seem to be reluctant to store their personal data in the cloud and specifically the data related to bank accounts and the health care domain. Our goal is to enhance the access control mechanisms that can be used in the healthcare domain for enhancing the security and privacy of EHR systems.

A promising approach for alleviating the security risks associated with cloud computing is to define effective context-aware security controls for the sensitive data of cloud applications. This dissertation hinges upon an access control scheme that takes into account the inherently dynamic nature of cloud environments and that will capture the knowledge that lurks behind such a scheme (e.g., actions, subjects, locations, environmental attributes, etc.) This access control scheme calls for the incorporation of the notion of context in access control policies, i.e., the consideration of dynamically-changing contextual attributes that may characterize data accesses. Context can be perceived as any information that can be used to characterize the situation of an entity (person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves [1]. In fact, the use of contextual information makes it possible to apply access control policies by mainly considering the circumstances under which access requests to sensitive data, should be granted. This characteristic, which involves the development of a re-usable and generic context-aware security model, is further elaborated in terms of this work.

Access control protocols are responsible for deciding if a user has the right to execute a certain operation on a specific object. Objects can be a server, a service, an application, an entire relational database, a single row in table or even an entire wide column in a NoSQL datastore. Common operations are read, write, delete, update etc. The user is considered as the active element and is called subject. A permission associates an object with an operation. Static access control models, usually, provide a list of permissions that each subject has on certain objects. Commonly used access control models are the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) and the Role-Based Access Control (RBAC) [2]. All these models are known as identity-based access control models where user (subjects) and resources (objects) are identified by unique names [3]. In the literature, a fourth type has been identified, the Attribute Based Access Control (ABAC) [4] which is by nature dynamic. In ABAC, there are no static lists of permissions that associate subjects with objects, but instead there are "snapshots" of such associations that can be generated and dynamically change, based on the current context.

A recent model for encrypted access control is Attribute-Based Encryption (ABE) [5], in which ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography, but both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes instead.

All the above mentioned privacy preserving mechanisms could be incorporated for access control in clinical decision support system. Clinical decision support comprises a set of tools and interventions, computerized as well as non-computerized. Non-computerized tools comprise medical guidelines or digital medical decision support resources such as UpToDate® or ClinicalKey®[6, 7]. This kind of clinical decision support systems (CDSS) are identified as information management tools. Another type of CDSS, which are tools to aid focus attention, are called simple or basic clinical decision support systems. Examples of these CDSS comprise laboratory information systems (LISs) underlining acute care or pharmacy information systems (PISs) introducing a new drug alert ordering and suggesting a feasible drug-drug interaction [8, 9]. An additional category is the advanced CDSS which provide patient-specific recommendations such as verifying interactions of drug disease.

The quality and quantity of medical information is growing, comprising Electronic Health Records (EHRs), registry of disease, information exchanges and patient surveys. Nonetheless, digitalization and big data do not guarantee undoubtedly advanced patient treatment. Studies have suggested that establishing an EHR and computerized physician order entry (CPOE) has decreased the number of errors, and introducing others [10 - 12]. Thus, high-quality medical decision support is important if medical institutions want to attain the most possible privileges of EHRs and CPOE. In the ongoing medical environment when making a decision, medical professionals regularly aren't aware of certain patient information that is at their disposal in the EHR, and is difficult for them to access this information, due to the lack of time to search for this particular information or are not knowledgeable on the most recent healthcare-related insights. In addition, the medical providers regularly face the problem of information overload [13 - 15]. Additionally, decisions by medical professionals are regularly made throughout direct patient contact. The majority of decisions are made within seconds and are dependent on the medical professional who has at her disposal at the time of the decision all the available parameters of patients and knowledge of medicine. Therefore, ongoing decisions are driven by doctor's knowledge and experience. In addition alterations in the patient's health state arising before ward admission or hospital are frequently not taken under consideration due to the fact that medical professionals commonly examine the patient in her present health condition without considering her previous health state. On the contrary, an information system considers all the available information in order to observe changes in the patient's health state beyond the doctor's scope.

Categorization of CDSS is generally related to the characteristics of: human computer interaction, decision making process, style of communication, model for giving advice and system function [16]. The characteristic "System function" characterizes two types of functions. i) Systems deciding: "what is true" which include diagnostic CDSS such as differential diagnosis websites of Diagnosaurus® or WebMD® [17, 18]. These CDSS depend their recommendations on a fixed dataset that is readily available or user inputted. ii) The other type of CDSS decide "what to do", recommending which drug to prescribe regarding the present health status of the patient or enhanced differential diagnosis. Nonetheless, the differentiation above is of limited value as most recent CDSS comprise both functions: firstly they decide what is true regarding the patient and then they recommend what to do with that patient.

An additional parameter of CDSS is the way of giving suggestions, either active or passive. On the one hand, the challenge of active ones is the prevention of a large number of alerts which cause user's alert fatigue. On the other hand passive ones need the user's action so that he receives recommendation, such as opening a tab or selecting a button. However, the passive ones have been abandoned due to their dependence in human factor and lack of efficiency [19, 20].

An additional characteristic of the CDSS is the style of communication, which distinguishes a critiquing and consulting model. On the one hand, a critiquing system allows the user to determine the right dose and only then alerts the user that the prescribed dose for this therapy is too low. On the other hand, regarding a consulting model the system is an advisor by proposing subsequent actions and asking questions. More specifically, when inserting a medication order, the information system requests the diagnosis and recommends an alternative treatment or the right dose of medication.

Another clinical decision support system characteristic is the human computer interaction. Traditionally CDSS were difficult to use and access and slow. Nevertheless, the recent CDSS by exploiting the modern computing power, they overcome the old problems of computer mobility and electronic health record integration. The human computer interaction is useful for categorizing CDSS defining EHR overlay or integration, voice or keyboard recognition and recommendations via messaging systems, acoustic alarms or pop-ups.

The last characteristic of CDSS is the fundamental decision-making process or model. The most basic models are problem-based flowcharts encoded for information system's usage. More complex models have been researched and used since, such as Bayesian models [21, 22], Artificial Neural Networks (ANNs) [23], Support Vector Machines (SVMs) [24] and Artificial Intelligence (AI) [25] with the accessibility of growing computing power, mathematical techniques and additional statistical models. Most of those systems are utilized to aid selecting the best course of action, prioritize treatment, and ameliorate the prediction of outcome. However, the usage of these systems in practice is delayed primarily due to trust issues towards "black box" systems. More particularly, if an information system suggest the healthcare professional to start drug A for a patient depending only on a mathematical model, without a guideline to support it, the healthcare professional wouldn’t be persuaded. Connected to the severe trust issue towards “black box” systems is the concurrent guidelines based on these studies and current model of evidence based medicine. Would healthcare professional be willing to overlook an international guideline which demonstrates to the patient to start on drug A only because the CDSS suggests on drug B instead? For this reason, decision tree models are the oldest but to this day the most used models for medical purposes. These CDSS use a tree model of decisions including multiple steps based on “if then else” logic. The decision tree models follow logical steps dependent on conventional clinical guidelines and have the privilege of being interpretable by humans. These decision tree models are alternatively named decision support algorithms, computer-interpretable guidelines (CIGs) or clinical rules (CRs) [10]. Rather than predicting the outcome a CDSS only automates information collection and gives recommendations based to a guideline.

The protection of privacy of a patient’s Electronic Medical Record (EMR) is imperative, even in emergencies. In critical access control systems, static control rules are typically applied, which usually involve the role (e.g., doctor) or even an explicit enumeration of individuals that should be allowed to access a patient’s EMR. As a result, in emergencies, we witness the so-called ‘break-glass’ procedure, during which medical personnel may bypass rigid access control rules and acquire access to a patient’s medical history. However, we advocate that access control under emergency conditions should be supported with the required dynamism instead of adopting a break-glass procedure. Furthermore, in many cases, parts of the patient’s EMRs remain unreachable even in emergencies because they are located in information systems outside the treating hospital’s boundaries. Therefore, the availability of EMRs across organizational boundaries has been proposed to enhance the quality of information available for decision-making during acute care [26].

Cloud storage services match the needs of remote and ubiquitous access to medical data for multiple healthcare organizations. However, security and privacy challenges still hamper the wide adoption of cloud services. Moreover, patients and healthcare organizations are afraid of losing control over the EMR when storing it on untrusted third-party clouds [27]. In May 2018, the General Data Protection Regulations (GDPR) (European Union) came to reinforce the need for personal data protection, defining conditions for data sharing and processing across multiple domains. Under the GDPR, the healthcare organizations, the 'data controllers', have accountability for fulfilling these regulatory requirements. The accountability relies on their ability to demonstrate that appropriate procedural security measures are being applied and, most importantly, compliant with the GDPR. When a single cloud-based EMR system is used, the GDPR classifies healthcare organizations as joint data controllers. These jointly determine 'why' and 'how' personal data should be processed for complying with the GDPR rules designed specifically for healthcare data processing (European Commission). Therefore, a cloud-based EMR system's access control mechanisms should be designed to support multi-organization collaboration and offer accountability and auditability at individual, team and organization levels.

The main goal of an EMR system is patient data availability; therefore, the access control must not block any rightful request for the sake of the patients' vital interest. Because of that, the access control models usually are more permissive than needed for patient treatment. This may pose threats to patient privacy [28] because the users might abuse the permissions and use the data for other purposes than treating a particular patient, for example, for curiosity sake. Researchers have proposed using the Attribute-Based Access Control (ABAC) model to achieve a more fine-grained access control; however, its adoption in real healthcare applications remains challenging. One reason is that the information workflow during acute care involves cross-organisation data sharing, which is complex and difficult to understand and model adequately. Consequently, the existing access control models using ABAC usually cover well only the conventional access situations (e.g. doctor appointments), leaving the acute care case less protected.

New cryptographic schemes were recently introduced to preserve sensitive data confidentiality and enforce fine-grained access control. The most noteworthy involved different variants of Attribute-Based Encryption schemes (ABE) [29] that allow users to decrypt files and therefore access them if and only if the attributes (of their key) satisfy the underlying policy. This refers to the realisation of an implicit authorisation, i.e., authorisation is included in the encrypted data, and only people who satisfy the associated policy can decrypt data. ABE schemes are classified into two main categories [29]: (1) Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and (2) Key-Policy Attribute-Based Encryption (KP-ABE). In CP-ABE [30], for every user, a private key is generated involving a set of attributes that may characterise the user (e.g., role in the hospital, specialisation etc.), which can be assigned and verified by one or more trusted authorities.

In addition, the cyphertext of the data to be protected specifies an access policy over a defined universe of attributes within the system. The anti-diametric stands for KP-ABE, where the attributes accompany the encrypted data and the private keys' policies. The decryption works if at least a threshold number of attributes match the policy. Other variants of ABE do exist, like multi-authority ABE (MA-ABE) [31] and dual-policy ABE (DP-ABE) [32] but their majority present some limitations, especially when it comes to production systems for protecting EMRs during acute care. Their first limitation resides in the complexity of the key revocation process. The revocation process in ABE schemes can be challenging since each attribute possibly belongs to multiple different users, whereas in traditional public key infrastructures (PKI) systems, the public/private key pairs are uniquely associated with a single user. Several approaches tried to overcome this problem [33] mainly through techniques such as ciphertext delegation [33]. However, this kind of access control flexibility, enabled by ABE, came at the cost of enforcing access control schemes that require significant computational resources [34] as the generated ABE ciphertexts become rather large. Secondly, ABE schemes are efficient for access control enforcement when the policies are defined to involve a limited number of attributes using only conjunction or disjunction operators. This means that the complexity of ABE policies cannot reach the one that can be supported in ABAC schemes while their efficiency, as we have presented in [35], [36], [37], is strongly affected by the number of attributes involved and the size of data to be protected (i.e., encryption/decryption times and computational load).

As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient’s health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. A major challenge in this area is to enable trustworthiness and to achieve traceability of access control to personal health data in emergency situations.

Blockchain based technologies implemented in the medical sector hold various benefits, but also many challenges as well regarding the acceptance by the medical community. Even if the technology of blockchain has benefits such as system performance, collaborative ecosystem, or innovative technological features, its applications in healthcare are in their early stage [38]. The perceptions of the individual issues such as the lack of knowledge, the organizational issues such as the implementation, the technological issues such as the blockchain model types, and market-related issues such as regulatory concerns indicate that blockchain-based applications in healthcare constitute an emerging field. This study points out the practical implications and thus is capable to assist developers and medical managers in identifying possible issues in implementing, developing, and planning blockchain-based health information exchange systems. According to the author, tackling these barriers can assist the widespread usage of blockchain-based health information exchanges in various medical settings and facilitate connectivity and interoperability in community and regional health information networks. Additionally, barriers of acceptance include among others, usability constraints, lack of management commitment, lack of a security-oriented culture, lack of awareness regarding legislations and health information technology risks [39]. Nevertheless, blockchain is being explored by stakeholders to enable better use of healthcare-related data, enhance compliance, improve patient outcomes, lower costs, and optimize business processes [40]. Nonetheless, in assessing if blockchain can fulfill the hype of a technology described as disruptive and revolutionary, it is important to ensure that blockchain design elements take under consideration the actual medical needs of regulators, providers, patients, and consumers. It is worth mentioning that the authors point out that the most praiseworthy advantages of blockchain are yet to be realized. However, the efforts of blockchain pilots will finally lead to the promise of patient-driven medical systems in the form of open health data markets and precision medicine, finally reaching the patient.

B. Contribution

The contribution of the current dissertation is summarized to the following scientific areas:

1) **It proposes a Multi-continent Descriptive Analysis for correlation of health metrics and diseases.** In health-based descriptive analysis, the patient's health-related contextual information should be taken into account along with the age, the gender and the nationality in order to detect their correlation with health problems such as obesity, hypertension or smoking habits. Such a descriptive analysis is necessary so that healthcare professionals have at their disposal such a statistical analysis so as to have an overall clinical profile concerning the patient's condition. In this work, by using descriptive analytics we introduced a multi-continent overview based on patient's health indices and their correlation to contextual information such as gender and age, that serve as a basis for identifying health problems such as obesity, hypertension and smoking habits. In addition, by our analysis, a descriptive synthesis is produced, based on our literature review, which conducts a continent-based investigation according to the patient's heath related information. Finally, in order to validate and compare the results which were extracted by this systematic literature review, we developed and implemented a web application capable of processing and analyzing real datasets in order to present each patient's current health information along with the mean value of the health metrics of SBP, DBP, BMI and the corresponding percentages of smoking and hypertension per continent so as to facilitate the doctor.

2) **It proposes Personalized Context Handlers.** i) *It proposes Non-complex Personalized Fuzzy Context Handlers for Diagnostic Access Control***.** In an emergency situation, the criticality of a patient's medical condition should be taken into account when granting access to her EHRs. Such emergency access controls are necessary so

that healthcare professionals make informed decisions in life threatening situations. In this work, we introduced contextual attributes that serve in the criticality assessment of situations where access to patients' data is requested. We extended ABAC with healthcare-related context handlers, capable of inferring access policies by dynamically evaluating contextual attributes when granting access to healthcare data. We also created personalized context handlers so as to take into account the specificities of each patient when inferring access policies. ABAC with personalized context handlers is more capable than baseline ABAC and ABAC with non-personalized context handlers in detecting critical situations, especially in the oldest age group that is the most important. ii) *It proposes Complex Fuzzy Personalized Context Handlers for Diagnostic Access Control.* Implementing personalized complex context handlers in critical situations, for emergency access control, results in more adequate access control, which is dependent on objective patients' metrics and on subjective expert knowledge as well. By exploiting a fuzzy logic approach, in which conjunctive complex fuzzy rules associate the fuzzy variables per health metric with the criticality, we achieve to evaluate the patient's health risk level. Additional personal information is considered, e.g., the patient's age, and finally access control is deduced based on a new and complex fuzzy rule-based inference process, which calculates the patients' criticality risk. In an acute care situation, the criticality of a patient's health status should be considered when yielding access to healthcare professionals regarding her medical data so as to decide about emergency cases. In this work, we introduced complex context handlers, able of deducting access control policies by dynamically examining contextual attributes when permitting access to medical sensitive information. We conclude that ABAC with personalized complex context handlers is more efficient than baseline ABAC and ABAC with non-personalized complex context handlers in identifying emergency conditions, notably in the oldest age group which is the most crucial.

3) **It proposes Prognostic-based Context Handlers.** In an emergency situation, the criticality of a patient's medical condition should be taken into account when granting access to her EHRs. Such emergency access controls are necessary so that healthcare professionals make informed decisions in life threatening situations. In this

dissertation, machine learning techniques are developed, based on patients' health metrics and integrated them with an ABAC paradigm which can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers which can be used so as to identify acute care conditions. The predicted health metrics values were evaluated by our personalized fuzzy context handlers, in order to predict the criticality of patient's status. In addition, based on patient's health metrics and personal information, a prediction if the patient is in peril for hypertension or cerebrovascular diseases, was made, by leveraging NNs. In addition, this in this dissertation a sufficient web application was developed, so as to evaluate this work. The dissertation reached a consensus that 4.2%, 14.9% and 5.4% of the patients per each prognostic ABAC case respectively, have different access control results regarding the current and the future health status on the next couple of hours.

4) **It proposes a Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records.** As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient's health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. The research objective of our work is to develop a proactive access control method that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party. To enable proactivity, we apply Long Short Term Memory (LSTM) Neural Networks (NNs) that utilize patient's recent health history to prognose the next two-hour health metrics values. Fuzzy logic is used to evaluate the severity of the patient's health state. These techniques are incorporated in a private and permissioned Hyperledger-Fabric blockchain network, capable of securing patient's sensitive information in the blockchain network. Integrating this predictive mechanism within the blockchain network proved to be a robust tool to enhance the performance of the access control mechanism. Furthermore, our blockchain network can record the history of who and when had access to a specific patient's sensitive EHRs, guaranteeing the integrity and security of the data. This proposed mechanism informs proactively the emergency

team about patients' critical situations by combining fuzzy and predictive techniques, and it exploits the distributed data of the blockchain network, guaranteeing the integrity and security of the data, and enhancing the users' trust to the mechanism.

5) **It proposes Neural-Network based context handlers for Diagnostic Access Control.** In this work machine learning techniques were developed, based on patients' health metrics and integrated them with an ABAC paradigm which can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers which can be used so as to identify probable medical diseases. In addition, based on patient's health metrics and personal information we made a prediction if the patient is in peril for hypertension or cerebrovascular diseases, by leveraging NNs. In addition, in this work an appropriate web application was developed, so as to evaluate this work.

C. *Relation to Research Projects*

The current PhD dissertation has been partially financially supported by the following European Commission project:

- ASCLEPIOS (Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare), H2020 project has received funding from the EU under Grant Agreement 826093 (https://www.asclepios-project.eu/).

- The vision of ASCLEPIOS is to maximize and fortify the trust of users on cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. While researchers have developed many theoretical models that could enhance the security level of healthcare services, only a rudimentary set of techniques are currently in use. ASCLEPIOS is exploiting this gap by using several modern cryptographic approaches to build a cloud-based eHealth framework that protects users' privacy and prevents both internal and external attacks.
- ASCLEPIOS offers the ability to users to verify the integrity of their medical devices before receiving them while receiving simultaneously certain guarantees about the trustworthiness of their cloud service provider. Furthermore, ASCLEPIOS offers a novel solution through which healthcare practitioners and medical researchers

are able to calculate statistics on medical data in a privacy-preserving way. Finally, various activities will be organized by the project to raise awareness in the healthcare industry. All these results are shown by three demonstrators provided by ASCLEPIOS healthcare partners, involving three leading European hospitals.

- The main parts of the current Ph.D. dissertation are based upon the work conducted in the context of the ASCLEPIOS project, as presented in Chapter 12.2 and 12.3.

D. Research Design and Structure of the Dissertation

This dissertation hinges upon fundamental scientific areas of Clinical Decision Support Systems, Contextual Information, Attribute-based Access Control, Fuzzy Logic, Artificial Neural Networks, Long Short Term Memory Neural Networks, Healthcare Analytics, and a Blockchain Network (Hyperledger Fabric Platform) as presented in the following Figure 1.1.

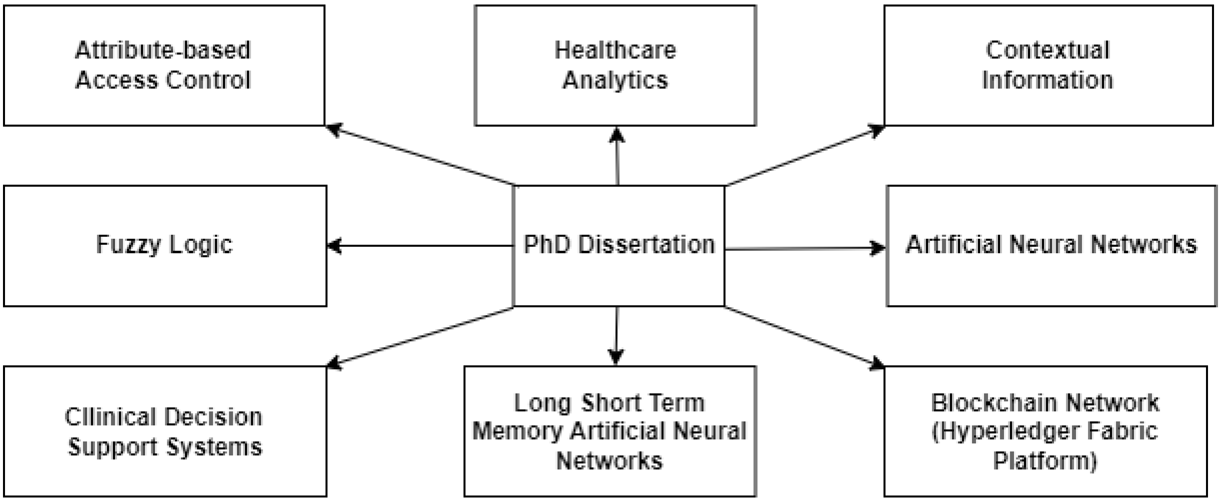

Attribute-based Access Control
Healthcare Analytics
Contextual Information
Fuzzy Logic
PhD Dissertation
Artificial Neural Networks
Cllinical Decision Support Systems
Long Short Term Memory Artificial Neural Networks
Blockchain Network (Hyperledger Fabric Platform)

Figure 1. 1 The fundamental scientific areas of this dissertation.

In addition, the main contributions of this PhD dissertation are presented in the following Figure 1.2, as presented in Chapters 4 - 8 respectively.

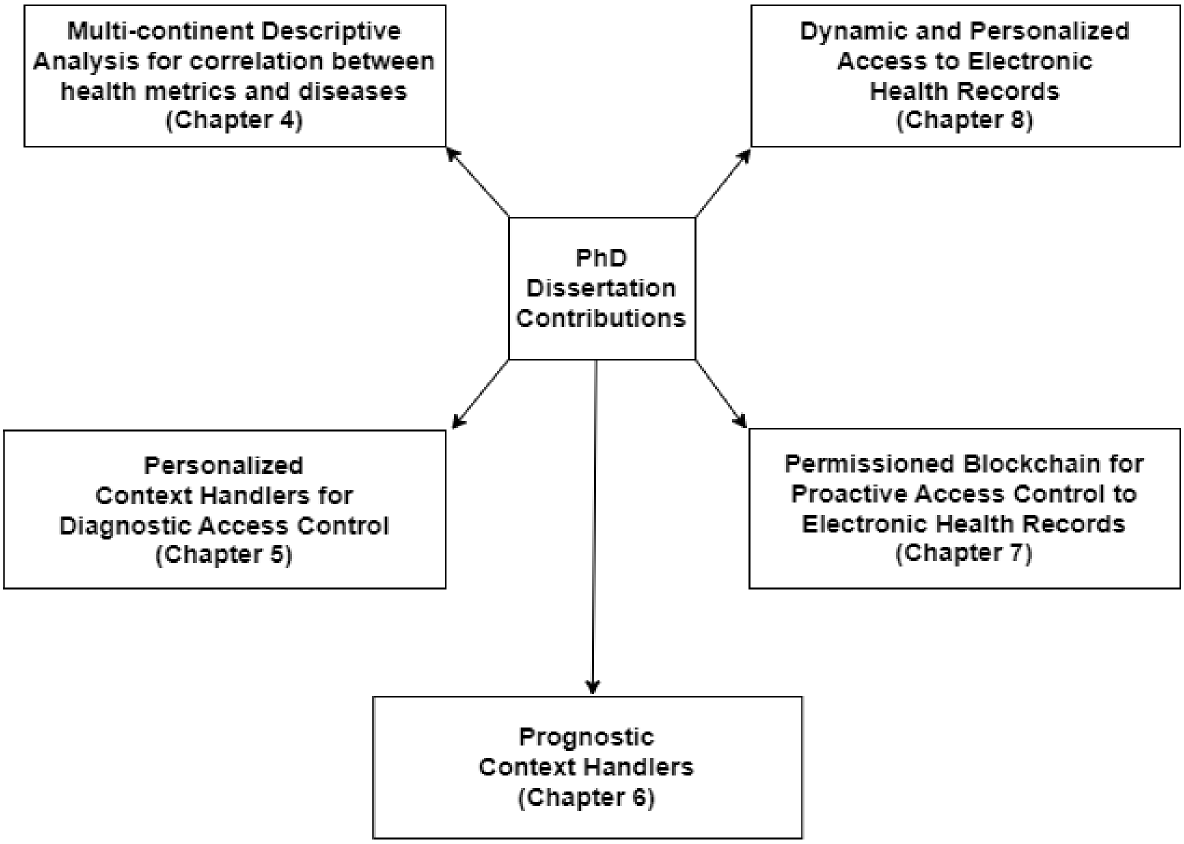

Multi-continent Descriptive Analysis for correlation between health metrics and diseases (Chapter 4)
Dynamic and Personalized Access to Electronic Health Records (Chapter 8)
PhD Dissertation Contributions
Personalized Context Handlers for Diagnostic Access Control (Chapter 5)
Permissioned Blockchain for Proactive Access Control to Electronic Health Records (Chapter 7)
Prognostic Context Handlers (Chapter 6)

Figure 1. 2 The main contributions of this PhD dissertation.

The following table presents the contents of each step of the adopted research methodology as well as the Chapters of the PhD dissertation to which they correspond.

Table 1. 1 The steps of the adopted research methodology and the chapters of this Ph.D.dissertation

Research Methodology Steps	Contents
Related Work based on ASCLEPIOS project (Chapter 2)	• Access Control ○ Attribute-based Access Control Architecture ○ Examples of ABAC and ABE Policies, and Policy Validations ▪ Scenario of the example ▪ ABAC Policy • Contextual information ○ Context Definition ○ Non-Healthcare-related Contextual Information ○ Healthcare-related Contextual Information ○ Contextual Attributes for Emergency Assessment ○ CAPEC Taxonomy • OpenEHR ○ OpenEHR Definition

	○ OpenEHR Architecture ○ Archetype Editor ○ Template Designer • Medical Taxonomies
Research Questions (Chapter 3)	• Motivation of Research Questions • Summary of Research Questions
Multi-continent Descriptive Analysis for correlation health metrics and diseases (Chapter 4)	• Motivation • Methods and Tools ○ Survery Methodology ▪ Search Strategy of Single-continent-oriented Descriptive Analysis ▪ Research Questions of Single-continent-oriented Descriptive Analysis ▪ Search Strategy of Single-continent-oriented Descriptive Analysis ▪ Selection Criteria of Single-continent-oriented Descriptive Analysis ▪ Results of Single-continent-oriented Descriptive Analysis ▪ Search Strategy of Multi-continent-oriented Descriptive Analysis • Evaluation / Validation ○ Results ▪ DBP and SBP per Continent ▪ Body Mass Index per Continent ▪ Hypertension based on BMI per Continent ▪ Smoking Habits based on BMI per Continent ○ Validation ○ Discussion ▪ Relations between SBP and DBP with age and gender per continent ▪ Relations between BMI and age and gender per continent ▪ Relations between Hypertension and BMI per continent ▪ Relations between Smoking habit and BMI per continent
Personalized Context Handlers for Diagnostic Access Control (Chapter 5)	• Motivation • Methods and Tools ▪ Methods ❖ A fuzzy-logic based approach for context handling ❖ Criticality Assessment using Fuzzy Context Handlers ❖ Example ○ Example with non-complex fuzzy rules ○ Example with conjunctive fuzzy rules ❖ Personalization of context handling ○ Personalization of context handling with non-

	complex fuzzy rules ○ Personalization Approach for Complex Context Handling ○ Evaluation / Validation ▪ Personalzation of context handling with non-complex fuzzy rules ❖ Implementation ❖ Datasets & Scenarios ❖ Access Control Results ○ Permit and Deny Results for each ABAC Method per age Group ○ False Positives and Negatives for each ABAC Method per Age Group ▪ Complex Fuzzy Personalized Context Handlers ❖ Implementation ❖ Access Control Results ○ Permit and Deny Access Control Results Grouped per Age for each ABAC Method ○ False Positives and Negatives per ABAC Method and Age Group
Prognostic-based Context Handlers (Chapter 6)	• Motivation ○ Analytics ▪ Analytics definitions and Categories ▪ Health Analytics definition and Categories ▪ LSTM in healthcare • Methods and Tools ○ Fuzzy Context Handlers ○ Predicting Mechanism • Evaluation / Validation ○ Technical Implementation ○ Evaluation Scenarios and Datasets ○ Results
Permissioned Blockchain for Proactive Access Control to Electronic Health Records (Chapter 7)	• Motivation ○ Introduction ○ Blockchain technologies in the medical sector ○ Hyperledger Fabric Blockchain Platform • Methods and Tools ○ Proactive Access Control Mechanism • Evaluation / Validation ○ Implementation ▪ Architecture of Blockchain-based Access Control Mechanism ▪ Technical Implementation ○ Evaluation ▪ Evaluation Scenarios and Datasets

	▪ Evaluation Results ○ Discussion ▪ Access Control Schemes in Critical Medical Conditions ▪ Contextual Attributes for Access Control in Critical Medical Conditions ▪ Hyperledger Fabric Blockchain for Access Control in Critical Medical Conditions ▪ Non-Hyperledger Fabric Blockchain-based for Access Control in Critical Medical Conditions ▪ Positioning
Dynamic and Personalized Access to Electronic Health Records (Chapter 8)	• Motivation ○ Introduction ○ Access Control in Critical Medical Cases ○ Context-based Information for Access Control ○ Health Analytics Using ANNs • Methods and Tools ○ Diagnostic Context Handlers ○ ANNS for Predicting Health State ○ Methodology ○ Implementation • Evaluation/Validation ○ Evaluation Scenario, Datasets, and Positioning ○ Results ○ Discussion
Conclusions and Future Work (Chapter 9)	• Conclusions • Future Work
List of publications (Chapter 10)	
References (Chapter 11)	
Appendix (Chapter 12)	• EHRServer ○ EHRServer Definition ○ Competitive Advantage of EHRServer ○ Main use cases of EHRServer ▪ Shared Healthcare Record ❖ Typical scenario ▪ Backend for Clinical Mobile Applications ▪ Clinical Research Data source

- - - Distributed Clinical Data Store
      - Main scenario for an EHRServer cluster
  - Exploiting OpenEHR capabilities in EHRServer
    - Administrative User Interface (AUI)
    - Upload an opt file to EHRServer
    - Creation of EHRs
    - Clinical Document Instance Generator XML
    - XML Clinical Document Instance uploading to EHRServer via insomnia
    - XML Clinical Document Instance in the EHRServer (contribution)
    - Creation of three contributions
    - Queries
      - Queries 1st option – Get data
      - Queries 2nd option – Get full document
    - Authorization proxy server
- Context-aware Security Model, Context-aware Security Model Editor and Policy Editor
  - Motivation
  - Methods and Tools
    - ASCLEPIOS Context Aware Security Model
      - Security Context Element Overview
      - Security Context Element Details
    - Context-aware Security Editor and Policy Editor
      - Approach and Architecture
        - Conceptual Architecture
        - Techical Architecture
      - Implementation and Walkthrough
      - Discussion
  - Evaluation / Validation
- Cross-Organization Access Control
  - Methods and Tools
    - Electronic Medical Records during Acute Care
    - Attribute-Based Access Control for Electronic Medical Records
    - Methodology for Dynamic and Fine-Grained Access Control Mechanism
    - Attribute-Based Access Control Modelling for Acute Care
      - Preparation phase
      - Analysis phase
      - Development phase
      - Policies definition phase
      - Policies enforcement phase
  - Evaluation / Validation
    - Implementation and evaluation

	• Acute care information workflow • Correctness evaluation • Performance evaluation • Discussion

The first step (Chapter 3) deals with posing the Research Questions and outlining the proposed solution of the dissertation aiming at paving the way i) to extend the ABAC paradigm by creating personalized context handlers for permitting or denying access to healthcare professionals and additionally performing diagnosis and prognosis of the patient’s health state in order to assist the final decision of the healthcare professional. This ABAC extension is possible by having as a basis the developed Context-aware Security Model, Context-aware Security Model Editor and Policy Editor, which are presented in the Appendix (Chapter 12). In addition, stochastic approaches and machine learning techniques are implemented and used in these context handlers, as well as a blockchain network is implemented for better accuracy.

In the second step (Chapter 4) by using descriptive analytics this dissertation introduces a multi-continent overview based on patient’s health indices and their correlation to contextual information such as gender and age, that serve as a basis for identifying health problems such as obesity, hypertension and smoking habits. In addition, by our analysis, a descriptive synthesis is produced, based on our literature review, which deducts continent-based investigation according to the patient’s heath related information. Finally, in order to validate and compare the results which were extracted by our systematic literature review, we developed and implemented a web application capable of processing and analyzing real datasets in order to present each patient’s current health information along with the mean value of the health metrics of SBP, DBP, BMI and the corresponding percentages of smoking and hypertension per continent so as to facilitate the doctor.

The third step (Chapter 5) introduces personalized context handlers, able of deducting access control policies by dynamically examining contextual attributes when permitting access to medical sensitive information. We conclude that ABAC with personalized complex context handlers is more efficient than baseline ABAC and

ABAC with non-personalized complex context handlers in identifying emergency conditions, notably in the oldest age group which is the most crucial.

The fourth step (Chapter 6) deals with the development of machine learning techniques based on patients' health metrics which are integrated within an ABAC paradigm which can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers which can be used so as to identify acute care conditions. The predicted health metrics values were evaluated by our personalized fuzzy context handlers, in order to predict the criticality of patient's status. In addition, based on patient's health metrics and personal information we made a prediction if the patient is in peril for hypertension or cerebrovascular diseases, by leveraging NNs. This chapter also presents the development of a sufficient web application so that our work is evaluated. We reached a consensus that 4.2%, 14.9% and 5.4% of the patients per each prognostic ABAC case respectively, have different access control results regarding the current and the future health status on the next couple of hours.

In the fifth step (Chapter 7) a permissioned blockchain network is introduced for access control management in emergency health situations, which incorporates machine learning techniques along with a personalized fuzzy mechanism for estimating the patient's future health metrics, related to his recent history. The access control mechanism offers secure access for emergency health care professionals to sensitive medical data. The developed access control mechanism provides secure access for emergency clinicians to sensitive information and simultaneously safeguards the patient's private data. The proposed permissioned blockchain network is capable of securing patient's sensitive information-based on the personalized policies in the blockchain network. Furthermore, this approach is proactive because it provides access control based on near-future predictions about the criticality of the patient's situation. Moreover, it has the ability to track the history of who and when gained access to the sensitive patient's data so that trust is achieved as well.

The sixth step (Chapter 8) introduces machine learning techniques based on patients' health metrics and integrated them with an ABAC paradigm which can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers which can be used so as to identify medical diseases. In addition, based on patient’s health metrics and personal information this dissertation proposes a prediction if the patient is in peril for hypertension or cerebrovascular diseases, by leveraging NNs. In addition, in this work an appropriate web application was developed so as to evaluate this approach.

Chapter 2

2. Background Technologies and Related Works

A. Access Control

1) Attribute-based Access Control Architecture

ABAC architecture (Figure 2.1) comprises: (i) the Policy Enforcement Point (PEP), responsible for securing applications and data; It is responsible for intercepting requests and propagating authorization requests to the Policy Decision Point (PDP); (ii) the Policy Information Point (PIP), which bridges external sources of attributes e.g., LDAP databases; and (iii) the Policy Administration Point (PAP) which managed policies. Policies in ABAC are statements which combine attributes to define acceptable or not actions, therefore permitting or denying access to sensitive data. For example, if a requestor wants to access a specific health record, her request is intercepted by PDP, which evaluates relevant policies managed by PAP and using attribute values fetched from PIP. ABAC has been utilised to control access to Electronic Health Record Systems [1].

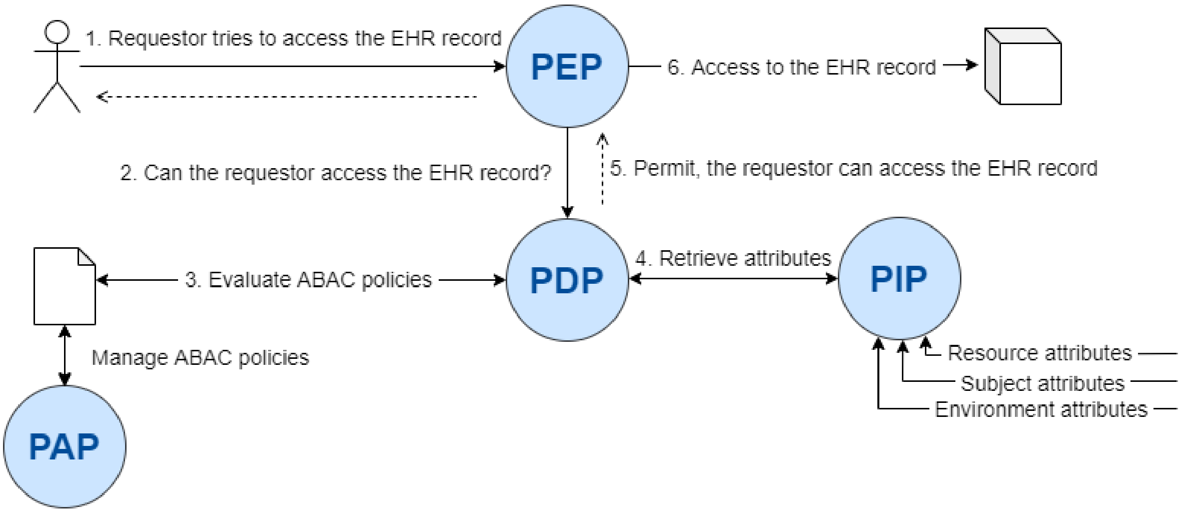

1. Requestor tries to access the EHR record
PEP
6. Access to the EHR record
2. Can the requestor access the EHR record?
5. Permit, the requestor can access the EHR record
3. Evaluate ABAC policies
PDP
4. Retrieve attributes
PIP
Manage ABAC policies
PAP
Resource attributes
Subject attributes
Environment attributes

Figure 2. 1 ABAC Architecture.

In XACML (eXtensible Access Control Markup Language) [2], a context handler is the system entity that converts decision requests in the native request format to the XACML canonical form and converts authorization decisions in the XACML canonical form to the native response format [3]. Independently of whether the XACML standard is used or not, context handlers are used in ABAC in order to convert the attribute representations into means that are relevant to the application environment. Low-level context is useful for inferring higher level context towards identifying critical situations, such as in the case of an emergency medical dispatcher situation. This knowledge is pertinent in deciding whether access to personal healthcare data should be granted or not.

Alternatively to XACML architecture, the Open Policy Agent (OPA) [4] constitutes an open source, general-purpose policy engine which unifies policy enforcement. It provides a high-level declarative language for specifying policy as code and APIs to offload policy decision-making from software. When software needs to make policy decisions, it queries OPA and supplies structured data, e.g., JSON, as input. OPA policies are expressed in the Rego high-level declarative language which is purpose-built for expressing policies over complex hierarchical data structures. According to Siebach [5] OPA system uses its own policy grammar. The difficulty with this system is that it breaks domain boundaries in its approach to obtain attributes, or the policy language used is not simple enough to allow business owners to write the policies. For example, with grammar difficulties, Rego, the language for writing policies in OPA is very expressive, but it requires significant technical development skills to develop policies with it.

For example, let us consider a defined access control policy that permits access to a patient’s Electronic Health Records (EHRs) to doctors only if they are currently located in a specific hospital. A simple service that retrieves the latitude and the longitude of a doctor (e.g., based on a mobile device that transmits GPS data) is not sufficient for enabling the authorization system to yield a permit or deny decision. Additional functionality is required in order to consider the semantic level of the information that the access policy requires and then convert the raw data to indicate whether or not the registered GPS position refers to the specific hospital or not. Therefore, context handlers are dedicated software components that are used for processing raw contextual data relevant to an access control decision and semantically uplifting them as instances of a context model. Context handlers are responsible for fusing the context-aware policy enforcement mechanism with contextual information in a usable format that will enable the evaluation of access control policies. We note that the scope of context handlers can be quite broad and this is why their design and development should use as background knowledge an appropriate context model.

We first introduced the need for context handlers capable of processing raw contextual data and inferring knowledge which is useful for access control as part of our previous work [6] in the cloud platform-as-a-service security domain. Specifically, we have developed context handlers that are able: i) to provide real-time measurements with respect to certain contextual attributes and ii) to uplift the registered attribute value(s) to a semantic level that is appropriate for the application domain and the access control policy at hand. In this work, we further enhance our approach so that it can support context-aware access control in the healthcare domain.

Additionally, the Capability-based Access Control (CapBAC) mechanism exists, where the concept of capability was originally introduced in [7] as "token, ticket, or key that gives the possessor permission to access an entity or object in a computer system". In addition, according to Gusmeroli et al. [8] a capability is a communicable, unforgeable token of authority and it refers to a value that uniquely references an object along with an associated set of access rights. Similarly, in comparison of ABAC with CapBAC we view the following differences. On the one hand, ABAC mechanism has the following advantages over CapBAC: First of all, according to the work of Gusmeroli et al. [8] the ABAC approach, specifies access policies by directly using subject's properties (e.g.: age, location, position etc.), as well as resources and environmental properties, that results in more powerful (and complex) rules and more processing and data availability requirements. In addition, the authors [8], report that the main disadvantage of the capability-based authorization is that it requires issuing capabilities to all subjects, and the selection by the requesting subject of a specific capability when submitting a request. Although capability-based methods have been used as a feature in many access control solutions for the IoT-based applications, applying the original concept of capability-based access control model in IoT network has raised several issues, like capability propagation and revocation [9]. Finally, according to [8], as for other access control mechanisms that have to operate in open, cross domains or cross-enterprise contexts, it is worth mentioning that there is a need to standardize the structure of the capability tokens, the CapBAC supporting services and their access protocols. On the other hand, CapBAC has the following advantages over ABAC: Firstly, Gusmeroli et al. [8] state that a consistent definition of the attributes within a domain is perquisite for ABAC. Additionally, according to the authors [8] ABAC and RBAC systems do not provide flexible delegation rights features.

*2) **Examples of ABAC Policies, and Policy Validations***

a) Scenario of the example

Let a physician needs access to patient data in order to perform his/her work. A (patient) data controller, i.e. a person responsible for collecting and making the data available, imposes certain restrictions on data usage (due to GDPR and corporate policies). Specifically:

- Only users who are physicians with “emergency radiology” classification can access data;
- Access to data is possible during a specific period of time;
- Data controller can, at any time, modify data (in order to remove records of a patient that has withdrew his/her consent for using them).

To make the example more concrete let’s assume that:

- User Id of physician is Physician#45
- User Id of data controller is DC#3
- The dataset path starts with "/datasets/DS12345/"
- Access period is from 2019-10-01 00:00:00Z till 2019-12-31 23:59:59Z
- The user role is given by "user-role" attribute and user classification by "user-classification".

In the following subsections the relevant ABAC authorization policies are discussed while guidelines for policy inspection and security awareness assessment are also provided.

b) *ABAC Policy*

ABAC policy will be used to authorize write operations of data controller and deny write operations of anyone else. In practice the ABAC policy will be captured using XACML language and will be evaluated using an XACML-capable authorization engine.

Table 2. 1 ABAC policy example

Rule #1, permits write operations on data, only if user is the data controller:

```
IF (user-action="WRITE") AND (user-id="DC#3") AND
  (resource-path STARTS WITH "/datasets/DS12345/")
THEN permit
```

Rule #2, grants access only during specific period:

```
IF (current-timestamp NOT BETWEEN
      '2019-10-01 00:00:00Z' AND '2019-12-31 23:59:59Z')
THEN deny
```

Rule #3, grants read access to any user:

```
IF (user-action="READ") AND
  (resource-path STARTS WITH "/datasets/DS12345/")
THEN permit
```

Rule #4, denies access in any other case:

```
IF true THEN deny
```

ABAC policy combining algorithm is "First Applicable", meaning that the first rule that will match (i.e. its IF part evaluates to true) will provide the final result of the policy.

B. Contextual information

1) Context Definition

In healthcare, contextual information, such as information indicating an emergency or criticality in patient's medical condition, should be taken into account when granting access to her medical data in order to ensure the best possible medical response. Hence, there is a need to apply access control protocols with capabilities that incorporate the notion of context, i.e., the consideration of dynamically-changing contextual attributes that may characterize a situation. Context can be perceived as any information that can be used to characterize the situation of an entity (person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves [10]. In fact, the use of contextual information makes it possible to apply access control policies by considering the circumstances under which access requests should be evaluated. For example, in acute care cases, an emergency doctor wants to access parts of the patient's healthcare and medical information to cope best with an acute care situation. Contextual attributes values can be acquired for example from IoT sensors. Consider, for example, a smartwatch with blood pressure measurement capabilities. Still, contextual attributes are often too low-level and cannot be used to characterise a situation of used in isolation. Contrary, by processing contextual attributes, context can be uplifted: low-level contextual attributes can be used to detect higher-level context that characterises a situation.

2) Non-Healthcare-related Contextual Information

This section cites scientific works from the literature which introduced contextual attributes that were the basis for the development of our context model. For example, biometric information has been proposed as attributes that can be used for authorizing access to sensitive data [11]. Bethencourt et al. [12] used attributes, such as the Name and the City of location of a person, in order to authorize access to a particular dataset. Müller et al. [13] introduced as attribute the term of being underage or not, and Moffat et al. [14] considered as attributes the role, the gender and the country. Additionally, Wang et al. [15] considered the role of Employee as an attribute.

3) ***Healthcare-related Contextual Information***

In the Healthcare domain [16], were proposed as attributes the role of Doctor and Researcher. In the example given, a party might want to share medical data only with a user who has the attribute of Doctor or the attribute of Researcher. Paper [17] proposed as attributes the roles of: Surgeon, Medical Researcher and Rehabilitation Doctor. As an example, in an e-Health system, a patient may like to share medical data with a user who has the attribute Surgeon issued by a hospital and the attribute Medical Researcher issued by a clinical research center. In addition to this, a patient should define an access policy as ("Surgeon" AND "Medical Researcher") before encrypting his/her data under this policy. In this scenario two authorities exist: the hospital and the clinical research center. In case of a surgeon's resignation from the hospital, s/he loses the attribute Surgeon and cannot decrypt previously shared data anymore. Apart from that, when the patient needs rehabilitation guidance, s/he needs to update the encrypted medical data in order to give Rehabilitation Doctor permission to access the data with the new policy ("Rehabilitation Doctor" AND "Medical Researcher"). In [18] were proposed as attributes, among others, the social security number, the age, the gender and the health condition of a subject. Article [19] considered as subjects the Doctor, the Patient and the Patient's Family Members. In the example given, the patient intents to permit some doctors and family members to access his/her personal health record and simultaneously he may keep the medical condition secret from others. In the approach of [20], were proposed three categories of sets/policies: Person: {Trainee, Doctor}, Place: {Paris, Zip:75001}, Content: "(Kidney and Disease) or Emergency", with a 'composition policy' such as "Person or (Place and Content)", which plays the role of concluding the whole policy. A ciphertext could be associated to Person: "Senior and Doctor", Place: "Paris or London", Content: {Kidney, Disease, Cancer}. Paper [21] considered, among others, as attributes the role of Doctor and the role of Researcher. In the example given, they proposed the following context expression: (“Doctor” or “Researcher”). Article [22] considered, among others, as attribute the role of Doctor and the role of Researcher. In the approach of paper [23], are proposed as attributes, among others, the doctor’s specialty and the associated hospital. In the example given, they proposed the following context expression: (“Cardiologist” and (“Hospital A” or “Hospital B”)).

4) __Contextual Attributes for Emergency Assessment__

Context describes a specific situation by capturing the setting or circumstances in which an event occurs. A contextual attribute represents a measurable contextual primitive (e.g., a user’s current location). It is the full set of contextual attributes that comprise the context of a situation (e.g., an access request that is initiated by a user from a specific location, to access a resource, at a particular time of day, on a specified day of the week). Our approach extends ABAC with healthcare-related context handlers that can uplift raw contextual information so as to consider the critically of a patient’s health condition in the access control process.

Attributes in ABAC fall into four different categories [24]: (i) Subject attributes which define the user requesting the access e.g., age, department. (ii) Action attributes which define the requested action e.g., read, delete. (iii) Resource (or object) attributes which define the object of access e.g., the object type (medical record). (iv) Contextual (environment) attributes associated with dynamic aspects of the access control scenario, e.g. time.

To identify contextual attributes that can serve in the assessment of health emergencies, we reviewed several existing works. Yunda et al. [25] consider Age, Body Mass Index (BMI), Gender, Systolic Blood Pressure, and Medication intake as inputs, so as to estimate the Cardiovascular disease risk. Likewise, Kalaivani and Sivakumar [26] evaluate as inputs the Systolic Blood Pressure, Heart Rate, and Blood Sugar so as to estimate the patient’s Risk Level. Guzman et al. [27] propose the attributes of Systolic and Diastolic Blood Pressure in their neuro-fuzzy hybrid model which is proposed as a new artificial intelligence method to classify blood pressure. A novel fuzzy expert system for detection of Coronary Artery Disease, using cuckoo search algorithm, is described by Moameri and Samadinai [28] by considering the attributes: Age, Chest pain type, Resting blood pressure, Electrocardiographic Results, Maximum Heart Rate, and Cholesterol level.

A number of researchers take into account personal characteristics of a user when evaluating access policies. For example, elevated heart rate can be considered critical for a certain patient only if the age, the current activity or even his medical conditions are considered. Leyla and MacCaull [29] focus on Personalized Access Control where the patient decides who can access his health records. Zerkouk et al. [30] propose an access control model, based on the user capabilities and behavior, in order to assist automatically the dependent people according to the occurred situation.

5) ***CAPEC Taxonomy***

The Common Attack Pattern Enumeration and Classification (CAPEC) taxonomy [31] represents concepts related to security awareness. For example, the class Subvert Access Control, a subclass of Mechanisms Of Attack, has instances that correspond to an attacker who actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication as well as manage access to its resources or authorize functionality [31]. Subclasses of Subvert Access Control include Authentication Abuse and Authentication Bypass. The former has instances which correspond to an attacker who obtains unauthorized access to an application, service or device either through knowledge of the inherent weaknesses of an authentication mechanism, or by exploiting a flaw in the authentication scheme's implementation. The latter has instances that correspond to an attacker who gains access to application, service, or device with the privileges of an authorized or privileged user by evading or circumventing an authentication mechanism.

C. ***OpenEHR***

1) ***OpenEHR Definition***

OpenEHR is a technology for e-health, produced and managed by the openEHR Foundation, an international non-profit organization established in 2003. All health data of a patient is stored in a consistent, patient-centered EHR. An openEHR solution may be deployed as a common platform between a set of health care providers.

OpenEHR consists of:

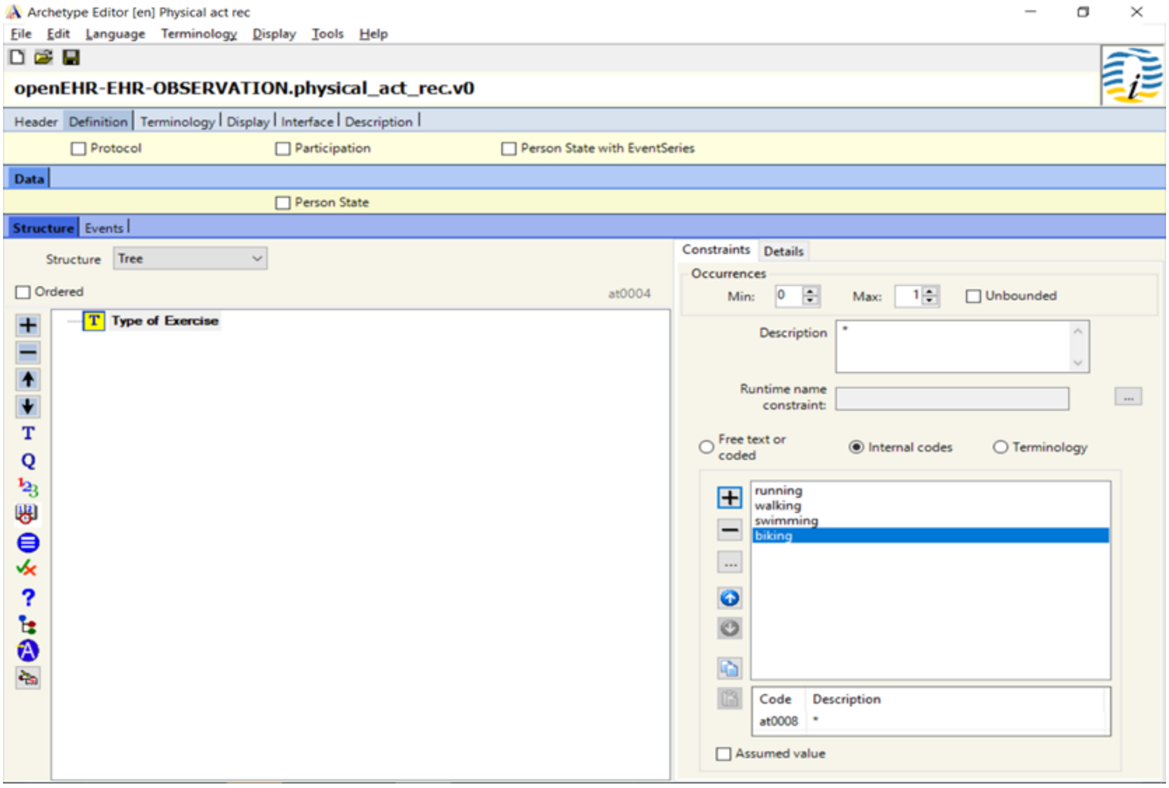
- **Specifications**: formal models and languages defining the openEHR technical platform
- **Clinical models**: building archetypes which act as international standards for re-usable clinical content
- **Softwares**: open source implementations of tools and healthcare information system components
- **Education**: aims to enable the efficient use of openEHR within diverse healthcare cultures and environments

2) OpenEHR Architecture

The openEHR specifications include information models for healthcare data, including:

- **The EHR** (how to record clinical observations)
- **A query language**. It enables queries to be built based on the archetypes, rather than physical database schemata, thus decoupling queries from physical persistence details.
- **The archetype formalism**. The ‘archetypes' and 'templates' are formal models of clinical and related content. A growing set of lightweight REST-based APIs based on archetype paths are used for application access.
- **An open API specification**. A growing set of lightweight REST-based APIs based on archetype paths are used for application access.

3) ***Archetype Editor***


Archetype Editor [en] Physical act rec
File Edit Language Terminology Display Tools Help
Header Definition Terminology Display Interface Description
Data
Structure Events
Constraints Details
Occurrences
Runtime name constraint:
...

openEHR-EHR-OBSERVATION.physical_act_rec.v0

□ Protocol □ Participation □ Person State with EventSeries

□ Person State

Structure: Tree

□ Ordered at0004

Type of Exercise

Min: 0 Max: 1 □ Unbounded

Description: *

○ Free text or coded ● Internal codes ○ Terminology

running
walking
swimming
biking

Code	Description
at0008	*

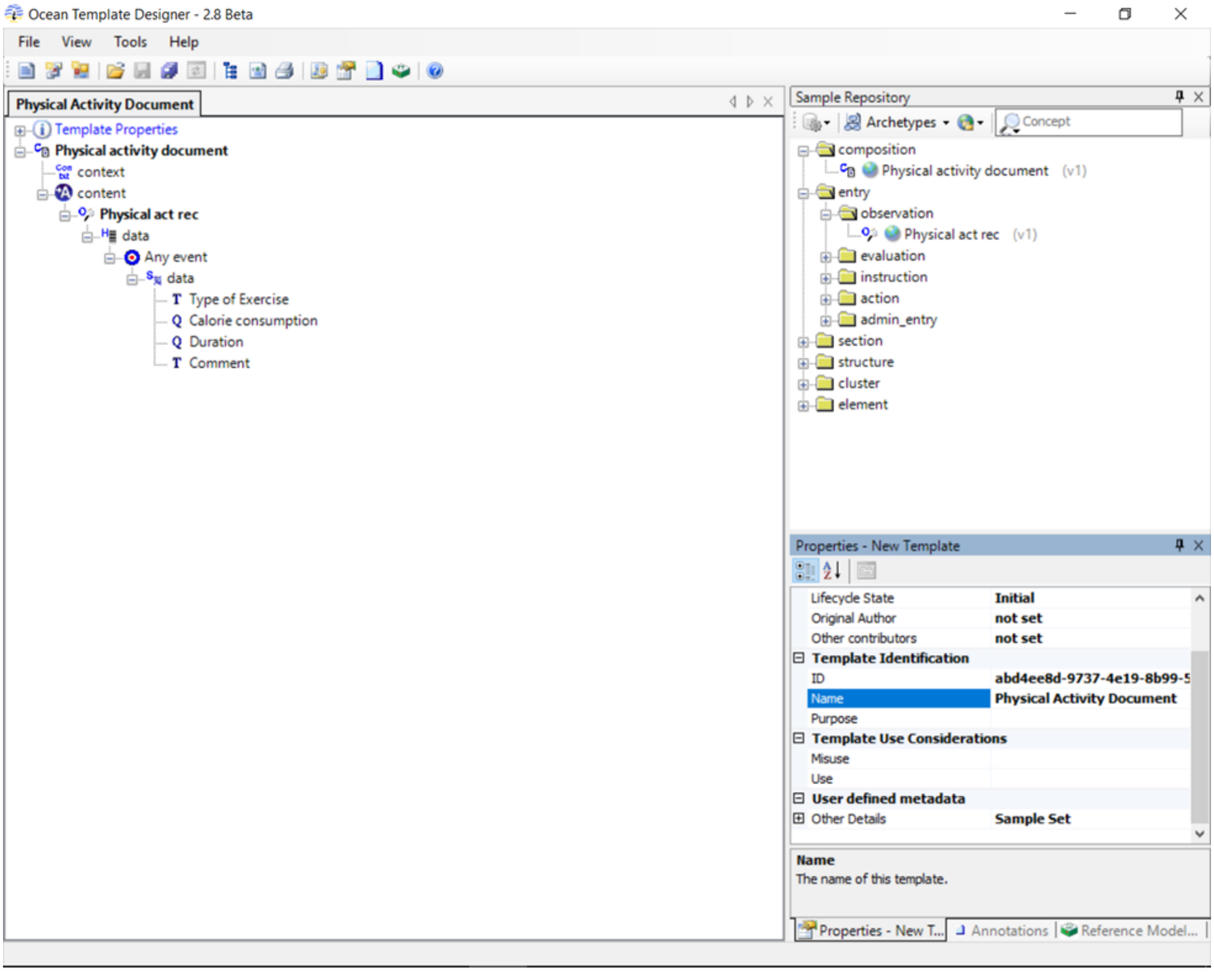
□ Assumed value

Figure 2. 2 Archetype Editor.

Archetype Editor is a software which is used to create a definition of the clinical record that will be stored in a EHR. A template is a full definition of a clinical document or a clinical record. Before creating the template we need to create the parts of that document. Those parts of that document are called “Archetypes” Since every data structure in OpenEHR is contained in a composition (a composition is the model for clinical document in EHR) we need to create a composition that contains this physical activity record (observation).

4) ***Template Designer***

Template Editor is a tool useful to develop a clinical template from given archetypes.



Lifecycle State	Initial
Original Author	not set
Other contributors	not set
Template Identification	
ID	abd4ee8d-9737-4e19-8b99-5
Name	Physical Activity Document
Purpose	
Template Use Considerations	
Misuse	
Use	
User defined metadata	
Other Details	Sample Set

Name
The name of this template.

Figure 2. 3 Template Designer.

D. *Medical Taxonomies*

In general, medical terms could have different meaning among some members of the medical community, or it could be possible to use different terms which have the same meaning. Under these circumstances, there was the need of a cohesive and structured vocabulary. In order to enable the medical community worldwide to communicate under a common vocabulary, with the same meaning and without vagueness, a medical international nomenclature was established. Thus, medical taxonomies were defined. There are a lot of such taxonomies which serve this cause and ensure the cohesiveness of the medical terms. We briefly present below some of the most used ones.

A classification of drugs internationally was assigned by the Food and Drug Administration of USA which designated specific codes for drugs that constitute the National Drug Code (NDC) taxonomy [32]. First of all, NDC taxonomy includes the following categories: the “Product ID” which is a forty character code, the “Product

NDC" which is an eight digit code which also defines the first eight digits of the product id, the "Product Type Name" which describes the general type of the drug e.g. "Human OTC Drug" (OTC drugs are those sold directly to a consumer without the prescription from a healthcare professional as opposed to prescription drugs), the "Proprietary Name" which is the brand name e.g. "aspirin adult low dose aspirin", the "Proprietary Name Suffix", the "Non Proprietary Name" which is an official generic given to a pharmaceutical drug in order to make communication more precise e.g. "Aspirin", the "Dosage Form Name" e.g. "tablet, delayed release", the "Route Name" which is the way of taking the drug e.g. "oral", the "Start Marketing Date" e.g. "20070112", the "End Marketing Date", the "Marketing Category Name" e.g. "OTC monograph final", the "Application Number" e.g. "part343", the "Labeller Name" e.g. "Liberty Pharmaceuticals, Inc"., the "Substance Name" e.g. "Aspirin", the "Active Numerator Strength" e.g. "81", the "Active Ingrid Unit" e.g. "mg/1", the "Pharm Classes" which describes the drug's pharmacological classification like its chemical type, the "DEA Schedule" which is a classification by United States Drug Enforcement Administration, according to the need of prescription for controlled substances, the "NDC Exclude Flag" which indicates whether the product has been removed/excluded from the NDC Directory and the "Listing Record Certified Through" which indicates the date when the drug will expire if not updated or certified by the firm.

The Health Level Seven Version 3 (HL7 V3) Normative Edition [33] which is a suite of specifications based on HL7's Reference Information Model (RIM), provides a single source that allows implementers of V3 specifications to work with the full set of messages, data types, and terminologies needed to build a complete implementation. The Version 3 Normative Edition represents a new approach to clinical information exchange based on a model driven methodology that produces messages and electronic documents expressed in XML syntax. The V3 specification is built around subject domains that provide storyboard descriptions, trigger events, interaction designs, domain object models derived from the RIM, hierarchical message descriptors (HMDs) and a prose description of each element. Implementation of these domains further depends upon a non-normative V3 Guide and normative specifications for: data types; the XML technical specifications (ITS) or message wire format; message and control "wrappers", and transport protocols. This classification of patient demographic information, which refers to a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers, includes the following categories: the “Partial or complete patient name” which is printed on the patient record or is told by the patient, the “Patient ID” which may be obtained from printed barcode or a bed-side chart etc., the “Partial ID entry or scan”, the “Date of birth / age range” and the “Bed ID”.

The classification of Procedures in healthcare area is set by the American Medical Association through the Current Procedural Terminology (CPT) [34] which is a taxonomy that describes medical, surgical, and diagnostic services and is designed to communicate uniform information about medical services and procedures among physicians, coders, patients, accreditation organizations, and payers for administrative, financial, and analytical purposes. According to this classification, procedures are defined by a ten digit code number and they are classified in the following main sections: “Anesthesia”, “Surgery”, “Radiology”, “Pathology and Laboratory procedures”, “Medicine Services and Procedures”, “Evaluation and Management Services”, “Category II Codes”, “Multianalyte Assay”, “Category III Codes” and the “Laboratory Analyses”.

A classification of medical specialties was assigned by the National Uniform Claim Committee (NUCC) [35]. This NUCC taxonomy includes the following categories:

- the “Code” which is a ten character code
  e.g. “1223P0221X”

- the “Grouping” which describes the general group of the specialty
  e.g. “Dental Providers”

- the “Classification” which describes the specialty
  e.g. “Dentist”, “Oral Medicinist”, “Dental Hygienist”, “Dental Therapist”

- the “Specialization”
  e.g. “Pediatric Dentistry”

- the “Definition”
  e.g. “An age-defined specialty that provides both primary and comprehensive preventive and therapeutic oral health care for infants and children through adolescence, including those with special health care needs”

- “Notes”
  e.g. “Source: Council on Dental Education and Licensure, American Dental Association”

Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT) [36] is a systematically organized computer processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting. SNOMED CT is considered to be the most comprehensive, multilingual clinical healthcare terminology in the world. SNOMED CT is maintained and distributed by SNOMED International, an international non-profit standards development organization. SNOMED CT was created in 2002. Below is a list of the Top Level Concepts with a brief description of the content represented in their branch of the hierarchy.

- Clinical finding - the result of a clinical observation, assessment or judgment (e.g. asthma, headache).
- Procedure - activities performed in the provision of health care (e.g. appendectomy, physiotherapy, subcutaneous injection).
- Situation with explicit context - concepts in which the clinical context is specified as part of the definition of the concept itself (e.g. endoscopy arranged, past history of myocardial infarction, family history of glaucoma).
- Observable entity - a question or assessment which can produce an answer or result (e.g. systolic blood pressure, colour of iris, gender).
- Body structure - normal and abnormal anatomical structures (e.g. mitral valve structure, adenosarcoma).
- Organism - organisms of significance in human and animal medicine (e.g. streptococcus pyogenes, beagle).

- Substance - general substances, the chemical constituents of pharmaceutical/biological products, body substances, dietary substances and diagnostic substances (e.g. methane, insulin, albumin).
- Pharmaceutical/biologic product - drug products (e.g. amoxicillin 250mg capsule, paracetamol + codeine tablet).
- Specimen - entities that are obtained (usually from the patient) for examination or analysis (e.g. urine specimen, prostate needle biopsy specimen).
- Special concept - concepts that do not play a part in the formal logic of the concept model of the terminology, but which may be useful for specific use cases (e.g. navigational concept, alternative medicine poisoning).
- Physical object - natural and man-made physical objects (e.g. vena cava filter, implant device, automobile).
- Physical force - physical forces that can play a role as mechanisms of injury (e.g. friction, radiation, alternating current).
- Event - occurrences excluding procedures and interventions (e.g. flood, earthquake).
- Environments and geographical locations - types of environments as well as named locations such as countries, states and regions (e.g. intensive care unit, academic medical centre, Denmark).
- Social context - social conditions and circumstances significant to health care (e.g. occupation, spiritual or religious belief).
- Staging and scales - assessment scales and tumour staging systems (e.g. Glasgow Coma Scale, FIGO staging system of gynaecological malignancy).
- Qualifier value - the values for some SNOMED CT attributes, where those values are not subtypes of other top level concepts. (e.g. left, abnormal result, severe).
- Record artefact - content created for the purpose of providing other people with information about record events or states of affairs. (e.g. patient held record, record entry, family history section).
- SNOMED CT Model Component - contains technical metadata supporting the SNOMED CT release.

Logical Observation Identifiers Names and Codes (LOINC) [37] is a database and universal standard for identifying medical laboratory observations. A fully specified name in LOINC includes.

Table 2. 2 LOINC taxonomy's fields – example

Field	**Description**	**Examples**
Component (analyte)	The name of the component or analyte measured	Potassium, Hemoglobin, Hepatitis C antigen.
Property measured	The characteristic of how the component is being measured	A mass concentration, Enzyme activity (catalytic rate).
Timing	Whether the measurement is an observation at a moment of time, or an observation integrated over an extended duration of time	24-hour urine.
System	The type of sample	Urine, Blood
Scale	Whether the measurement is: 1. quantitative (a true measurement) 2. ordinal (a ranked set of options) 3. nominal (that do not have a natural ordering) 4. narrative	1. The mm diameter of the inhibition zone. 2. An antimicrobial susceptibility that can be reported as resistant, intermediate, susceptible. 3. E. coli, Staphylococcus

		aureus. 4. Dictation results from x-rays.
Method	Where relevant, the methodology used to produce the result or other observation.	Rapid Plasma Reagin, Branched chain DNA (bDNA).

International Classification of Diseases (ICD) [38] is an international standard (diagnostic classification) for reporting diseases and health conditions. It defines the universe of diseases, disorders, injuries and other related health conditions, listed in a comprehensive, hierarchical fashion that allows for: easy storage, retrieval and analysis of health information for evidenced-based decision-making; sharing and comparing health information between hospitals, regions, settings and countries; data comparisons in the same location across different time periods. The uses of ICD include monitoring of the incidence and prevalence of diseases, observing reimbursements and resource allocation trends, and keeping track of safety and quality guidelines. They also include the counting of deaths as well as diseases, injuries, symptoms, reasons for encounter, factors that influence health status, and external causes of disease.

ICD-10 taxonomy, which is the latest version, includes the following fields:

Table 2. 3 ICD-10 taxonomy's fields – example

Field	**Description**	**Example**
ICD10Chapter	Chapter in which this entity is located	01
ICD10Code	ICD-10 code for the entity. Note that the groupings do not have a code.	1A07.Z
ICD10Title	Title of the entity	Typhoid fever, unspecified

ICD10ClassKind	Class kind for the ICD-10 entity. It is one of the three (chapter, block, category). Chapter is top level classification entities. Blocks are high level groupings that do not bear a code. Categories are entities that have a code.	Category

The ATC/DDD taxonomy [39] is a standard for international drug utilization monitoring and research. The Anatomical Therapeutic Chemical (ATC) is a classification system. Defined Daily Dose (DDD), which serves as a measuring unit, is the assumed average maintenance dose per day for a drug used for its main indication in adults. It is developed by the Norwegian Institute of Public Health "World Health Organization Collaborating Centre (WHOCC) for Drug Statistics Methodology" as a modification and extension of the European Pharmaceutical Market Research Association (EphMRA) classification system.

The ATC taxonomy includes the following fields:

- ATC code - the several classification levels are depicted in the code
- Name - the name of the chemical substance or the name of the ATC level
    - 1st level - main anatomical or pharmacological group
    - 2nd level - pharmacological or therapeutic group
    - 3rd level - chemical, pharmacological or therapeutic subgroup
    - 4th level - chemical, pharmacological or therapeutic subgroup
    - 5th level - the chemical substance

Table 2. 4 ATC taxonomy's fields – example

ATC code	Name
A	Alimentary tract and metabolism (1st level, anatomical main group)

A10	Drugs used in diabetes (2nd level, therapeutic subgroup)
A10B	Blood glucose lowering drugs, excl. insulins (3rd level, pharmacological subgroup)
A10BA	Biguanides (4th level, chemical subgroup)
A10BA02	metformin (5th level, chemical substance)

The combined ATC/DDD classification includes the following additional fields:

- DDD (Defined Daily Dose) - the number of units of the dose
- Unit - the unit in which the dose is measured e.g. milligram, millilitre etc.
- Route of administration - the way of taking a drug e.g. inhalation, nasal, oral etc.

Table 2. 5 ATC/DDD taxonomy's fields – example

ATC code	**ATC level name or generic name**	**DDD**	**Unit**	**Administration Route**
G04BX15	pentosan polysulfate sodium	0.3	G	O (Oral)

The Clinical Document Architecture (CDA) [40] is a document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients. It is developed by Health Level Seven International (HL7). HL7 is a not-for-profit standards developing organization, dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. More specifically, there is a range of complexity allowed within the specification and users must set their own level of compliance. CDA introduces the concept of incremental semantic interoperability. A minimal CDA consists of a small number of XML-encoded metadata fields such as provider name, document type, document identifier, and a body which can be any commonly-used Multipurpose Internet Mail Extensions (MIME) type such as pdf or doc or even a scanned image file.

The "GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – Patient Summary for unscheduled care" [41] utilizes this taxonomy and has the following fields:

- Patient Administrative data include:
    - Identification
    - Personal information
    - Contact information
    - Insurance information
- Patient Clinical data include:
    - Alerts
    - Medical history
    - Medical problems
    - Medication summary
    - Social history
    - Pregnancy history
    - Physical findings
    - Diagnostic tests
- Metadata include:
    - Country
    - Patient Summary (PS)
    - Nature of the PS
    - Author organization

The "GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – ePrescriptions and eDispensations" [42] utilizes this taxonomy and has the class ePrescriptions.

The Clinical information for cross-border exchange about ePrescription/eDispensation data are set according to the provisions in the “GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – ePrescriptions and eDispensations” which was adopted by the eHealth Network on 21 November 2016.

- ePrescriptions data include:
    - Identification of the patient
    - Authentication of the prescription
    - Identification of the prescribing health professional
    - Identification of the prescribed product
    - Prescription information

Chapter 3

3. Research Questions

A. Motivation of Research Questions

The proposed solution aims to fulfill the identified research gaps and thus, to answer to the aforementioned research questions. The way with which the current dissertation addresses the research questions are described in the following sections. The following table shows the alignment of research questions with the dissertation's propositions along with the related publications and chapters (Chapters 4 - 8). More precisely, the five research questions are aligned with the five Chapters 4 - 8. Additionally, the publications related to the chapters 4, 5, 6, 7, and 8, have their respective information systems which are in details analyzed regarding their technical and usability functionalities and the respective evaluation results per system. Additionally, Chapter 9 discusses the overall evaluation results and respective results which are derived by this dissertation, as well as the limitations of the current research and future work which can alleviate these current limitations. Finally, Chapter 10 cites the journal and conference research works, which have been created within this Ph.D. dissertation.

Table 3. 1 Research Questions – Dissertation's Proposition - Publications

#	Research Questions	Dissertation's Proposition	Related Publications	Chapter
RQ1	How a descriptive analysis all over the world which connects patient's personalized information with healthcare diseases, is to define specific relation patterns among continents?	Multi-continent Descriptive Analysis for correlation between health metrics and diseases	c1	4
RQ2	Which method is to be	Complex / Non-	j1	5

	developed that can be used by medical experts to characterize critical, emergency situations requiring extraordinary access to healthcare data based on dynamically changing contextual attributes?	complex Fuzzy Personalized Context Handlers for Diagnostic Access Control		
RQ3	Which machine learning techniques are to be developed and applied for acquiring the prognosis of emergency situations?	Machine Learning-based Context Handlers for Prognostic Access Control	j2	6
RQ4	Which proactive access control method can be developed that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party?	Permissioned Blockchain for Proactive Access Control to Electronic Health Records	j4	7
RQ5	Which machine learning techniques are to be developed and applied for achieving diseases' diagnosis for medical access control?	Dynamic and Personalized Access Control to Electronic Health Records	j5	8

1) ***Multi-continent Descriptive Analysis for correlation between health metrics and diseases***

The research objectives of this chapter's work (c1) refer to the descriptive analysis all over the world of the relation of the patient's nationality, age and gender with the systolic blood pressure (SBP) and diastolic blood pressure (DBP), the Body Mass Index (BMI), and the potential of being hypertensive or smoker, along with correlations between them, and to define specific relation patterns among continents. Existing surveys focus on country-based or continent-based health metrics combination and do not address all the multi-continent aspect. This approach provides a comprehensive and systematic literature review that, after the selection process, covers 36 papers on the field of country-based health metrics combination. We bring together all these research works by aggregating them and thus achieving a descriptive synthesis, based on the reported descriptive analysis.

2) ***Personalized Context Handlers for Diagnostic Access Control***

The research objectives of this chapter (j1) are threefold: First, to develop a method that can be used by medical experts to characterize critical, emergency situations requiring extraordinary access to healthcare data, based on dynamically changing contextual attributes. Second, to apply the ABAC paradigm and its context-handling capabilities in order to implement the proposed context-uplifting method for characterizing situations. Third, to enable personalization in the way contextual attributes are used to characterize situations for different users.

3) ***Prognostic-based Context Handlers***

The main research objective of this chapter's study (j2) is the development and application of machine learning techniques based on patients' health metrics and integrate them with an ABAC paradigm. This mechanism can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers in which raw contextual information e.g., data from IoT devices, can be used in order to identify acute care conditions and permit access to sensitive medical information. More specifically, we are going to use the patient's health history in order to predict the health metrics of the next couple of hours by implementing Long Short Term Memory (LSTM) Neural Networks (NNs). The prognosed health metrics values are to be evaluated by our personalized fuzzy context handlers, so as to estimate the criticality of the health condition of patient. Finally our objective is to develop a sufficient web application so as to evaluate our approach and compare with our previous work (j1).

4) ***Permissioned Blockchain for Proactive Access Control to Electronoc Health Records***

The research objective of this chapter's work (j4) is to develop a proactive access control method that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party. We build a proactive access control mechanism within the blockchain system that exploits smart contracts of our private and permissioned Hyperledger Fabric-based blockchain network, which, based on our predictive model, and combined with our personalized fuzzy approach, examines recent health metrics of a patient and outputs the patient's health criticality assessment, effectively managing access to the patient's EHRs.

5) ***Dynamic and Personalized Access Control to Electronic Health Records***

The main research objective of this chapter's study (j5) is the development and application of machine learning techniques based on patients' health metrics and integrate them with an ABAC paradigm. This mechanism can grant access to a sensitive EHRs system by applying Neural Network based-context handlers in which raw contextual information e.g., data from IoT devices, can be used in order to to estimate if the current patient suffers by hypertension or cerebrovascular diseases, and permit access to sensitive medical information.

B. *Summary of Research Questions*

This Section presents the five research questions of the current thesis. The following Table 3.2 outlines these research questions and their constituting parameters, and Figure 3.1 the research design.

Table 3. 2 Research Questions

#	Research Questions	Areas of Investigation
RQ1	How a descriptive analysis all over the world which connects patient's personalized information with healthcare diseases is to define specific relation patterns among continents?	• Which personal aspects are to be used regarding the dissertation's global descriptive analysis? • Which healthcare diseases the patients' personal contextual attributes can be associated with? • How can this dissertation's multi-continent descriptive analysis assist the doctor for the patient's overall clinical profile in order to make a more accurate medical diagnosis? • How the patient's nationality serves as the basis for this descriptive analysis, besides the personalized health metrics? • Which particular correlations of health metrics and diseases are realized?
RQ2	Which method is to be developed that can be used by medical experts to characterize critical and emergency	• Which access control paradigm should be applied so as to exploit its context-handling

	situations requiring extraordinary access to healthcare data, based on dynamically changing contextual attributes?	capabilities and implement the proposed context-uplifting method for characterizing situations? • How to enable personalization in the way contextual attributes are used to characterize situations for different users? • What are the advantages of the creation and implementation of personalized context handlers for emergency access control? • Which personalization parameters should be applied? • How these personalized context handlers should be used for the diagnosis of the patient's critical health situation? • In which critical situations can this method be applied?
RQ3	Which machine learning techniques are to be developed and applied for acquiring the prognosis of emergency situations?	• Which access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses? • Which health metric values should be prognosed in the next couple of hours? • How this dissertation's prognosis of healthcare-based

		emergency conditions is able to assist the doctor in making the final medical decision? • How the fuzzy logic is able to serve complementary to the machine learning techniques for the information system's prognosis?
RQ4	Which proactive access control method can be developed that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party?	• Which access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses? • Which are the benefits of a private and permissioned blockchain network? • Which health metric values should be prognosed in the next couple of hours? • How this dissertation's prognosis of healthcare-based emergency conditions is able to assist the doctor in making the final medical decision? • How the fuzzy logic is able to serve complementary to the machine learning techniques for the information system's prognosis?

RQ5	Which machine learning techniques are to be developed and applied for achieving diseases' diagnosis for medical access control?	• Which access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses? • Which deseases are diagnosed? • How this thesis' medical diagnosis of diseases prediction is able to assist the doctor in making the final diagnosis?

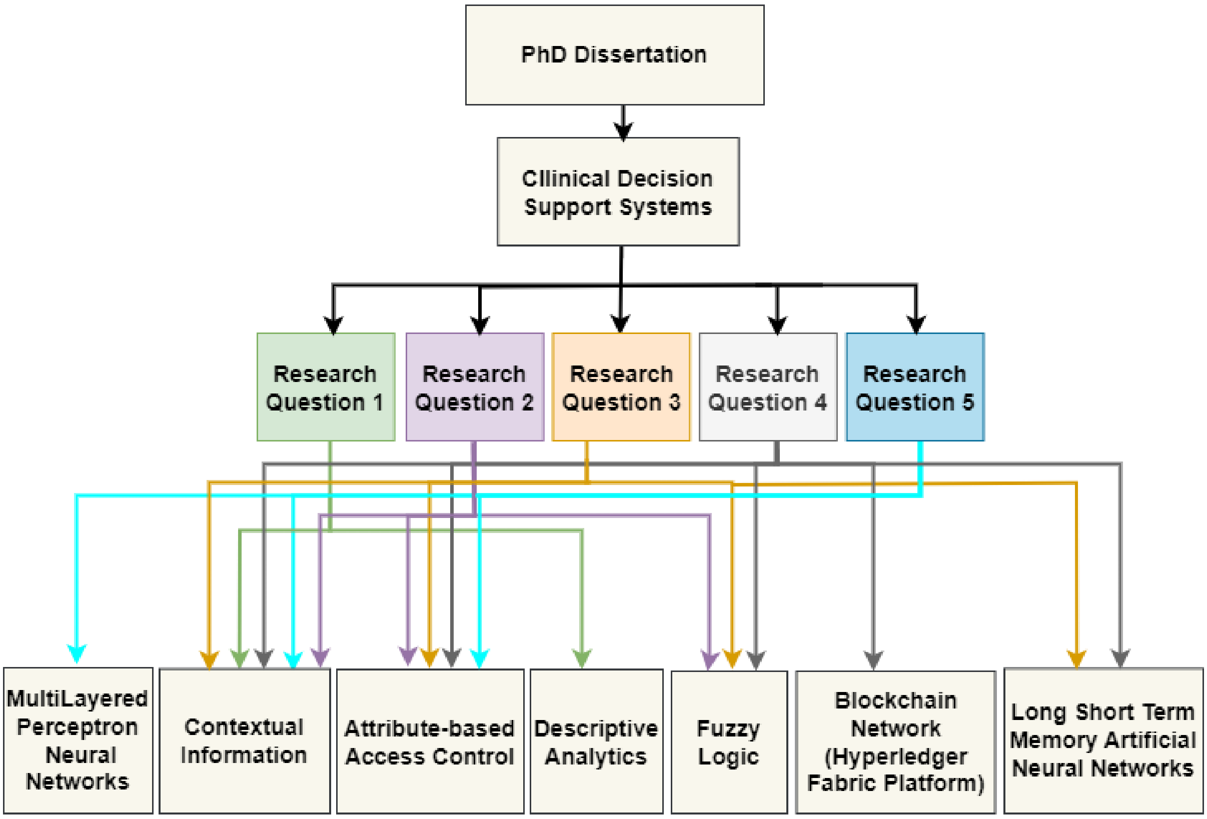

PhD Dissertation
Cllinical Decision Support Systems
Research Question 1
Research Question 2
Research Question 3
Research Question 4
Research Question 5
MultiLayered Perceptron Neural Networks
Contextual Information
Attribute-based Access Control
Descriptive Analytics
Fuzzy Logic
Blockchain Network (Hyperledger Fabric Platform)
Long Short Term Memory Artificial Neural Networks

Figure 3. 1 Research Design

1) ***Research Question 1:*** **How a descriptive analysis all over the world which connects patient's personalized information with healthcare diseases is to define specific relation patterns among continents?**

The three major health problems of hypertension, obesity and smoking are the cause of death of millions of people yearly worldwide. More specifically, the statistics of the World Health Organization regarding the year of 2020 about the healthy living expectancy and the life expectance as well, showed that the more frequent causes of death are the following, as described below. According to the World health Organization, the main global causes of mortality in the world are high blood pressure (responsible for 13% of deaths globally), tobacco use (9%), high blood glucose (6%), physical inactivity (6%), and overweight and obesity (5%). More specifically, according to World Health Organization, raised blood pressure is estimated to cause 7.5 million deaths worldwide, that is about 12.8% of the total of all deaths, while tobacco kills more than 8 million people worldwide per year. Precisely, more than 7 million of deaths are the result of direct tobacco use, while around 1.2 million are the result of non-smokers being exposed to second-hand smoke. Lastly, according to the World Health Organization, obesity has globally reached epidemic proportions, with at least 2.8 million people dying worldwide per year, as a result of being overweight or obese. Once associated with high-income countries, obesity is now also prevalent in low and middle-income countries. So, this current issertation chooses to study the health problems of obesity and hypertension as well the lifestyle choice of smoking because they are related to mortality.

The additional research questions that rise complementary to the main Research Question 1 are the following:

- Which personal aspects are to be used regarding the dissertation's global descriptive analysis?
- Which healthcare diseases the patients' personal contextual attributes can be associated with?
- How can this dissertation's multi-continent descriptive analysis assist the doctor for the patient's overall clinical profile in order to make a more accurate medical diagnosis?

- How the patient’s nationality serves as the basis for this descriptive analysis, besides the personalized health metrics?
- Which particular correlations of health metrics and diseases are realized?

2) ***Research Question 2:*** **Which method is to be developed that can be used by medical experts to characterize critical and emergency situations requiring extraordinary access to healthcare data, based on dynamically changing contextual attributes?**

Controlling access to healthcare data is of great importance because the preservation of the privacy of the patient’s information, such as his medical history, is a legal and societal requirement. Access control models deal with the rights a subject has upon performing some operations (such as read, write, etc.) on specific data objects. In healthcare, contextual information, such as information indicating an emergency or criticality in patient’s medical condition, should be taken into account when granting access to her medical data in order to ensure the best possible medical response. Hence, there is a need to apply access control protocols with capabilities that incorporate the notion of context, i.e., the consideration of dynamically-changing contextual attributes that may characterize a situation.

In fact, the use of contextual information makes it possible to apply access control policies by considering the circumstances under which access requests should be evaluated. For example, in acute care cases, an emergency doctor wants to access parts of the patient’s healthcare and medical information to cope best with an acute care situation. Contextual attributes values can be acquired for example from IoT sensors. Consider, for example, a smartwatch with blood pressure measurement capabilities. Still, contextual attributes are often too low-level and cannot be used to characterise a situation if used in isolation. Contrary, by processing contextual attributes, context can be uplifted: low-level contextual attributes can be used to detect higher-level context that characterizes a situation.

This dissertation argues that context handlers can be valuable for enforcing dynamic authorization processes that take into consideration the criticality of a certain health emergency, before yielding an access control decision. This is quite important, since in emergency situations paramedics and first response teams should have immediate access to patients' health records, although they could not have been considered in the defined policies at design time.

The additional research questions that rise complementary to the main Research Question 2 are the following:

- Which access control paradigm should be applied so as to exploit its context-handling capabilities and implement the proposed context-uplifting method for characterizing situations?
- How to enable personalization in the way contextual attributes are used to characterize situations for different users?
- What are the advantages of the creation and implementation of personalized context handlers for emergency access control?
- Which personalization parameters should be applied?
- How these personalized context handlers should be used for the diagnosis of the patient's critical health situation?
- In which critical situations can this method be applied?

3) ***Research Question 3:*** **Which machine learning techniques are to be developed and applied for acquiring the prognosis of emergency situations?**

Handling access to medical information is essential, as the safeguarding of the patient's sensitive data privacy, e.g., her health history, is of prime importance. Access control models are related to the privileges an entity has upon handling particular data objects. In the medical sector, contextual information which characterizes an emergency in patient's healthcare state, should be deemed when controlling access to the healthcare sensitive information by guaranteeing the most efficient treatment. Accordingly, the implementation of access control models which integrate the context concept, such as the notion of dynamically changing contextual attributes which indicate a status, is needed.

Exploiting contextual data facilitates the implementation of access control policies by taking into account the conditions of access requests evaluation. For instance, in critical situations, an emergency healthcare professional intends to access partially the patient’s healthcare data to encounter best a critical condition. The values of contextual information are obtained for instance from IoT devices, such as a wearable able to gauge the blood pressure. This dissertation reports that context handlers are beneficial for implementing processes of dynamic authorization which consider the critical status of a specific medical acute care event before making a decision access control. In critical conditions the emergency medical teams should access immediately the patients’ medical records.

The additional research questions that rise complementary to the main Research Question 3 are the following:

- Which access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses?
- Which future diseases are to be prognosed and based on which prediction algorithm?
- Which health metric values should be prognosed in the next couple of hours?
- How this dissertation’s prognosis of healthcare-based emergency conditions is able to assist the doctor in making the final medical decision?
- How the fuzzy logic is able to serve complementary to the machine learning techniques for the information system’s prognosis?

4) ***Research Question 4:*** **Which proactive access control method can be developed that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party?**

Access control to healthcare data is vital as the protection of the patient’s sensitive data privacy, e.g. the health history, is of great importance. Access control models are associated with the rights an entity has upon managing particular data objects. These are based on user identity access control models, such as Role-Based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC). Contrarily to these static approaches, the Attribute-Based Access Control (ABAC) paradigm has been introduced, which is dynamic in nature. In ABAC, there are connections’ snapshots that are produced and dynamically altered based on the current context, instead of statically-defined lists of permissions that link entities with objects.

As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient's health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. A major challenge in this area is to enable trustworthiness and to achieve traceability of access control to personal health data in emergency situations.

The additional research questions that rise complementary to the main Research Question 4 are the following:

- Wh*i*ch access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses?
- Which are the benefits of a private and permissioned blockchain network?
- Which health metric values should be prognosed in the next couple of hours?
- How this dissertation's prognosis of healthcare-based emergency conditions is able to assist the doctor in making the final medical decision?
- How the fuzzy logic is able to serve complementary to the machine learning techniques for the information system's prognosis?

5) ***Research Question 5:*** **Which machine learning techniques are to be developed and applied for achieving diseases' diagnosis for medical access control?**

Handling access to medical information is essential as the safeguarding of the patient's sensitive data privacy, e.g., her health history, is of prime importance. Access control models are related to the privileges an entity has upon handling particular data objects. In the medical sector, contextual information which characterizes an emergency in patient's healthcare state, should be deemed when controlling access to the healthcare sensitive information by guaranteeing the most efficient treatment. Accordingly, the implementation of access control models which integrate the context concept, such as the notion of dynamically changing contextual attributes which indicate a status, is needed.

Exploiting contextual data facilitates the implementation of access control policies by taking into account the conditions of access requests evaluation. This dissertation reports that context handlers are beneficial for implementing processes of dynamic authorization which consider the patient's medical status. Additionally, the proposed system, by leveraging artificial neural networks, proceeds to the diagnosis of the patient's medical diseases, so that the medical team have access to the patients' medical records.

The additional research questions that rise complementary to the main Research Question 5 are the following:

- Which access control paradigm should be enforced so that medical professionals acquire access to private healthcare recourses?
- Which diseases are diagnosed?
- How this thesis' medical diagnosis of diseases prediction is able to assist the doctor in making the final diagnosis?

Chapter 4

4. MULTI-CONTINENT DESCRIPTIVE ANALYSIS FOR RELATION OF HEALTH METRICS AND DISEASES

A. Motivation

As reported by the World Health Organization (WHO), hypertension, obesity and smoking are among the causes of death of millions of people yearly worldwide [1]. Relevant surveys focus on continent-based data and lack a global perspective. The research objectives of this work refer to analysis of the relation of the patient's nationality, age and gender with the Diastolic Blood Pressure (DBP), Systolic Blood Pressure (SBP), and Body Mass Index (BMI) with the health diseases of hypertension, and obesity along with the unhealthy habit of smoking. Our study provides a literature review that covers all continents, analyzes reported descriptive analyses, and synthesizes them by aggregating available results. The Research Question of our work is presented in Table 4.1.

Table 4. 1 Research Objective

Identifier	Question
RQ1	How the patient's nationality, gender, age and BMI are related with BP, hypertension, and smoking habit?

The chapter's structure is as follows: In the section 4.2, a continent-based survey has been conducted which clusters single-continent research works. In the section 4.3.1., a multi-continent based descriptive analysis has been conducted which consist of four parts. The first part 4.3.1.1 of this section comprises the study of interaction between gender, age and nationality with SBP and DBP, while the second part 4.3.1.2. examines the relation of the same factors with BMI. The third part 4.3.1.3 is focused on the relation of BMI with hypertension across continents by taking into account people's age and gender, while the fourth part 4.3.1.4. studies the relation between the smoking, and the same factors. In the section 4.3.2., we present the datasets results per health metric and continent. Lastly, the section 4.3.3. summarizes the overall results of this work providing a clear outcome concerning the relation of health metrics with the patient’s lifestyle and health problems based on age, gender and continent.

B. Methods and Tools

1) Survery Methodology

This section introduces the method we applied to perform our literature review, along with the research questions and the selected search strategy. Furthermore, the process of the article selection is demonstrated, along with the considered inclusion and exclusion criteria.

Our search was conducted by considering the keywords: Age, Gender, SBP, DBP, Hypertension, BMI, Smoking and Continent. In our search we used the “~” symbol, so as not to exclude the gender’s synonyms. The search string ‘age’ AND ~gender AND ‘systolic’ AND ‘diastolic’ AND ‘blood pressure’ AND ‘hypertension’ AND ‘BMI’ AND ‘smoking’ AND ‘continent’ was applied to retrieve publications from the academic databases Google Scholar [2] and PubMed [3]. Exclusion (EC) and Inclusion Criteria (IC) of Table 4.2 were set for the selection process. The articles should meet all IC to be considered for review. Thus, a publication is taken out even at least one EC is satisfied.

Table 4. 2 Criteria for article selection.

IC-EC	Description
Inclusion criteria	
IC1	Publication date is till November 2021.
IC2	Publication represents a scientific article.
IC3	Publication is country or continent based.
Exclusion criteria	
EC4	Remove early results of the same research work.
EC5	Remove papers that exist simultaneously in Google Scholar and PubMed.

IC-EC	Description
Inclusion criteria	
EC6	Remove non peer-reviewed research works.

The search period was up to November 2021. In our research we used the two academic search engines Google Scholar and PubMed Central, with the following findings: i) Considering the first one, the literature search identified 89 references, of which 12 duplicates were removed. From the remaining 77 works, upon full-text evaluation, we identified 31 original papers, 4 review papers, 1 paper abstract, and 41 books, theses and dissertations. Then, these 41 were excluded. From the 31 original papers, 1 paper has 2 different versions, one short and one extended and as we chose the extended one, the remaining original examined papers are 30. The final exclusion criterion regarded the removal of the non-peer reviewed research works, which were 2 of the original articles, by having the 28 remaining original examined papers [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], and the 4 review papers of [32], [33], [34], [35]. Thus, 32 articles were included in this review, from Google Scholar engine. ii) From PubMed, the literature search identified 18 references, without duplicates. Considering these 18 works, upon full-text evaluation, we identified 7 original papers, from which 5 were also considered in Google Scholar [4], [9], [14], [22], [34], and 11 books, theses and dissertations. Then, these 11 works were excluded. Thus, 2 articles [36], [37] were included from PubMed. Finally, 34 papers were selected.

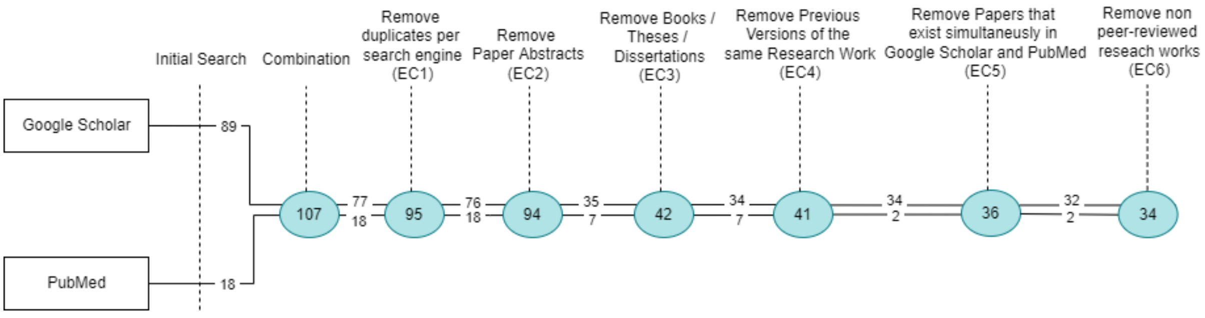

Initial Search
Combination
Remove duplicates per search engine (EC1)
Remove Paper Abstracts (EC2)
Remove Books / Theses / Dissertations (EC3)
Remove Previous Versions of the same Research Work (EC4)
Remove Papers that exist simultaneusly in Google Scholar and PubMed (EC5)
Remove non peer-reviewed reseach works (EC6)
Google Scholar
PubMed
89
18
107
77
18
95
76
18
94
35
7
42
34
7
41
34
2
36
32
2
34

Figure 4. 1 Article selection process.

Considering the regarding continents per paper we notice that there isn't any other research which considers all the continents, as in our work. We record the number of considered papers per continent as described below. a) Africa is examined in 10 papers from which: i) 9 are from Google Scholar where 7 of them are original articles [4], [5], [6], [7], [8], [9], [10] and 2 are review papers [32], [33]. ii) Accordingly, from the PubMed Central search, 1 article was considered for Africa [36]. The 10 in total papers include the regions of: Nigeria [5], [6], Africa in general [32], [33], Cameroon [4], Sudan [7], South Africa [8], Angola [9], São Tomé and Príncipe [9], Mozambique [9], Guinea Bissau [9], Cape Verde [9], Egypt [10], and Ethiopia [36]. b) Asia is examined in 17 papers from which: i) 17 are from Google Scholar, where 13 of them are original articles [9], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22] and 4 are review papers [32], [33], [34], [35], and ii) none was found from the PubMed Central search. More specifically, the 17 papers of Asia include the regions of: India [11], [14], [16], [20], [21], Asia in general [32], [33], [34], [35], Japan [13], [17], Western Asia [22], Israel [12], Taiwan [13], Singapore [13], Philippines [13], Bangladesh [15], East Timor [9], Iraq [18], and Turkey [19]. c) Europe is examined in 13 papers from which: i) 12 are from Google Scholar, where 8 of them are original articles [23], [24], [25], [26], [17], [20], [22], [27], and 4 are review papers [32], [33], [34], [35], and ii) 1 was found from the PubMed Central [37]. The 13 papers include the regions of: Europe in general [33], [17], [34], [35], Italy [25], [20], United Kingdom [24], [37], Western Europe [23], Germany [26], Romania [27], and Eastern Europe [22]. d) America is examined in 8 papers from which: i) 8 are from Google Scholar where 4 of them are original articles [28], [9], [29], [30] and 4 are review papers [32], [33], [34], [35], and ii) none was found from the PubMed Central. The 8 papers include the regions of: America in general [32], [33], [34], [35], Venezuela [29], [30], and Brazil [9], [28]. e) Oceania is examined in 1 paper which is an original article from Google Scholar [31], and none was found from the PubMed Central. This paper includes the region of Tonga [31]. Overall, we notice that surveys consider Asia and Oceania the most and least, respectively.

C. Evaluation/Validation

1) Results

To aggregate each metric M per age group i for a specific continent we used formula (1), where j represents each of the k countries per continent, S_{j_i} represents the sample size per country j and age group i, and M_{j_i} is the metric value per country j and age group i. In case where the age groups do not coincide then a statistical representative is selected per continent based on the sample size.

$$M_i = \frac{\sum_{j=1}^{k}(S_{j_i} * M_{j_i})}{\sum_{j=1}^{k}(S_{j_i})} \qquad (1)$$

a) DBP and SBP per Continent

Europe:

Existing research indicates that women have lower DBP than men till the age of 54, and that as age increases, so does the DBP. However, from the age of 65 years onwards there is a decrease in DBP. Furthermore, between the ages of 20 and 54 years men present higher SBP than women, while from the age of 55 onwards the opposite is observed.

Asia:

The data show that till the age of 74 years, women have lower DBP than men. For women, DBP increases with age up to the age of 64; above that age DBP decreases. Similarly, for men an increase is observed, but up to the age of 54 years, while from the age of 55 and above a decrease in DBP is observed. Similarly, women have lower SBP than men. In addition, there is a steady increase in SBP average values across all age groups in both genders.

America:

For America, women have lower DBP than men in the first four age groups, while in the last two groups DBP values coincide. For SBP, we observe a continuous increase in both genders except for the last age group of 80-89 years for men, where SBP remains constant. Moroever in the first four age groups, women have lower average values compared to men, while in the fifth age group they have equal SBP, and in the last age group men have lower SBP than women.

Africa:

In the Kenyan study, the sample consisted only of men, so the number of men is clearly higher than the corresponding number of women.

Globe:

The SBP and DBP values per continent of the descriptive data analysis are illustrated in the following Figure 4.2.the following Figure 4.2.

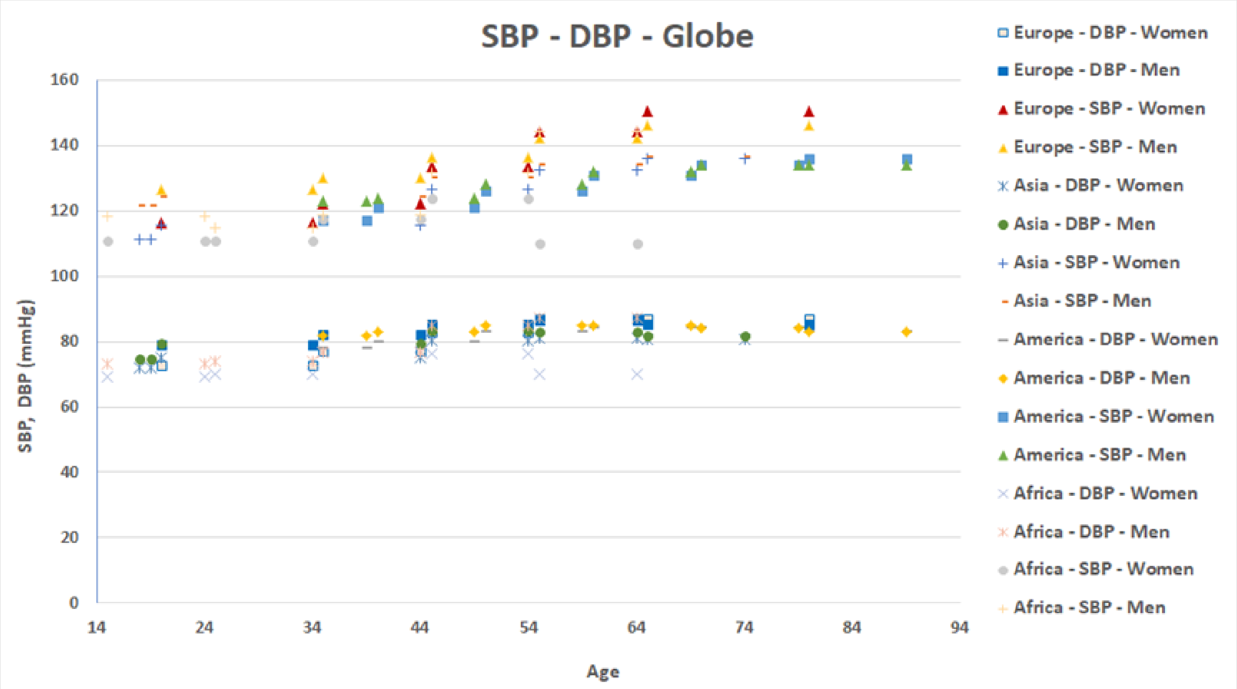


Figure 4. 2 Average SBP and DBP per continent.

b) ***Body Mass Index per Continent***

BMI is a health indicator for calculating a person's degree of obesity, which is defined as the quotient of the individual’s weight in kg divided by the square of her height in m2. In our work, an appropriate study of datasets concerning the BMI by country was conducted, depending on other parameters such as gender and age.

Europe:

For BMI, the three European surveys of Germany [38], Italy [48] and Norway [49] were considered. We notice that, as the age of women increases, the average BMI increases as well. A similar observation is recorded for men except for the higher age group, where there is a slight decrease in the corresponding measurements. Likewise, women have lower BMI than men except for the age group of 70-79 years, where the men's average BMI is lower than that of women. Another observation is that, the middle aged and older people, are overweight or obese.

Asia:

As far as the BMI is concerned, the three Asian surveys of Iran [50], Turkey [51] and India [52] were selected. The studies concluded that generally women had higher average BMI than men in all age groups. Besides, we notice an increase in BMI up to the penultimate age group, while in the latter age group there is a slight decrease. Finally, both genders are overweight except for the youngest age group.

America:

For America, only one study was found about Mexico [45]. The research showed that there exists a quite high average BMI for both genders in all the age groups up to the age of 59, and then there is a gradual decrease in BMI. In all groups, women have higher BMIs than men. Finally, both genders' values range from overweight to obese.

Africa:

For Africa, the data from the studies of Nigeria [46] and Kenya [47] were combined. The research showed that for men up to the age of 54, there is a gradual increase in BMI and then a gradual decrease. In all groups, women have higher BMIs than men. Finally, we notice that men in all age groups belong to the normal BMI, while women of age 35 or older belong to the overweight.

Oceania:

The distribution of BMI in Oceania was calculated by aggregating two surveys conducted in Australia [53]. A general increase in BMI was observed in both genders in all age groups as the values belong to the overweight. In addition, women have slightly lower BMI than men. Additionally, there is an increase in BMI as the age is increased, while it is decreased in the older ages.

Globe:

The BMI values per continent of the descriptive data analysis are illustrated in the following Figure 4.3.

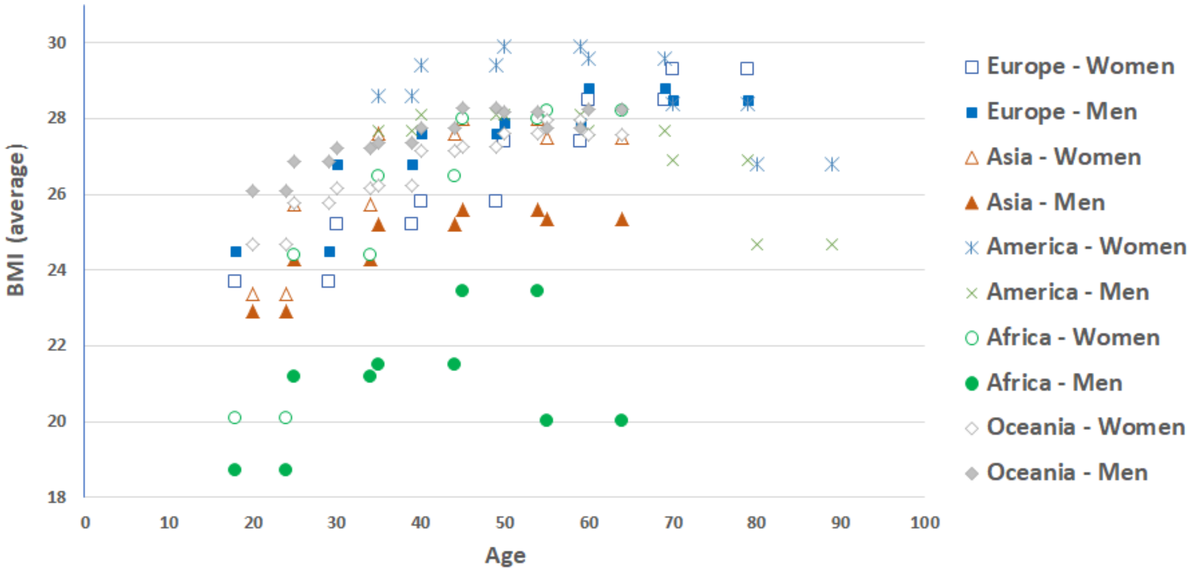


Figure 4. 3 Average BMI per continent.

c) ***Hypertension based on BMI per Continent***

In this part, the relation between high BP and BMI is studied and specifically, whether the body weight can affect the people's health by causing problems such as high BP. A study of scientific datasets regarding BMI by country is conducted, related to other parameters such as gender, age and hypertension.

Europe:

For Europe's statistical analysis, the data were collected from the studies of Germany [54], Greece [55], and Portugal [56]. The hypertension rates are quite high, over 30%, while the highest rate is found in obese.

Asia:

For the continent of Asia, all the data from the three studies of Iran [57], Iraq [58], and Pakistan [59] were combined. The highest percentages of people with hypertension are either overweight or obese.

America:

For the aggregative statistical analysis of America, both surveys of Mexico [60] and Brazil [61] were considered. In the first BMI category, the percentage of hypertension is low compared to the other two categories. In the obese, the hypertension rate amounts to 45.19%.

Africa:

All three medical studies of Egypt [62], Kenya [63], and Sudan [64] were combined for the aggregative statistical analysis of Africa. The highest rate of hypertension is found in obese people. However, even from the first BMI category the hypertension rate is quite high.

Globe:

The hypertension rate per continent of the descriptive data analysis is illustrated in the following Figure 4.4.

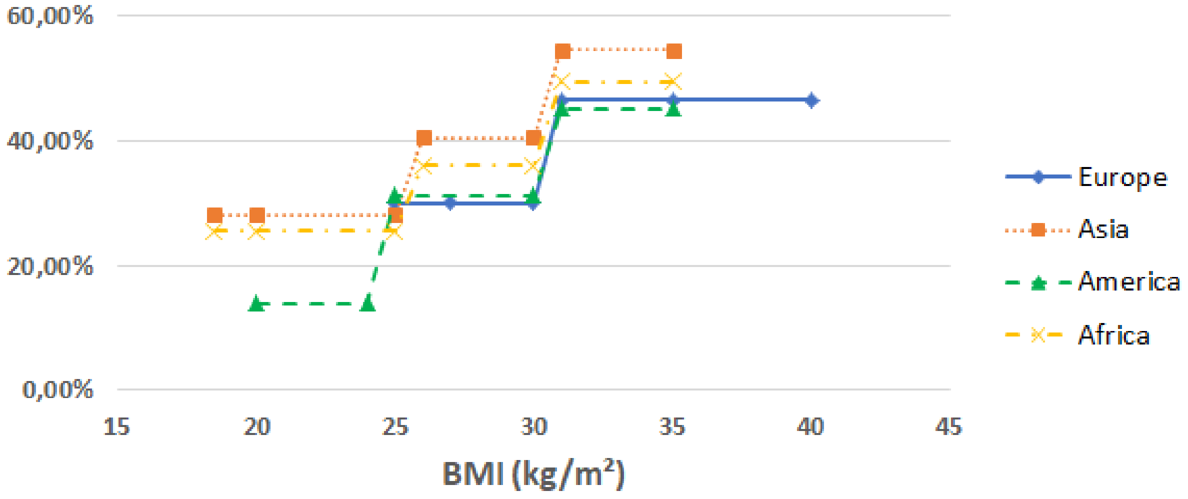


Figure 4. 4 Average Hypertension rate per continent.

d) *Smoking Habits based on BMI per Continent*

We reviewed research concerning smoking behavior which causes serious diseases related to BMI.

Europe:

For the relation between BMI and smoking, in order to illustrate an aggregative result from the two conducted surveys, of Portugal [65] and United Kingdom [66], and as the corresponding partial sizes per each BMI group were not defined explicitly, and as the ranges of BMI groups didn't match across surveys, we picked that from [66], because its sample size outnumbered [65]. For smokers, obese rate is lower than the categories of overweight, normal and underweight combined. As for the former smokers, the percentage of the obese is higher than that of overweight, normal and underweight combined.

Asia:

For the relation between BMI and smoking, the surveys in China [67], and Iran [68] were found, and as the BMI categories didn't match across surveys, we picked that from China, because its sample size outnumbered that of Iran. Firstly, the percentage of obese smokers is higher than that of overweight. Besides, the female non-smokers outnumber the male ones in all BMI categories.

America:

For the relation between BMI and smoking, in order to illustrate an aggregative result from the surveys of Mexico [69] and Brazil [70], and as the smoker categories per each BMI group didn't match across surveys, we picked that from Brazil, because the size of its sample outnumbered that from [69]. The overweight smokers' rate is higher than that of obese. In addition, the non-smokers percentage with normal BMI is higher than that of overweight or obese.

Africa:

For the relation between BMI and smoking, in order to illustrate an aggregative result from the conducted African surveys in Sudan [71], Tanzania [72], and Kenya [73], and as the corresponding smoker categories along with BMI groups didn't match across surveys, we picked that from Tanzania, because the size of its sample outnumbered the others. For smokers, the rate of the normal weight or underweight is higher than that of overweight or obese. Likewise, the smokers' rate for all BMIs is extremely low.

Globe:

The smoking rate per continent is illustrated in the following Figure 4.5.

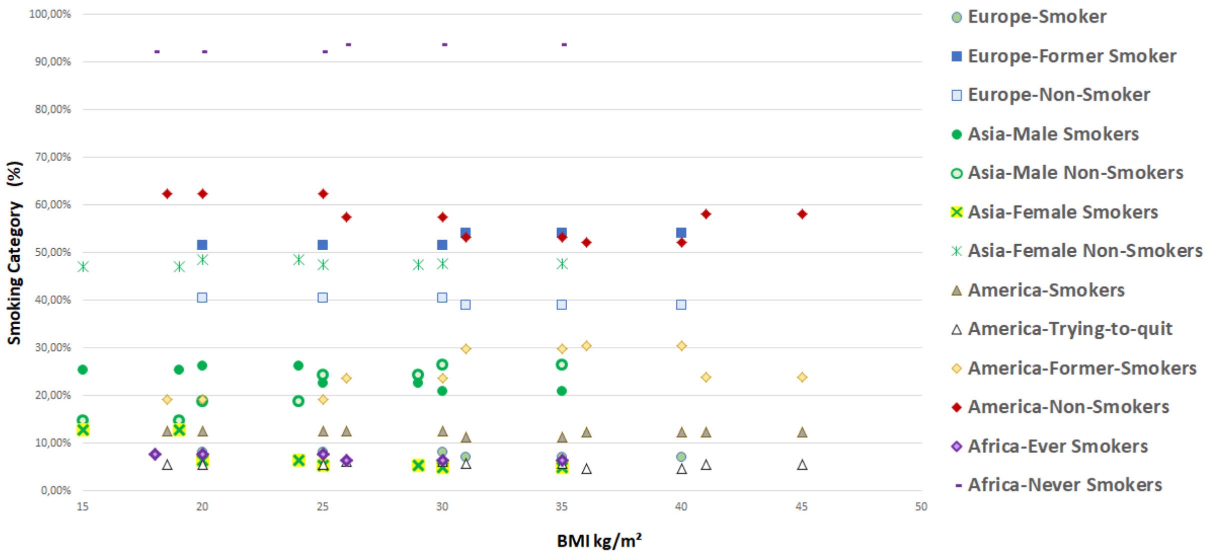
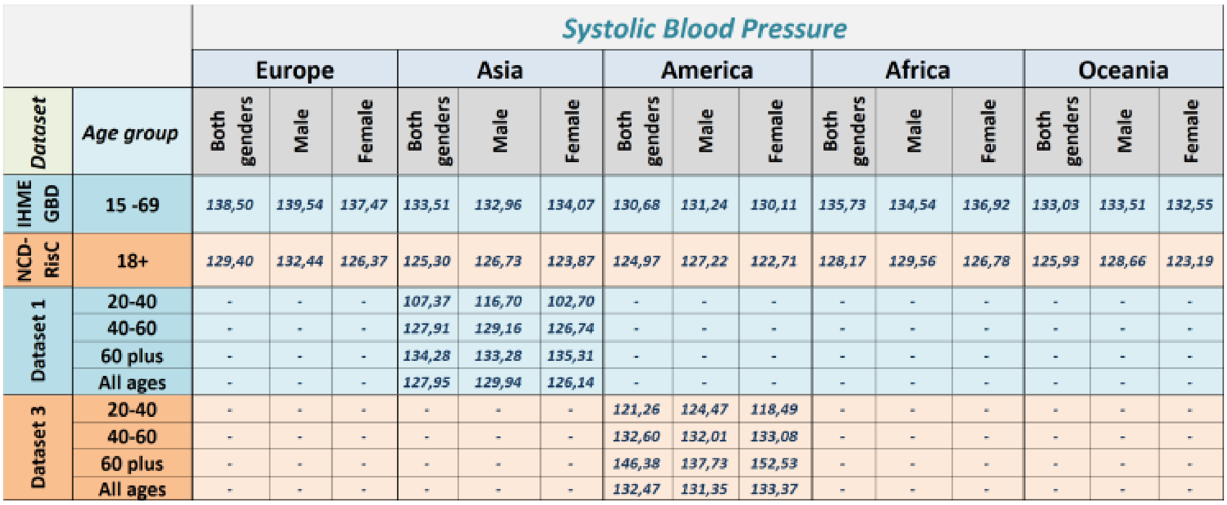


Figure 4. 5 Average Smoking rate per continent.

2) Validation

a) SBP per Continent

For SBP (Figure 4.6), the highest values are reported in Europe, and the lowest in America [78], [79]. In Asia and America, as the age increases, so does the SBP [74], [76]. Men have higher SBP than women in Europe, America, and Oceania [78], while in Asia and Africa women have higher SBP than men. Furthermore, men have higher SBP than women in all continents [79]. In Asia and America, men have higher SBP than women till middle age, and then women have higher SBP than men.

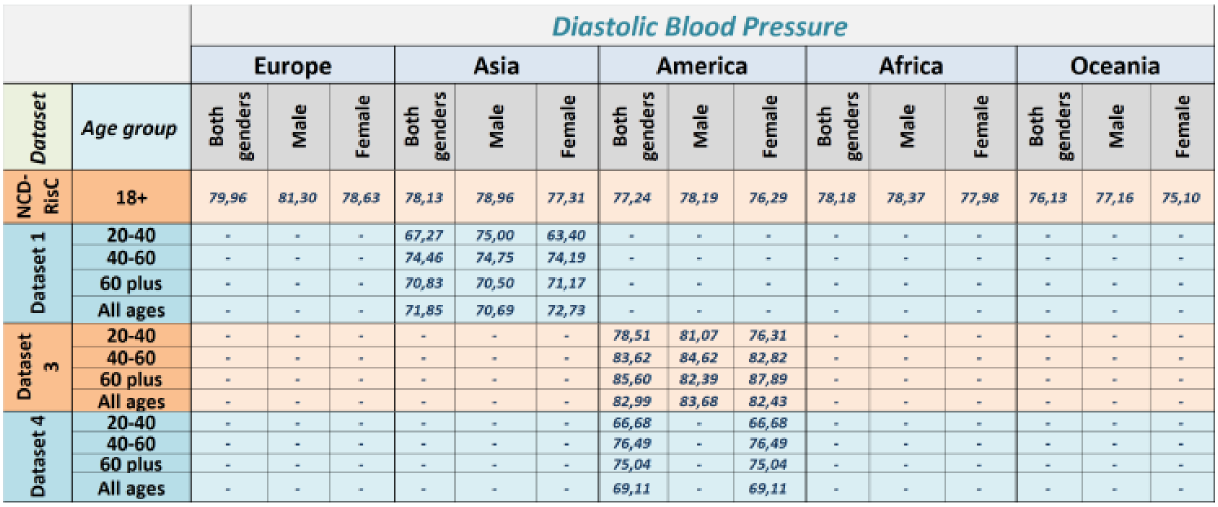


		Systolic Blood Pressure														
		Europe			Asia			America			Africa			Oceania		
Dataset	Age group	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female
IHME GBD	15 -69	138,50	139,54	137,47	133,51	132,96	134,07	130,68	131,24	130,11	135,73	134,54	136,92	133,03	133,51	132,55
NCD-RisC	18+	129,40	132,44	126,37	125,30	126,73	123,87	124,97	127,22	122,71	128,17	129,56	126,78	125,93	128,66	123,19
Dataset 1	20-40	-	-	-	107,37	116,70	102,70	-	-	-	-	-	-	-	-	-
	40-60	-	-	-	127,91	129,16	126,74	-	-	-	-	-	-	-	-	-
	60 plus	-	-	-	134,28	133,28	135,31	-	-	-	-	-	-	-	-	-
	All ages	-	-	-	127,95	129,94	126,14	-	-	-	-	-	-	-	-	-
Dataset 3	20-40	-	-	-	-	-	-	121,26	124,47	118,49	-	-	-	-	-	-
	40-60	-	-	-	-	-	-	132,60	132,01	133,08	-	-	-	-	-	-
	60 plus	-	-	-	-	-	-	146,38	137,73	152,53	-	-	-	-	-	-
	All ages	-	-	-	-	-	-	132,47	131,35	133,37	-	-	-	-	-	-

Figure 4. 6 Average SBP per continent.

b) ***DBP per Continent***

The highest DBP values are reported in Europe and the lowest in Oceania (Figure 4.7) [79]. Asia [74] and America [77] exhibit lower values in comparison with the corresponding values of dataset [79] and as the age increases, so does the SBP. Furthermore, in Asia women have lower DBP than men till the middle aged [74], and then women have higher DBP than men. Contrarily, in America men have higher DBP than women in all age groups [76].

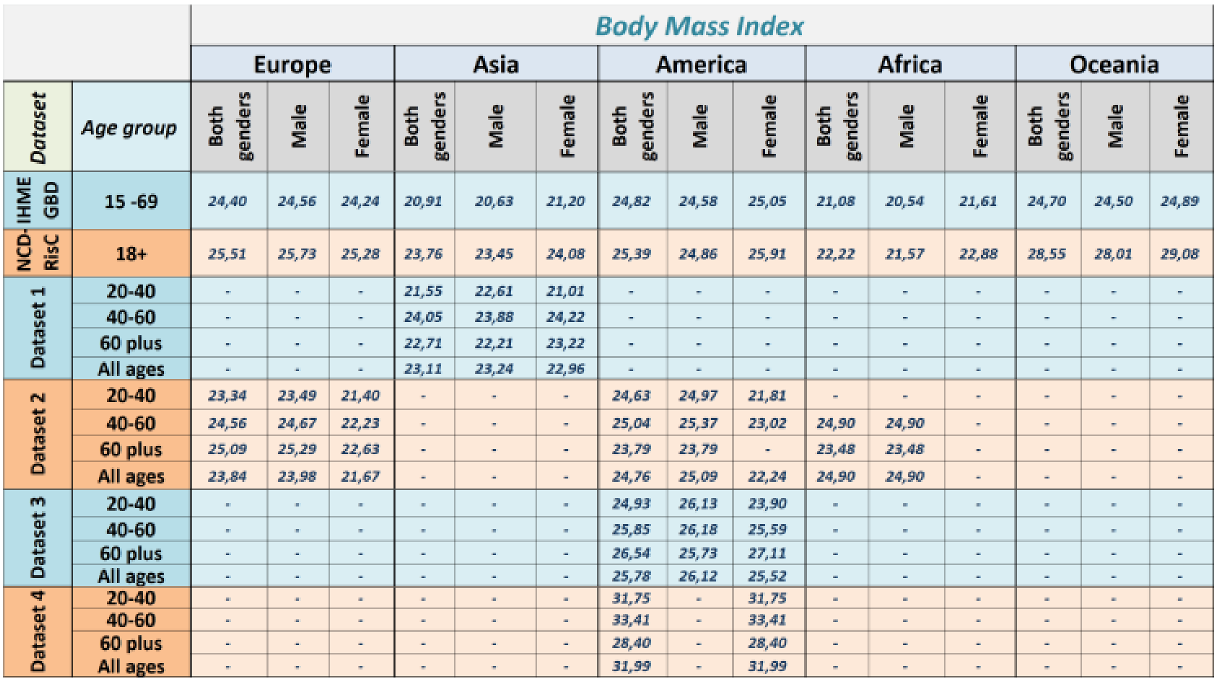


		Diastolic Blood Pressure														
		Europe			Asia			America			Africa			Oceania		
Dataset	*Age group*	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female
NCD-RisC	18+	*79,96*	*81,30*	*78,63*	*78,13*	*78,96*	*77,31*	*77,24*	*78,19*	*76,29*	*78,18*	*78,37*	*77,98*	*76,13*	*77,16*	*75,10*
Dataset 1	20-40	-	-	-	*67,27*	*75,00*	*63,40*	-	-	-	-	-	-	-	-	-
	40-60	-	-	-	*74,46*	*74,75*	*74,19*	-	-	-	-	-	-	-	-	-
	60 plus	-	-	-	*70,83*	*70,50*	*71,17*	-	-	-	-	-	-	-	-	-
	All ages	-	-	-	*71,85*	*70,69*	*72,73*	-	-	-	-	-	-	-	-	-
Dataset 3	20-40	-	-	-	-	-	-	*78,51*	*81,07*	*76,31*	-	-	-	-	-	-
	40-60	-	-	-	-	-	-	*83,62*	*84,62*	*82,82*	-	-	-	-	-	-
	60 plus	-	-	-	-	-	-	*85,60*	*82,39*	*87,89*	-	-	-	-	-	-
	All ages	-	-	-	-	-	-	*82,99*	*83,68*	*82,43*	-	-	-	-	-	-
Dataset 4	20-40	-	-	-	-	-	-	*66,68*	-	*66,68*	-	-	-	-	-	-
	40-60	-	-	-	-	-	-	*76,49*	-	*76,49*	-	-	-	-	-	-
	60 plus	-	-	-	-	-	-	*75,04*	-	*75,04*	-	-	-	-	-	-
	All ages	-	-	-	-	-	-	*69,11*	-	*69,11*	-	-	-	-	-	-

Figure 4. 7 Average DBP per continent.

c) ***BMI per Continent***

The highest average BMI values are reported in America and Oceania [78], [80], while the minimum values are reported in Asia and America (Figure 4.8). In Asia and America, women have lower BMI values than men till the middle aged [74], [76], while in the older ages women have higher BMI than men. Moreover, in Europe and America, men have higher BMI than women in all age groups [75].

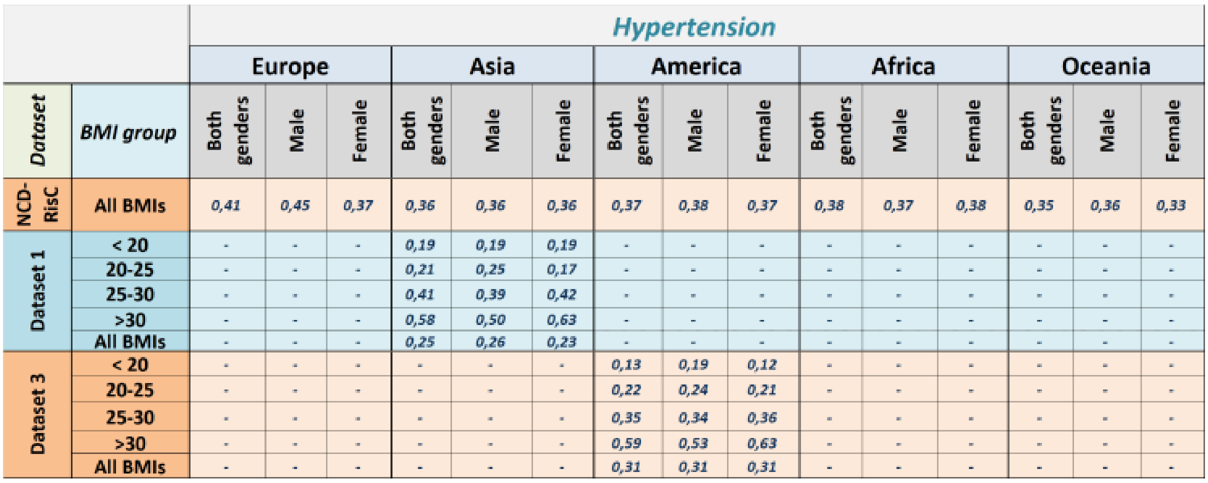


		Body Mass Index														
		Europe			Asia			America			Africa			Oceania		
Dataset	*Age group*	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female
IHME GBD	15 -69	24,40	24,56	24,24	20,91	20,63	21,20	24,82	24,58	25,05	21,08	20,54	21,61	24,70	24,50	24,89
NCD-RisC	18+	25,51	25,73	25,28	23,76	23,45	24,08	25,39	24,86	25,91	22,22	21,57	22,88	28,55	28,01	29,08
Dataset 1	20-40	-	-	-	21,55	22,61	21,01	-	-	-	-	-	-	-	-	-
	40-60	-	-	-	24,05	23,88	24,22	-	-	-	-	-	-	-	-	-
	60 plus	-	-	-	22,71	22,21	23,22	-	-	-	-	-	-	-	-	-
	All ages	-	-	-	23,11	23,24	22,96	-	-	-	-	-	-	-	-	-
Dataset 2	20-40	23,34	23,49	21,40	-	-	-	24,63	24,97	21,81	-	-	-	-	-	-
	40-60	24,56	24,67	22,23	-	-	-	25,04	25,37	23,02	24,90	24,90	-	-	-	-
	60 plus	25,09	25,29	22,63	-	-	-	23,79	23,79	-	23,48	23,48	-	-	-	-
	All ages	23,84	23,98	21,67	-	-	-	24,76	25,09	22,24	24,90	24,90	-	-	-	-
Dataset 3	20-40	-	-	-	-	-	-	24,93	26,13	23,90	-	-	-	-	-	-
	40-60	-	-	-	-	-	-	25,85	26,18	25,59	-	-	-	-	-	-
	60 plus	-	-	-	-	-	-	26,54	25,73	27,11	-	-	-	-	-	-
	All ages	-	-	-	-	-	-	25,78	26,12	25,52	-	-	-	-	-	-
Dataset 4	20-40	-	-	-	-	-	-	31,75	-	31,75	-	-	-	-	-	-
	40-60	-	-	-	-	-	-	33,41	-	33,41	-	-	-	-	-	-
	60 plus	-	-	-	-	-	-	28,40	-	28,40	-	-	-	-	-	-
	All ages	-	-	-	-	-	-	31,99	-	31,99	-	-	-	-	-	-

Figure 4. 8 Average BMI per continent.

d) Hypertension based on BMI per Continent

Regarding the hypertension rate per continent (Figure 4.9), the highest average hypertension rate is reported in Europe and the lowest in Oceania [81]. In Asia and America, men have higher rates of hypertension than women till the normal BMI, while in the overweight categories women have higher hypertension rates than men [74], [76].

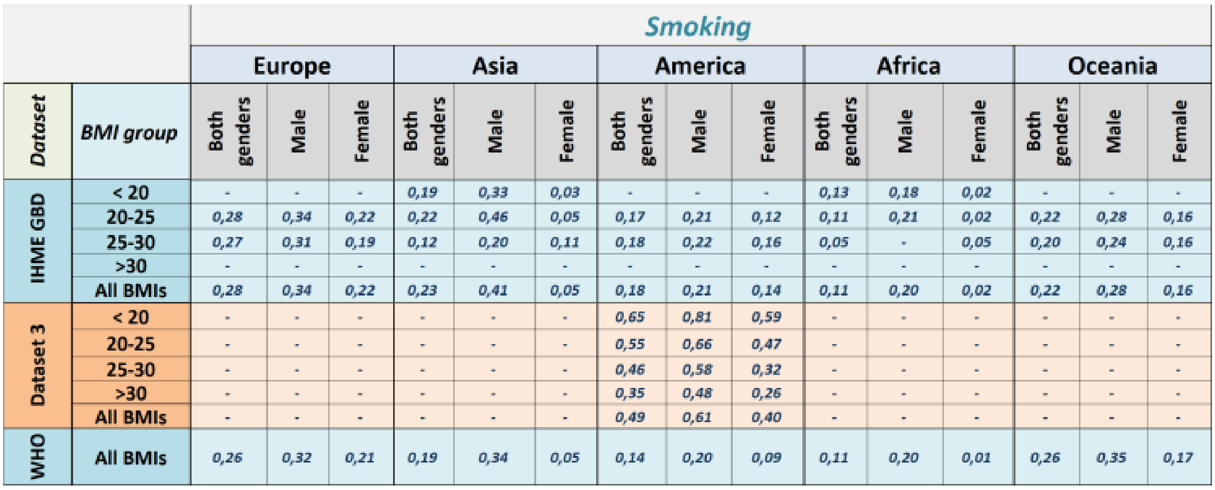


		Hypertension														
		Europe			Asia			America			Africa			Oceania		
Dataset	*BMI group*	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female
NCD-RisC	All BMIs	0,41	0,45	0,37	0,36	0,36	0,36	0,37	0,38	0,37	0,38	0,37	0,38	0,35	0,36	0,33
Dataset 1	< 20	-	-	-	0,19	0,19	0,19	-	-	-	-	-	-	-	-	-
	20-25	-	-	-	0,21	0,25	0,17	-	-	-	-	-	-	-	-	-
	25-30	-	-	-	0,41	0,39	0,42	-	-	-	-	-	-	-	-	-
	>30	-	-	-	0,58	0,50	0,63	-	-	-	-	-	-	-	-	-
	All BMIs	-	-	-	0,25	0,26	0,23	-	-	-	-	-	-	-	-	-
Dataset 3	< 20	-	-	-	-	-	-	0,13	0,19	0,12	-	-	-	-	-	-
	20-25	-	-	-	-	-	-	0,22	0,24	0,21	-	-	-	-	-	-
	25-30	-	-	-	-	-	-	0,35	0,34	0,36	-	-	-	-	-	-
	>30	-	-	-	-	-	-	0,59	0,53	0,63	-	-	-	-	-	-
	All BMIs	-	-	-	-	-	-	0,31	0,31	0,31	-	-	-	-	-	-

Figure 4. 9 Average hypertension rate per continent.

e) ***Smoking Habits based on BMI per Continent***

Regarding the average smoking rate (Figure 4.10), the highest rate is reported in Europe and the lowest in Africa [78], [82]. In all continents, men have higher smoking rate than women [78], [76], [82]. As the BMI increases the smoking rate decreases in Europe and Oceania, while the smoking rate increases in America [78]. In Africa, the smoking rate decreases from the normal weight and up, while in Asia as the BMI increases, the smoking rate decreases in men and increases in women [78]. Furthermore in America, as the BMI increases, the smoking rate decreases [76].



		Smoking														
		Europe			Asia			America			Africa			Oceania		
Dataset	*BMI group*	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female	Both genders	Male	Female
IHME GBD	< 20	-	-	-	0,19	0,33	0,03	-	-	-	0,13	0,18	0,02	-	-	-
	20-25	0,28	0,34	0,22	0,22	0,46	0,05	0,17	0,21	0,12	0,11	0,21	0,02	0,22	0,28	0,16
	25-30	0,27	0,31	0,19	0,12	0,20	0,11	0,18	0,22	0,16	0,05	-	0,05	0,20	0,24	0,16
	>30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	All BMIs	0,28	0,34	0,22	0,23	0,41	0,05	0,18	0,21	0,14	0,11	0,20	0,02	0,22	0,28	0,16
Dataset 3	< 20	-	-	-	-	-	-	0,65	0,81	0,59	-	-	-	-	-	-
	20-25	-	-	-	-	-	-	0,55	0,66	0,47	-	-	-	-	-	-
	25-30	-	-	-	-	-	-	0,46	0,58	0,32	-	-	-	-	-	-
	>30	-	-	-	-	-	-	0,35	0,48	0,26	-	-	-	-	-	-
	All BMIs	-	-	-	-	-	-	0,49	0,61	0,40	-	-	-	-	-	-
WHO	All BMIs	0,26	0,32	0,21	0,19	0,34	0,05	0,14	0,20	0,09	0,11	0,20	0,01	0,26	0,35	0,17

Figure 4. 10 Average smoking rate per continent.

3) ***Discussion***

a) ***Relations between SBP and DBP with age and gender per continent***

Women from Asia and Africa have lower SBP than women from other continents, independently of their age. In Europe and America, as the age increases up to the middle-aged, men have higher SBP than women, and then men have lower SBP than women. In addition, in Europe and Asia, as the age increases so does the SBP. Contrarily, in Africa, the SBP increases up to the age of 54 and afterwards it decreases. A particular case is observed in America where SBP increases proportionally with the age for women, while for men older than 80 years it remains at the same level. By comparing the SBP results of sections 4.3.1. and 4.3.2., we deduce the following: In both our review and the real dataset based approach we notice in Europe the highest SBP, while the lowest SBP is reported in Africa and America respectively. The dataset [79] confirms our review that men’s SBP in Asia and

Africa is higher than women's in all age groups, while dataset [78] isn't in accordance with that finding. In both our review and dataset [76] for America, women have lower SBP than men till the middle aged, while in the older ages women have higher SBP than men.

For DBP the following observations are made: Firstly, for Africa, women's DBP is lower than that of men for all ages, while in America, Europe and Asia women's DBP is lower than that of men till the middle-aged. Moreover, in all continents, as the age increases, so does the DBP till the middle aged, and then it decreases. Additionally, the turning point of age is different per continent, by having the lowest in Africa for women, whereas for men the DBP always increases per age group, while in Europe and Asia the average DBP increases till the middle age. The highest turning point of age up to which the DBP increases, is in America. By comparing the DBP results of sections 4.3.1. and 4.3.2., we deduce the following: In both our review and dataset [79], we notice that men have higher DBP than women. In addition, both our review and datasets [74], [76] are in accordance that women have lower values than men till the middle aged, while in the older ages women have higher DBP than men in Asia and America. Whilst in our review the highest DBP is reported in America and Asia for men and women respectively, in dataset [79] the highest DBP is reported in Europe. Likewise, in our review the lowest DBP is reported in Africa, while in dataset [79] the lowest DBP is reported in Oceania.

b) ***Relations between BMI and age and gender per continent***

Based on our section 4.3.1. review the following results were conducted: Firstly, in Oceania women have lower BMI than men for all ages, while in America, Asia and Africa women have higher BMI than men for all ages. An ad hock case is considered in Europe where women have lower BMI than men till 69 years, and then women have higher BMI than men. Secondly, the BMI increases in Asia, America, and Oceania, only for women, till the middle ages and it decreases afterwards. On the contrary, in Europe and Africa the BMI increases proportionally with the age, but especially for men it decreases in higher ages. Thirdly, in America and Oceania both genders are overweight or obese in all age groups, while in Asia and Europe they are characterized as such for ages older than 34 or 29, and 24 or 39 years for men and women respectively. On the contrary, in Africa, women are overweight from the age of 35, while men maintain the normal weight throughout all ages. By comparing the BMI results of sections 4.3.1. and 6.3.2., we deduce the following: Whilst, both in our review and dataset [80], the highest BMI is reported in Oceania, the dataset [78] reports the highest BMI in America. As for the minimum BMI, in our review it is reported in Africa in both genders while in Asia and America it is reported based on datasets [78] and [80].

c) ***Relations between Hypertension and BMI per continent***

We notice that as the BMI increases so does the hypertension rates. Secondly, the smallest hypertension rate corresponds to the normal weight for Asia, America and Africa. Thirdly, the higher hypertension rates are spotted in the obese for Europe, Asia, America and Africa. Overall, the highest hypertension rates for every BMI category are spotted in Asia, while the lowest hypertension rate for the obese and the normal BMI category is spotted in America, and for the overweight is found in Europe. By comparing the hypertension rates of sections 4.3.1. and 4.3.2., we deduce the following: Firstly, in both our review and datasets [74], [76], as the BMI increases, so does the hypertension rate. Based on dataset [81] and our review, the highest rate of hypertension is reported in Europe and Asia respectively. Moreover, the minimum hypertension rate is reported in America and Oceania based on our review and dataset [81].

d) ***Relations between Smoking habit and BMI per continent***

We observe that the rate which corresponds to overweight smokers is higher than that of obese in Asia and America. Additionally, the rate of smokers for the underweight or normal category is higher than that of overweight or obese in Asia and Africa. On the contrary in America and Europe, the rate of underweight or normal BMI is almost at the same level as the corresponding rate of overweight or obese. Asia is the only continent where there are available data for both genders. In this research we also notice that the female smokers’ rate is lower than that of male smokers in all BMI categories. In addition, the highest rate of female smokers belongs to the underweight, while that of male belongs to the normal category. By comparing the smoking rates based on BMI of sections 4.3.1. and 4.3.2., we deduce the following: Firstly, in Asia, in both literature review and the datasets approach, the smoking rate of the normal category is higher than that of overweight in dataset [78]. In addition, in both literature review and dataset [78] the smoking rate of America is in the same level for both the normal and the overweight, while according to dataset [76] as the BMI increases, the smoking rate decreases. Based on datasets [78], [82], the highest and lowest smoking rates are reported in Europe and Africa, while based on our review the highest and lowest rates are reported in Asia and Europe.

Chapter 5

5. Personalized Context Handlers for Diagnostic Access Control

A. Motivation

Controlling access to healthcare data is of great importance because the preservation of the privacy of the patient's information, such as his medical history, is a legal and societal requirement. Access control models deal with the rights a subject has upon performing some operations (such as read, write, etc.) on specific data objects. Prominent access control models that are based on the identity of a user include the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) or the Role-Based Access Control (RBAC) [1]. Apart from these models which are static, a dynamic model has been introduced, the Attribute-Based Access Control (ABAC) [2]. In ABAC, there are no static lists of permissions that associate subjects with objects, but instead there are 'snapshots' of such associations that can be generated and dynamically change based on the current context.

In healthcare, contextual information, such as information indicating an emergency or criticality in patient's medical condition, should be taken into account when granting access to her medical data in order to ensure the best possible medical response. Hence, there is a need to apply access control protocols with capabilities that incorporate the notion of context, i.e., the consideration of dynamically-changing contextual attributes that may characterize a situation. Context can be perceived as any information that can be used to characterize the situation of an entity (person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves [3]. In fact, the use of contextual information makes it possible to apply access control policies by considering the circumstances under which access requests should be evaluated. For example, in acute care cases, an emergency doctor wants to access parts of the patient's healthcare and medical information to cope best with an acute care situation. Contextual attributes values can be acquired for example from IoT sensors. Consider, for example, a smartwatch with blood pressure measurement capabilities. Still, contextual attributes are often too low-level and cannot be used to characterise a situation of used in isolation. Contrary, by processing contextual attributes, context can be uplifted: low-level contextual attributes can be used to detect higher-level context that characterises a situation.

We argue that context handlers can be valuable for enforcing dynamic authorization processes that take into the criticality of a certain health emergency before yielding an access control decision. This is quite important, since in emergency situations paramedics and first response teams should have immediate access to patients' health records although they could not have been considered in the defined policies at design time.

Employing personalized context handlers for emergency access control has the following advantages. First, access control is based on both objective patients' metrics and subjective expert knowledge. The latter in particular is easy to elicit and represent using a fuzzy logic approach, in which rules connect the fuzzy variables of each health metric with the criticality, which states the level of patient's health risk. Second, except from the patient's health metrics, additional personal information are taken under consideration such as the patient's age. Third, access control is evaluated based on a fuzzy rule-based inference process, which inferences the criticality risk of patients based on the fuzzy rules.

The limitations of our approach include the fact that only the age and a limited set of health metrics are taken into consideration in the fuzzy rules. The corresponding rules are reported as sound by medical experts; nevertheless, the incorporation of additional metrics would improve the completeness of the rules. Additional metrics include gender, BMI, education level, existence of chronic diseases, even lifestyle contextual information such as smoking or drinking habits.

In comparison to RBAC implementations of Break-the-Glass access control, in which the healthcare emergency medical team has predefined access in emergency situations because of their role, the proposed ABAC implementation leverages personalized context which takes into account patient's characteristics and current health metrics. It is worth highlighting that in our scenario, the break-the-glass access decision is made by ER medical personnel. Specifically, the personalized context handler's result (permit or deny) is sent to the ER team along with the patient's current health metrics and age. By having at their disposal both the system's access result and the patient's contextual information, the ER team can make an informed final decision.

Additionally, it is worth mentioning that the context handlers implemented in this work, where access policies are specified by directly using contextual information (e.g. the patient's age), manage adequately the dynamic attribute values. On the contrary, CapBAC lacks dynamicity as the capability token is composed by the permissions that a subject has upon an object.

The research objectives of our work are threefold: First, to develop a method that can be used by medical experts to characterise critical, emergency situations requiring extraordinary access to healthcare data based on dynamically changing contextual attributes. Second, to apply the ABAC paradigm and its context-handling capabilities in order to implement the proposed context-uplifting method for characterising situations. Third, to enable personalisation in the way contextual attributes are used to characterise situations for different users.

B. Tools and Methods

1) Methods

a) A fuzzy-logic based approach for context handling

We propose and develop advanced context handlers that are able to cope with the inherent ambiguity that exists in interpreting contextual information for detecting potentially critical health-related situations. In such situations the ambiguity exists in the frame of personalisation aspects; e.g., elevated heart rate can be considered critical for a certain patient only if the age, the current activity or even his medical conditions are considered.

As healthcare information can be considered subjective or fuzzy, healthcare applications have been improved by leveraging fuzzy logic-based approaches. Computer-aided diagnosis in medicine is considered one of the most applicable sectors of fuzzy logic [4]. Fuzzy logic has been used in this context to support medical image or biomedical signal analysis, segmentation, and feature extraction/selection. Our approach utilizes fuzzy logic to realize inferencing in relation to context handlers.

Fuzzy logic is intended to model logical reasoning with vague or imprecise statements and emerged in the context of the theory of fuzzy sets, introduced by Zadeh [5], [6]. It is based on the observation that people make decisions based on imprecise and non-numerical information. Fuzzy models or sets are mathematical means of representing vagueness and imprecise information. These models have the capability of making inferences by utilising information that is vague and lack certainty. In healthcare, it is often the case that there exists ambiguity in the definition as well as in the evaluation of attributes. Fuzzy logic provides the opportunity for modelling attributes and dependencies that are inherently imprecisely defined. Moreover, fuzzy logic models imprecise dependencies based on natural language. This simplifies the decision knowledge elicitation process since it is possible to interview medical experts in their own terms, i.e., they can take the rules that they already use in the decision process and model them as fuzzy rules to work within an inference system.

b) *Criticality Assessment using Fuzzy Context Handlers*

Contextual attributes are used for the definition of access control policy rules. We interviewed experts from the healthcare domain, including information technology officers and medical personnel from healthcare institutions (public agencies, hospitals, emergency services, etc.). Experts were asked to create access control policy rules in a structured way that allowed us to consolidate important contextual attributes that should be considered in our ABAC approach. Table 5.1 provides an example of an access policy provided by respondents.

Table 5. 1 Access control policy example.

Condition				Action
Requestor	Action	Resource	Context Conditions	
Emergency Doctor	Modify	Exam Results	Location IN Premises AND BETWEEN Mon.–Sat. AND Curr. Time BETWEEN 06:00 – 22:00 AND Systolic or Diastolic Blood Pressure = Low	Permit

The template uses the 'IF (Requestor Action Resource) AND (context conditions) THEN permit/deny' rule pattern. For instance, we can define the rule: 'If a doctor attempts to modify examination results, while his location is in premises (of the hospital), then access is permitted'. Context conditions can be Boolean expressions of simple conditions or other composite conditions. In several cases the simple conditions are constraints on context attributes (e.g., Location IN premises). Simple context conditions can be combined in order to form complex context conditions, using the standard AND, OR, NOT operators. A complete list of the contextual attributes, represented in a context model, is described in (c2), as analytically described in chapter 12.

The criticality assessment of a patient's condition is made using a rule-based approach. Note, that since many of the contextual variables, appearing in (c2) as analytically described in chapter 12, are evaluated by experts using linguistic terms, such as 'if blood pressure is high', our approach adopts the following fuzzy inferencing process:

1. *Fuzzification of variables*. For each variable appearing in the policy rules which is evaluated by experts using linguistic terms, such as blood pressure and heart rate, the fuzzy sets are defined.

2. *Calculation of Implication function*. Each fuzzy 'if-then' rule is a fuzzy relation R(x,y) which is called an implication relation. The implication relation is defined as follows:

$$R(x, y) \equiv \varphi(\, uA(x), uB(y)\,) \qquad (1)$$

where ϕ is the implication operator. In our case, we use the implication operator of Larsen Product:

$$\varphi_p\colon u_A(x) \;\bullet\; u_B(y) \qquad (2)$$

3. *Composition of fuzzy Relations*. The Generalised Modus Ponens (GMP) method (○) is applied in every rule "if x is A then y is B", to obtain B' for a given A' using the relation (3):

$$B' = A' o R(x, y) \qquad (3)$$

4. *Composition of Results*. Using the Sum method, the partial results obtained in step 3 are composed.

5. *Defuzzification of result.* Composite results obtained in step 4 are defuzzyfied using the Cendroid defuzzification method in order to produce a crisp value.

Note that alternative fuzzy operators may be used in the various steps of the fuzzy inferencing process. For example, the Mandani Min operator ($\varphi_c\colon u_A(x) \wedge u_B(y)$) may be used in step 2, the Max method in step 4, and the average-of-maxima in step 5.

c) <u>Example</u>

Example with non-complex fuzzy rules

Let us consider an example in which our approach is applied to estimate the overall critical situation of a patient, so as to decide about granting emergency access to an EHR system. A fuzzy context handler was developed based on the following fuzzy rules which map the fuzzy variables Systolic Blood Pressure (m1) and Diastolic Blood Pressure (m2) with fuzzy values 'Low', 'Normal', 'Elevated', and 'High', and the fuzzy variable Heart Rate (m3) with fuzzy values 'Low', 'Medium', and 'High', with the output fuzzy variable Criticality, with values 'Low', 'Medium', and 'High':

K1S: If Systolic Blood Pressure is Low then Criticality is High

K2S: If Systolic Blood Pressure is Normal then Criticality is Low

K3S: If Systolic Blood Pressure is Elevated then Criticality is Medium

K4S: If Systolic Blood Pressure is High then Criticality is High

K1D: If Diastolic Blood Pressure is Low then Criticality is High

K2D: If Diastolic Blood Pressure is Normal then Criticality is Low

K3D: If Diastolic Blood Pressure is Elevated then Criticality is Medium

K4D: If Diastolic Blood Pressure is High then Criticality is High

K1HR: If Heart Rate is Low then Criticality is High

K2HR: If Heart Rate is Medium then Criticality is Low

K3HR: If Heart Rate is High then Criticality is High

The corresponding fuzzy sets of each fuzzy variable appearing in the rules are defined according to the American Heart Association (AHA) for blood pressure [7] and for heart rate [8], see Tables 5.2 and 5.3.

Table 5. 2 Systolic and Diastolic Blood Pressure Ranges.

Blood Pressure Categories	Low	Normal	Elevated	High
SBP	60 - 95	85 – 125	115 - 145	135 - 200
DBP	50 - 63	57 – 83	77 - 93	87 - 130

Table 5. 3 Heart Rate Ranges.

	Low	Normal	High
HR	40 - 60	50 – 105	95 - 190

We quantify criticality in the form of the fuzzy sets uC/C shown next:

$$C_{\mathrm{LOW}} = \{1/0, 0{,}8/20, 0.5/50, 0.2/80, 0/100\}$$

$$C_{\mathrm{MEDIUM}} = \{0/0, 0.4/20, 1/50, 0.4/80, 0/100\}$$

$$C_{HIGH} = \{0/0, 0.2/20, 0.5/50, 0.8/80, 1/100\}$$

We calculate $\max(\mathrm{criticality}(\mathrm{m_i}))$, which is the maximum value of criticality(mi) of health metric mi and for all values of mi in the dataset. For systolic blood pressure for example, the distribution of criticality(m1) is depicted in Figure 5.1. Notice that $\max(\mathrm{criticality}(\mathrm{m_1})) = 67$. Similarly, we infer that $\max(\mathrm{criticality}(\mathrm{m_2})) = 67$ and $\max(\mathrm{criticality}(\mathrm{m_3})) = 67$.

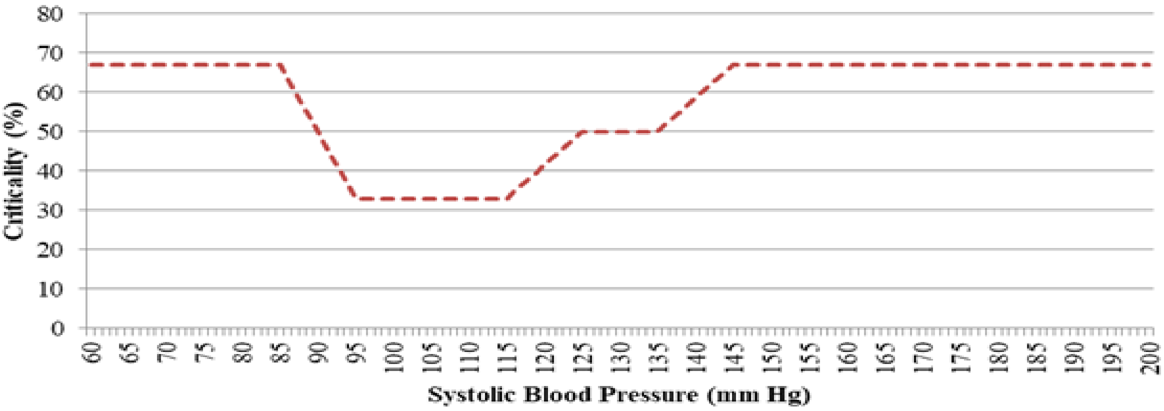


Figure 5. 1 Distribution of criticality(m_1), Systolic Blood Pressure.

Let us assume that a particular patient has the following health status metrics, which are gauged by the emergency dispatch personnel: $\mathrm{SBP_1} = 110\ \mathrm{mmHg}$, $\mathrm{DBP_2} = 72\ \mathrm{mmHg}$, $\mathrm{HR_3} = 63\ \mathrm{bpm}$. Using the inference process described in section 5.2, we calculate the corresponding criticalities, that are: $\mathrm{criticality(SBP} = 110) = 33$, $\mathrm{criticality(DBP} = 72) = 33$, and $\mathrm{criticality(HR} = 63) = 33$. If criticality(mi) reaches

$\max(\text{criticality}(m_i))$ then the situation is critical, as far as metric mi is concerned (4).

$$\text{If criticality}(m_i) = \max(\text{criticality}(m_i))$$
$$then\ (SITUATION_{m_i}\ is\ CRITICAL) \qquad (4)$$

By having calculated the three individual patient's criticalities per health metric, the overall patient's criticality is derived according to (5).

$$\text{If } ((SITUATION_{SBP} \text{ is CRITICAL})$$
$$\text{OR } (SITUATION_{DBP} \text{ is CRITICAL})$$
$$\text{OR } (SITUATION_{HR} \text{ is CRITICAL}))$$
$$then\ (SITUATION_{OVERALL} \text{ is CRITICAL}) \qquad (5)$$

So in our example, all individual criticalities give the output 'NON-CRITICAL'. According to the disjunctive relation (5), given that there isn't at least one partial result which provides the result 'CRITICAL', we conclude that the overall result about the patient's health condition is 'NON-CRITICAL'.

Example with conjunctive fuzzy rules

We estimate the patient's overall critical condition, in order to yield or not emergency access to an EHR. In this approach, we introduce the new and complex conjunctive fuzzy rules, which take into the correlation between Systolic and Diastolic Blood Pressure (SBP and DBP respectively), in order to evaluate the patient's Criticality value (indicated as CR), so as to infer if the patient is in an emergency situation or not. In case of an emergency the requestor will be permitted to access patient's EHR, as long she is a member of an emergency team. These new and complex fuzzy rules, which are based on conjunctive combination of the variables diastolic and systolic blood pressure, are the following:

L_1: If SBP is Low AND DBP is Low THEN CR is High

L_2: If SBP is Low AND DBP is Normal THEN CR is Medium

L_3: If SBP is Low AND DBP is Elevated THEN CR is High

L_4: If SBP is Low AND DBP is High THEN CR is High

L_5: If SBP is Normal AND DBP is Low THEN CR is Medium

L_6: If SBP is Normal AND DBP is Normal THEN CR is Low

L_7: IF SBP is Normal AND DBP is Elevated THEN CR is Medium

L_8: If SBP is Normal AND DBP is High then CR is Medium

L_9: If SBP is Elevated AND DBP is Low THEN CR is High

L_{10}: If SBP is Elevated AND DBP is Normal THEN CR is Medium

L_{11}: If SBP is Elevated AND DBP is Elevated THEN CR is Medium

L_{12}: If SBP is Elevated AND DBP is High THEN CR is High

L_{13}: If SBP is High AND DBP is Low THEN CR is High

L_{14}: If SBP is High AND DBP is Normal THEN CR is Medium

L_{15}: If SBP is High AND DBP is Elevated THEN CR is High

L_{16}: If SBP is High AND DBP is High THEN CR is High

The fuzzy sets per fuzzy variable included in the rules are determined by the American Heart Association (AHA) for blood pressure [7], as presented in (j1). The criticality quantification in the pattern of the fuzzy sets uCR/CR is presented as follows:

CR_{LOW} = {1/0,0.8/20,0.5/50,0.2/80,0/100}

CR_{MEDIUM} = {0/0,0.4/20,1/50,0.4/80,0/100}

CR_{HIGH} = {0/0,0.2/20,0.5/50,0.8/80,1/100}

The maximum value of criticality(mi,mj) of the health metrics mi, and mj is calculated as the max(criticality(mi,mj)). For example, regarding systolic and diastolic blood pressure the distribution of criticality(m1,m2) is depicted in Figure 5.2. It is worth mentioning that max(criticality(m1,m2)) = 67.0.

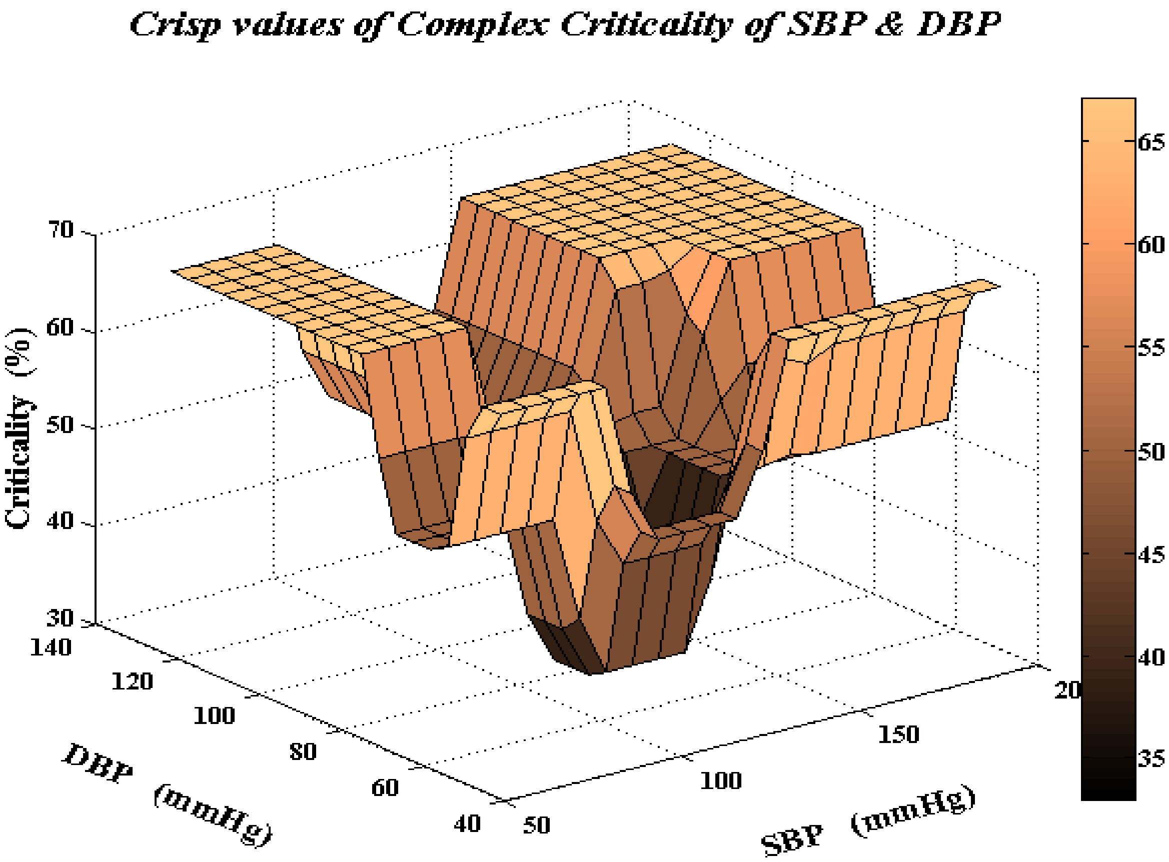


Figure 5. 2 Range of criticality(m_1,m_2) per SBP and DBP.

Consider a particular patient who has the following health metrics values: SBP1=110 mmHg, DBP2=72 mmHg. By applying the inference process presented in the previous section, the criticality is: criticality(SBP=110,DBP=72) = 33. If criticality(mi, mj) reaches max(criticality(mi, mj)) then there is an emergency situation, regarding the metrics mi and mj (1).

If criticality(m_i, m_j) = max(criticality(m_i, m_j))

then (SITUATION(m_i, m_j) is "CRITICAL") (1)

After having evaluated the patient's complex criticality per systolic and diastolic blood pressure, the overall patient's criticality is obtained according to (2).

If (SITUATION$_{\text{SBP AND DBP}}$ is "CRITICAL")

then (SITUATION$_{\text{OVERALL}}$ is "CRITICAL") (2)

According to our example, the complex criticality result is 'NON-CRITICAL'.

d) Personalization of context handling

Personalization of context handling with non-complex fuzzy rules

We approach the challenge of personalization of context handling by adjusting the fuzzy sets of each fuzzy variable appearing in the rules based on the patient's profile, by taking into consideration for example her age. The fuzzy sets of each fuzzy variable appearing in the rules are now defined according to the respective ranges per age group of patients (Tables 5.4, 5.5, 5.6).

According to the AHA [7], the Systolic Blood Pressure ranges in the following categories: 1) Normal (<120 mmHg), 2) Elevated (120-129 mmHg), 3) High (hypertension) stage_1 (130-139 mmHg), 4) High (hypertension) stage_2 (140-180 mmHg), 5) Hypertensive crisis (>180 mmHg). In addition, the normal Systolic blood Pressure per adult age groups ranges in the following categories [9]: 1) 19-40 years (95-135 mmHg), 41-60 years (110-145 mmHg), 61 years or older (95-145 mmHg). The National Health Service (NHS) [10] defines blood pressure ranges of low blood pressure (hypotension) lower than 90 mmHg.

Table 5. 4 Systolic and Diastolic Blood Pressure Ranges.

Age groups	Low SBP	Normal SBP	Elevated SBP	High SBP
19 - 40	60 - 100	90 - 140	130 - 160	150 - 200
41 - 60	60 - 115	105 - 150	140 - 170	160 - 200
60+	60 -100	90 - 150	140 - 170	160 - 200

We consider the following ranges of Systolic Blood Pressure of people who belong in the respective age groups 1) 19-40 years, 2) 41-60 years, and 3) older than 60 years, given in the form uS/S. The fuzzy sets of Systolic Blood Pressure for the age group 41-60 are the following: $\mathrm{S}_{\mathrm{LOW}}^{41-60} = \{1/60, 1/105, 0.5/110, 0/115, 0/200\}, \mathrm{S}_{\mathrm{NORMAL}}^{41-60}\{0/60, 0/105, 0.5/110, 1/120, 1/130, 1/140, 0.5/145, 0/150, 0/200\}, \mathrm{S}_{\mathrm{ELEVATED}}^{41-60} = \{0/60, 0/140, 0.5/145, 1/150, 1/160, 0.5/165, 0/170, 0/200\}, \mathrm{S}_{\mathrm{HIGH}}^{41-60} = \{0/60, 0/160, 0.5/165, 1/170, 1/200\}$.

According to AHA [7], the Diastolic Blood Pressure ranges in the following categories: 1) Normal (<80 mmHg), 2) Elevated (<80 mmHg), 3) High Diastolic Blood

Pressure (hypertension) stage_1 (80-89 mmHg), 4) High (hypertension) stage_2 (90-120 mmHg), 5) Hypertensive crisis (>120 mmHg). In addition, the normal Diastolic Blood Pressure per age group is divided in the following categories [9]: 1) 19-40 years (95-135 mmHg), 41-60 years (110-145 mmHg), 61 years or older (95-145 mmHg). The NHS [10] defines the blood pressure ranges of low blood pressure (hypotension) as lower than 60 mmHg.

Table 5. 5 Diastolic Blood Pressure Ranges.

Age groups	Low DBP	Normal DBP	Elevated DBP	High DBP
19 - 40	50 - 63	57 – 83	77 – 93	87 - 130
41 - 60	50 - 73	67 – 93	87 - 103	97 - 130
60+	50 - 73	67 – 93	87 - 103	97 - 130

We consider the following ranges of diastolic blood pressure of people who belong in the respective age groups 1) 19 – 40 years, 2) 41 – 60 years, and 3) older than 60 years, given in the form uD/D. The fuzzy sets of Diastolic Blood Pressure for the age group 41 – 60 are the following: $\mathrm{D}_{\mathrm{LOW}}^{41-60} = \{1/50, 1/63, 1/67, 0.5/70, 0/73, 0/130\}$, $\mathrm{D}_{\mathrm{NORMAL}}^{41-60} = \{0/50, 0/67, 0.5/70, 1/73, 1/87, 0.5/90, 0/93, 0/130\}$, $\mathrm{D}_{\mathrm{ELEVATED}}^{41-60} = \{0/50, 0/87, 0.5/90, 1/93, 1/97, 0.5/100, 0/103, 0/130\}$, $\mathrm{D}_{\mathrm{HIGH}}^{41-60} = \{0/50, 0/97, 0.5/100, 1/103, 1/130\}$.

According to Abdullah et al. [11], the fuzzy variable Heart Rate ranges in the following categories: Low, Medium, and High. According to Al-Dmour et al. [12], the following “warning scores” categories are provided: 1) score_3 (>130 bpm), 2) score_2 (<40 bpm or 111-130 bpm), 3) score_1 (41-50 bpm or 101-110 bpm), score_0 (51-100 bpm). According to the Centers for Disease Control [13] the heart rate during exercise and the maximum heart rate per age are demonstrated. This particular source informs that the maximum heart rate per age is calculated by the mathematical formula: max heart rate = 220 – age. In our approach, we consider as upper-medium limit the range of 50-85% of heart rate usage [13].

Table 5. 6 Heart Rate Ranges.

Age groups	Low HR	Normal HR	High HR
19 - 40	40 - 60	50 - 105	95 - 190
41 - 60	40 - 60	50 – 95	85 – 170
60+	40 - 60	50 – 80	70 – 160

We consider the following ranges of heart rate of people who belong in the respective age groups 1) 19-40 years, 2) 41-60 years, and 3) older than 60 years, given in the form uHR/HR. The fuzzy sets of Heart Rate for the age group 41-60 are the following: $\mathrm{HR}_{\mathrm{LOW}}^{41-60} = \{1/40, 1/50, 0.5/55, 0/60\}$, $\mathrm{HR}_{\mathrm{MEDIUM}}^{41-60} = \{0/50, 0.5/55, 1/60, 1/85, 0.5/90, 0/95\}$, $\mathrm{HR}_{\mathrm{HIGH}}^{41-60} = \{0/85, 0.5/90, 1/95, 1/170\}$.

The distribution of criticality(mi, age) depends on the age group in which the patient belongs to. For systolic blood pressure for example, two distributions of different age groups are depicted in Figue 5.3 and Figure 5.4.

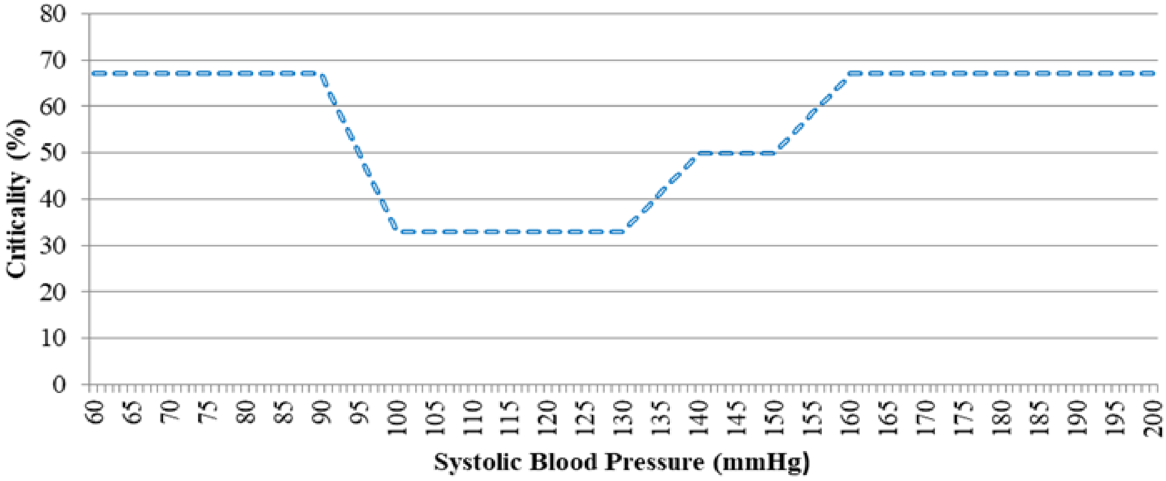


Figure 5. 3 Distribution of criticality(m_1,age), Systolic Blood Pressure for the age group 19 - 40.

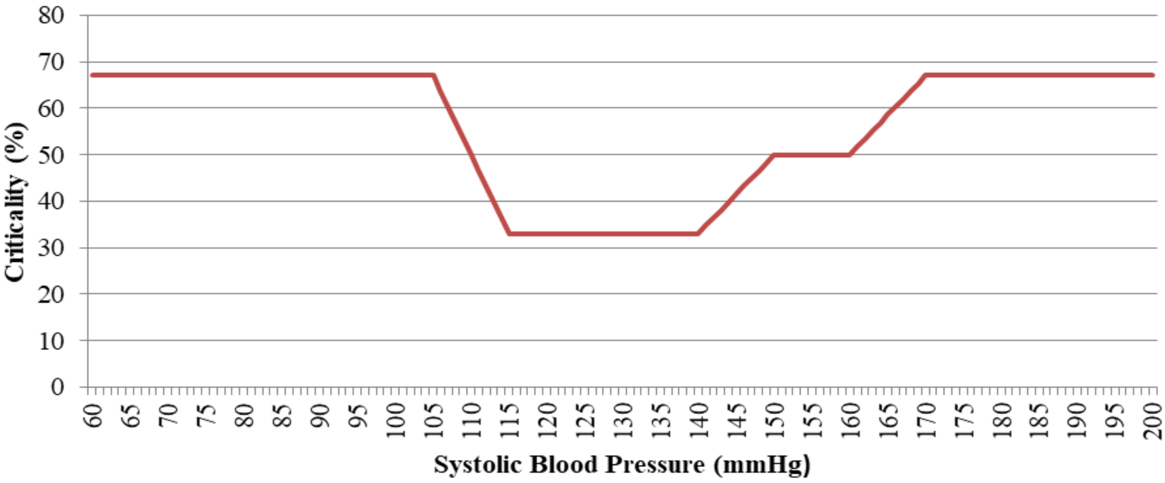


Figure 5. 4 Distribution of criticality(m$_1$,age), Systolic Blood Pressure for the age group 41 - 60.

The calculation of individual criticality in (4) is modified as follows:

$$\text{If } criticality(\mathrm{m_i}, \mathrm{age}) = \max(\, criticality(\mathrm{m_i}, \mathrm{age}))$$

$$\text{then } (SITUATION_{m_i} \text{ is CRITICAL}) \qquad\qquad (6)$$

Then, by having calculated the three individual patient's criticalities per health metric by (6), the overall patient's criticality is derived according to (5).

To illustrate the effect of personalisation, consider another patient with the following health status metrics, which are gauged by the emergency dispatch personnel: $\mathrm{SBP_1} = 160\ \mathrm{mmHg}$, $\mathrm{DBP_2} = 85\ \mathrm{mmHg}$, $\mathrm{HR_3} = 78\ \mathrm{bpm}$. If the patient's age group is 19-40, the criticalities are as follows: $\mathrm{criticality(SBP = 160, age = 35) = 67}$, $\mathrm{criticality(DBP = 85, age = 35) = 50}$, and $\mathrm{criticality(HR = 78, age = 35) = 33}$ and the assessment of the overall situation is 'CRITICAL'. If however, the patient belongs to the age group 41-60, the corresponding value of criticalities are: $\mathrm{criticality(SBP = 160, age = 54) = 50}$, $\mathrm{criticality(DBP = 85, age = 54) = 33}$, and $\mathrm{criticality(HR = 78, age = 54) = 33}$ and the assessment of the overall situation is 'NON-CRITICAL'. Hence, we derive two different assessment of the situation criticality depending on the patient's age group.

Personalization Approach for Complex Context Handling

We handle the demanding aspect of context handling personalization, by adapting the fuzzy variables which appear in the rules that are dependent on the patient's personal information, e.g., her age, as presented in (j1). The fuzzy sets of all fuzzy variables which appear in the rules are presented in (j1). The distribution of criticality(mi, mj, age) is based on the patient's age group. As an example, regarding systolic and diastolic blood pressure, the distribution of age group 19-40 is illustrated in Figure 5.5.

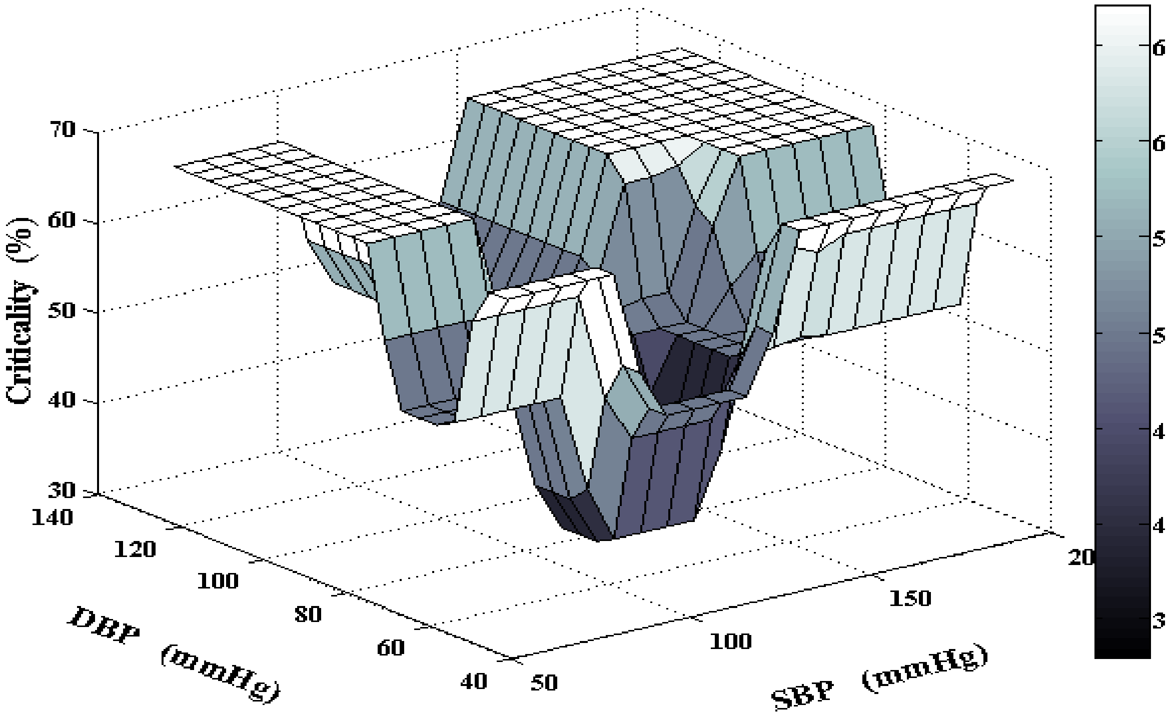


Figure 5. 5 Range of criticality(m_1,m_2,age) per SBP and DBP according to the age group 19-40.

The computation of complex criticality in (1) is computed based on the following pattern:

If criticality(m_i, m_j, age) = max(criticality(m_i, m_j, age))

then (SITUATION(m_i, m_j) is "CRITICAL") (3)

After having computed the patient's complex criticality using equation (3), the overall patient's criticality is deduced based on (2). To clarify the personalization effect, let us examine a patient with the following health metrics values: SBP1=160 mm Hg, DBP2 = 85 mm Hg. If the patient's age belongs in the 19-40 group, the criticality is: criticality(SBP = 160, DBP = 85, age = 35) = 67.0, and the overall situation is assessed as 'CRITICAL'. On the contrary, if the patient belongs to the 41-60 age group, the corresponding criticality is: criticality(SBP = 160, DBP = 85, age = 54) = 50.0, and the overall situation is assessed as 'NON-CRITICAL'. Thus, two different results are derived according to the patient's age.

C. Evaluation/Validation

1) Personalzation of context handling with non-complex fuzzy rules

a) Implementation

We validated our approach by implementing it and integrating it within EHRServer. EHRServer [14] is an open source clinical information management and sharing platform based on the openEHR standard [15]. We used our approach to handle access control to data stored in EHRServer. We examined the following three test cases.

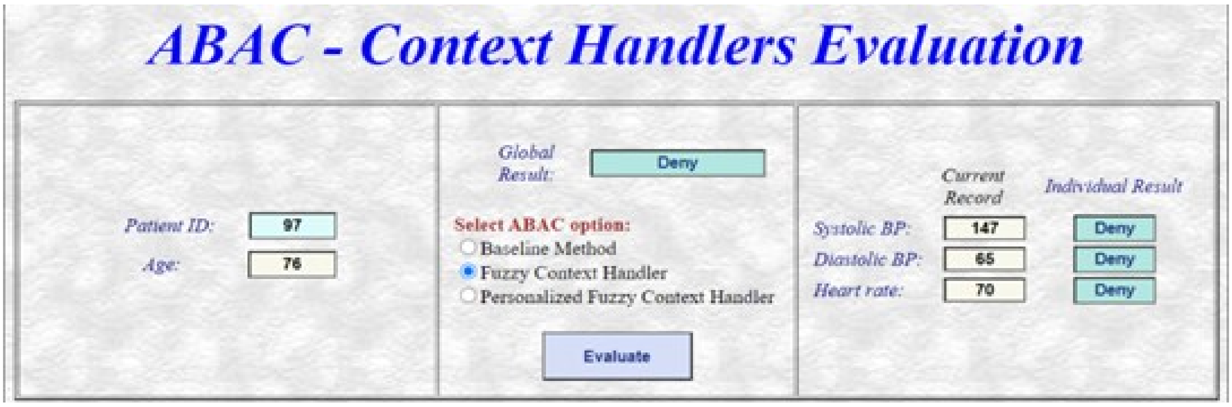
In the first case, we used the baseline ABAC method to control access. Specifically, if the data requestor is an ER (Emergency Room) doctor and the patients' metrics are in conjunction above the recommended limit, then the doctor has access to patient EHRs. The policy rule is shown next:

$$\begin{aligned}&\text{If (requestor} = \text{ER Doctor)}\\&\quad\text{AND contextual expression (SBP} > \text{SBP}_{\text{THRESHOLD}} \text{ OR}\\&\qquad\qquad\qquad\qquad\qquad \text{DBP} > \text{DBP}_{\text{THRESHOLD}} \text{ OR}\\&\qquad\qquad\qquad\qquad\qquad \text{HR} > \text{HR}_{\text{THRESHOLD}})\\&\text{then (permit access to patient EHRs)} \qquad (7)\end{aligned}$$

In the second case, we used ABAC with non-personalized context handlers and the following rule:

$$\begin{aligned}&\text{If ((requestor} = \text{ER Doctor)}\\&\text{AND context expression (CRITICAL}_{\text{SITUATION}} = \text{true))}\\&\text{then permit} \qquad (8)\end{aligned}$$

In the third case, we used ABAC with personalized context handlers. We developed a web application (Figure 5.6) so as to implement and validate the three types of ABAC methods.



ABAC - Context Handlers Evaluation

Patient ID: 97

Age: 76

Global Result: Deny

Select ABAC option:

○ Baseline Method
● Fuzzy Context Handler
○ Personalized Fuzzy Context Handler

Evaluate

	Current Record	Individual Result
Systolic BP:	147	Deny
Diastolic BP:	65	Deny
Heart rate:	70	Deny

Figure 5. 6 ABAC integration within EHRServer.

Finally, we compared the performance of each ABAC method (baseline, non-personalised and personalised context handlers) for each one of the three test cases (Figure 5.7). The ABAC method with personalised context handlers does have a performance penalty of approximately a factor of two. The performance penalty does not warrant its application in all but the most demanding applications in terms of performance.

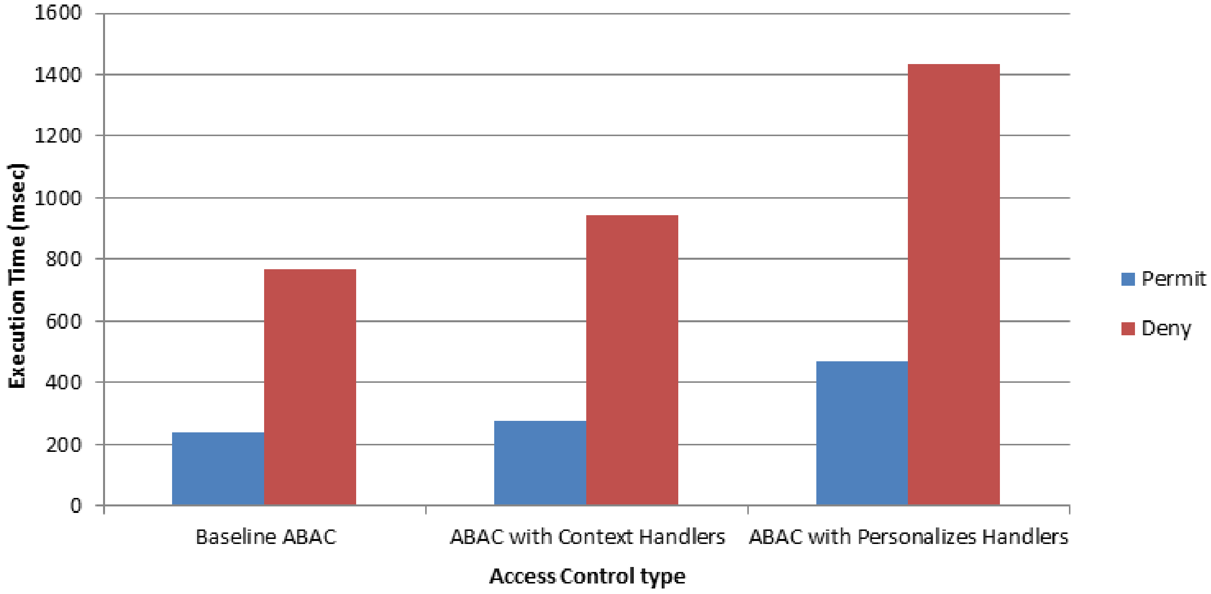


Figure 5. 7 Performance of each ABAC method integrated within EHRServer.

b) Datasets & Scenarios

To evaluate our approach, we used the PPG-BP (Photoplethysmograph – Blood Pressure) dataset [16], which contains 219 patient healthcare records. The patients' age varies from 20 to 89 years, with an average age of 58 years. The fields of each record are the following: ID, Gender, Age, Height, Weight, Systolic blood pressure, Diastolic blood pressure, Heart rate, BMI, Diseases (hypertension, diabetes, cerebral infarction, cerebrovascular disease). Three different emergency scenarios have been considered, based on the health metrics of systolic blood pressure, diastolic blood pressure, and heart rate. Comparisons between baseline ABAC, ABAC with context handlers and ABAC with personalized context handlers are shown.

c) Access Control Results

To evaluate the capability of our approach to characterise critical situations and to permit or deny access to data using the ABAC paradigm, we assessed the distribution of permit and deny results as presented next. To evaluate the capability of our approach to characterise critical situations and to permit or deny access to data using the ABAC paradigm, we assessed the distribution of permit and deny results as presented next.

Permit and Deny Results for each ABAC Method per age Group

The distribution of Permit and Deny results of the access control mechanism using the baseline ABAC method per age group is presented in Figure 5.8.

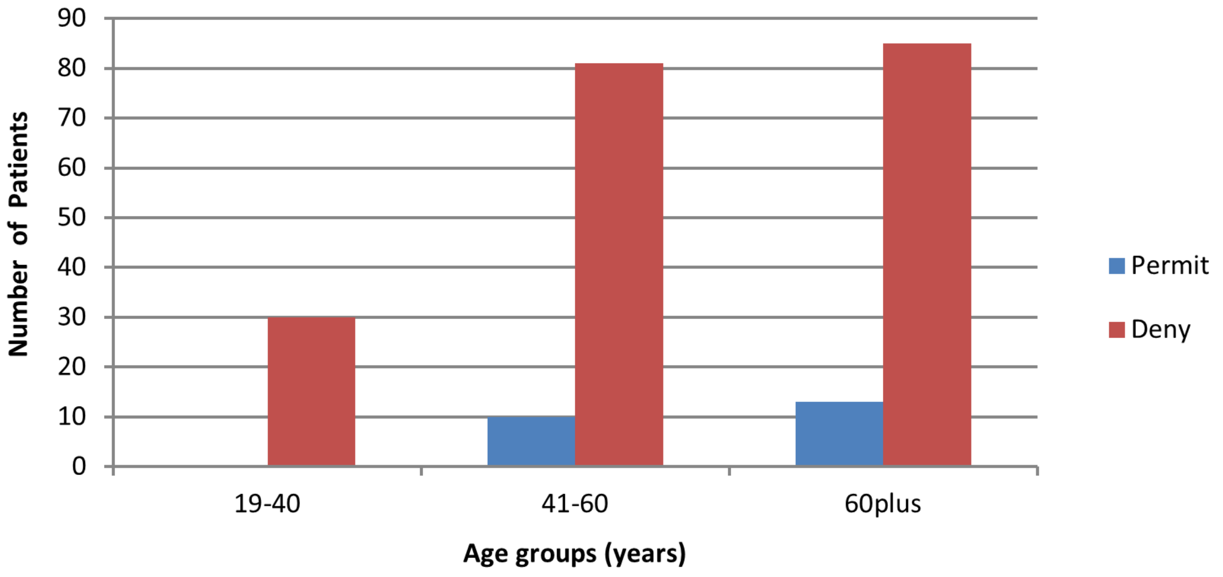


Figure 5. 8 Access control results, baseline ABAC.

The distribution of Permit and Deny results of the access control mechanism using our non-personalized fuzzy context handler per age group, is presented in Figure 5.9.

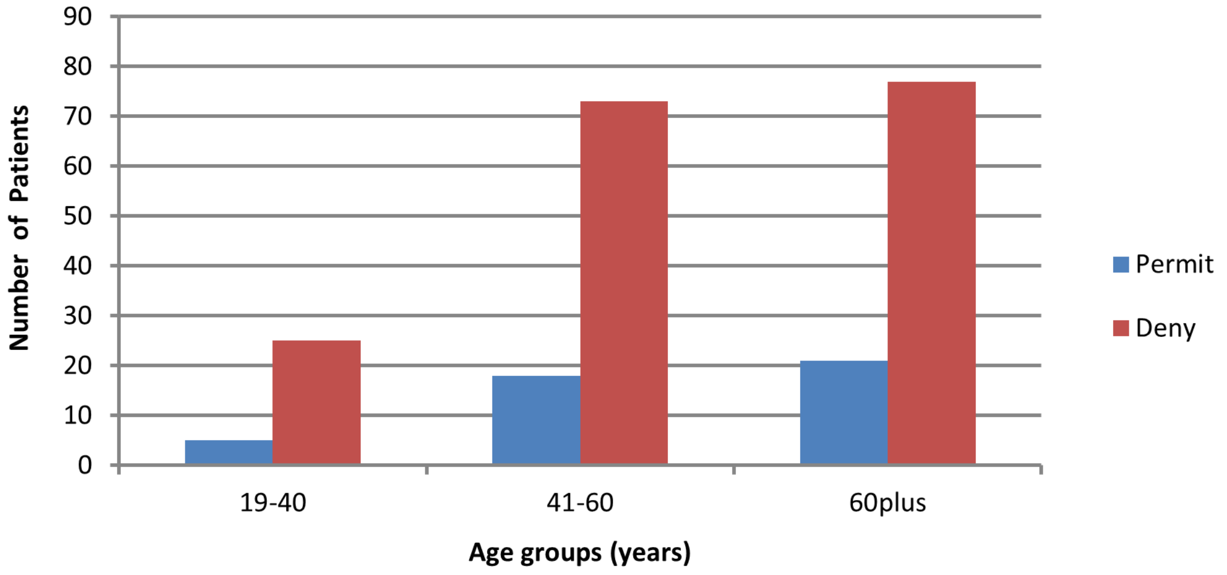


Figure 5. 9 Access control results, ABAC with context handlers.

The distribution of Permit and Deny results of the access control mechanism using personalized context handlers per age group is presented as follows in Figure 5.10.

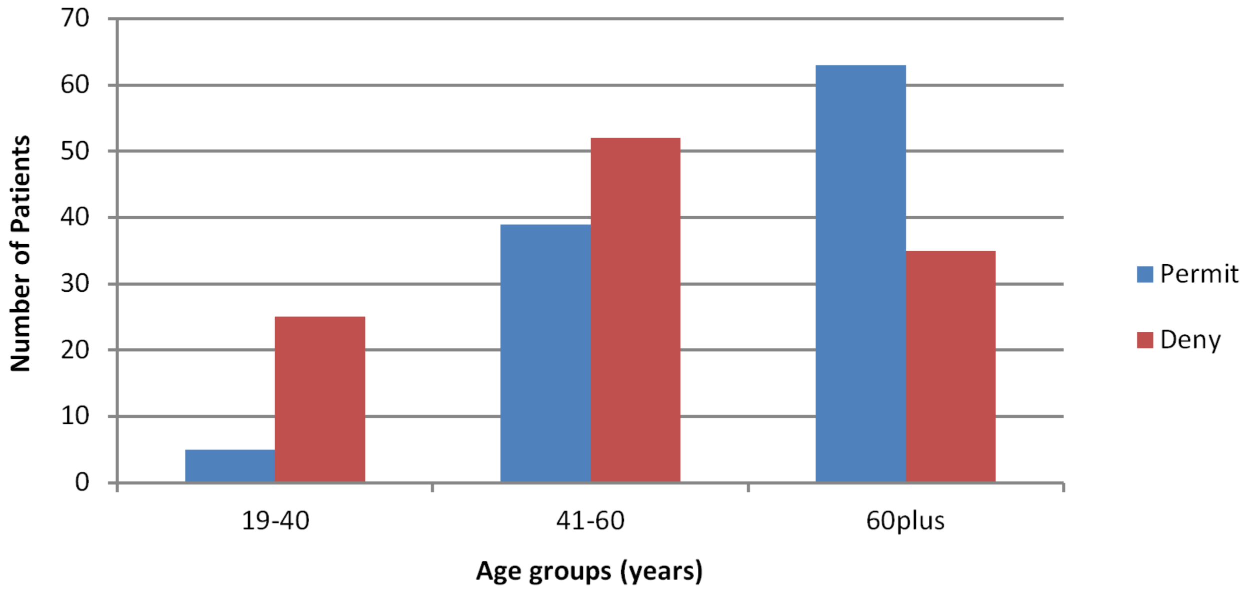


Figure 5. 10 Access control results, ABAC with personalized context handlers.

Notice that ABAC with personalized context handlers achieves the highest number of permits in critical situations, especially on the two older age groups.

False Positives and Negatives for each ABAC Method per Age Group

We also compared ABAC with personalised context handlers vs non-personalised as well as vs baseline ABAC in terms of false positives and false negatives. The former comparison is shown Figure 5.12, while the latter is shown in Figure 5.11.

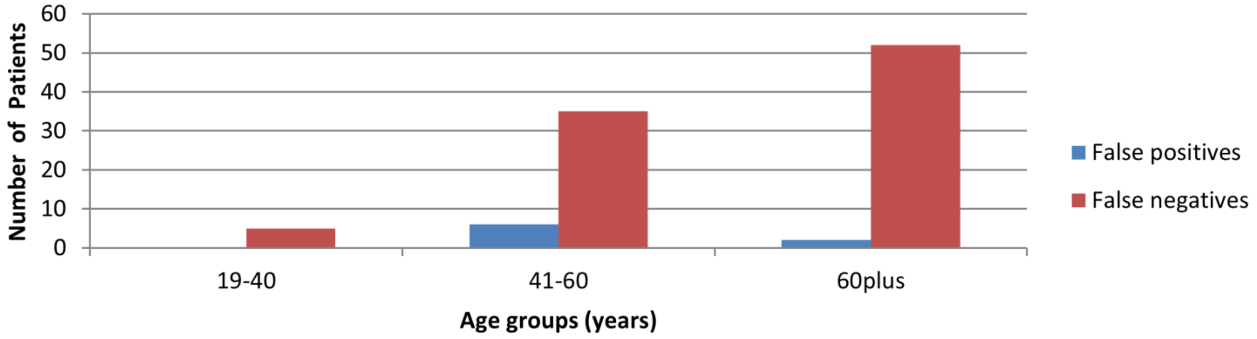


Figure 5. 11 False positives and negatives per age group, baseline ABAC.

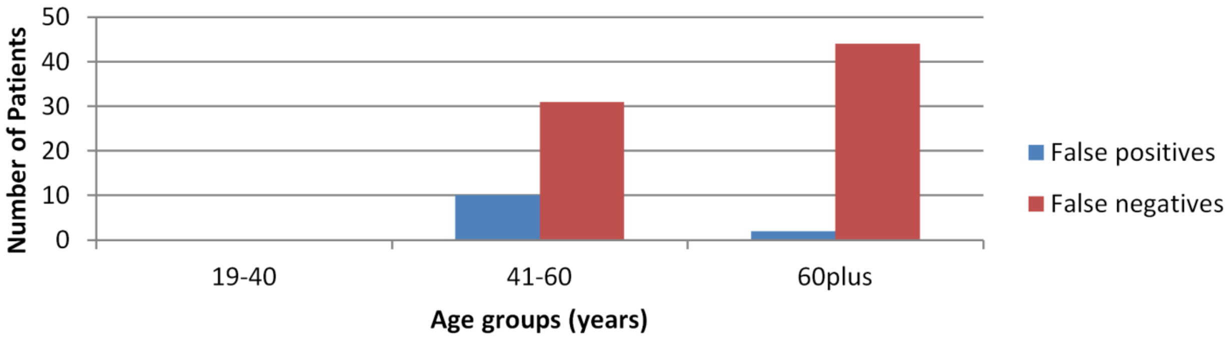


Figure 5. 12 False positives and negatives per age group, ABAC with context handlers.

Notice that baseline ABAC produces an increasing number of false negatives and positives as patients' age increases. False negative in particular are high and especially hazardous for the patient's life.

Similarly, we note that ABAC with non-personalised context handlers is not as capable as ABAC with personalized context handlers in detecting critical situations, especially in the oldest age group that is the most important.

2) *Complex Fuzzy Personalized Context Handlers*

a) Implementation

In order to validate our approach, we implemented and integrated our work within EHRServer [14], which is an open source system which complies with the standard of openEHR [15]. We applied our method for controlling access to medical information saved in EHRServer and investigated three cases. First, the baseline ABAC method was used to manage access. Specifically, if the requestor of sensitive information is a member of ED (Emergency Department) and the patients' metrics meet the suggested threshold, then the healthcare professional is granted access to patient's EHRs. The policy rule is the following:

If (requestor = ED Member) AND contextual expression

($SBP>SBP_{THRESHOLD}$ OR DBP $>DBP_{THRESHOLD}$)

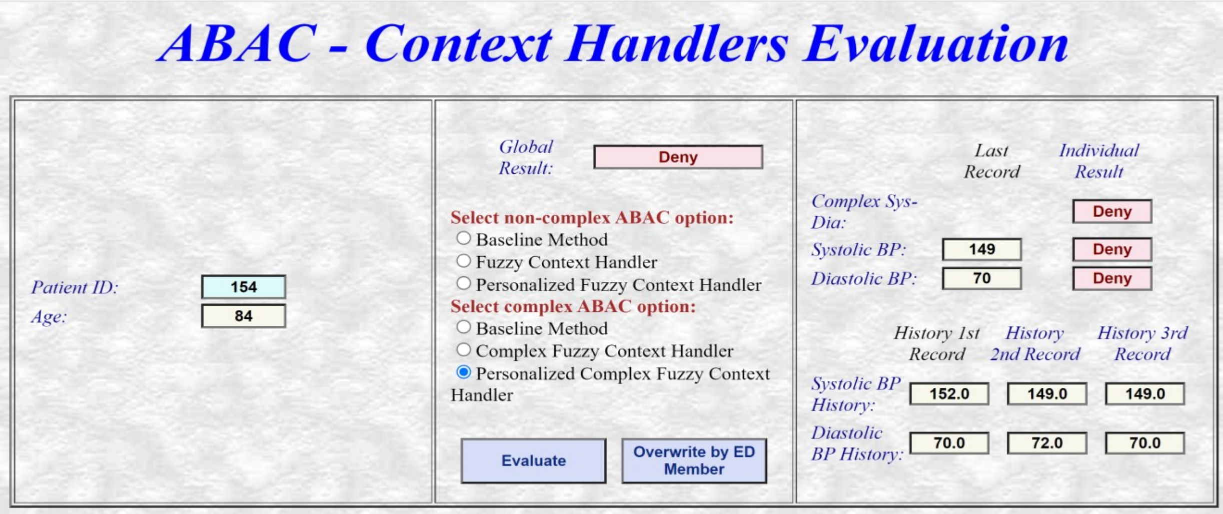
then (permit access to patient's medical information) (4)

Second, we exploited ABAC with non-personalized complex context handlers according to the following rule:

If (requestor = ED Member) AND contextual expression

(SITUATION(m_i, m_j) is "CRITICAL")

then (permit access to patient's medical information) (5)



ABAC - Context Handlers Evaluation

Patient ID: 154
Age: 84

Global Result: Deny

Select non-complex ABAC option:
○ Baseline Method
○ Fuzzy Context Handler
○ Personalized Fuzzy Context Handler

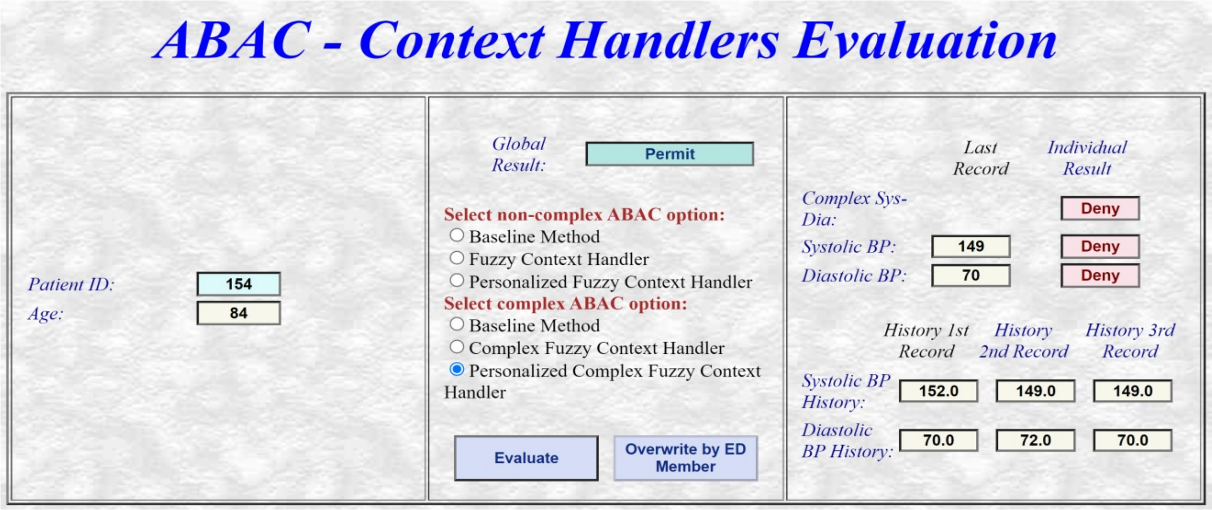
Select complex ABAC option:
○ Baseline Method
○ Complex Fuzzy Context Handler
● Personalized Complex Fuzzy Context Handler

Evaluate | Overwrite by ED Member

	Last Record	Individual Result
Complex Sys-Dia:		Deny
Systolic BP:	149	Deny
Diastolic BP:	70	Deny

	History 1st Record	History 2nd Record	History 3rd Record
Systolic BP History:	152.0	149.0	149.0
Diastolic BP History:	70.0	72.0	70.0

Figure 5. 13 ABAC integration within EHRServer – System's initial decision Deny.



ABAC - Context Handlers Evaluation

Patient ID: 154
Age: 84

Global Result: Permit

Select non-complex ABAC option:
○ Baseline Method
○ Fuzzy Context Handler
○ Personalized Fuzzy Context Handler

Select complex ABAC option:
○ Baseline Method
○ Complex Fuzzy Context Handler
● Personalized Complex Fuzzy Context Handler

Evaluate | Overwrite by ED Member

	Last Record	Individual Result
Complex Sys-Dia:		Deny
Systolic BP:	149	Deny
Diastolic BP:	70	Deny

	History 1st Record	History 2nd Record	History 3rd Record
Systolic BP History:	152.0	149.0	149.0
Diastolic BP History:	70.0	72.0	70.0

Figure 5. 14 ED member's final decision – Overwrite of deny access with permit.

Figure 5.13 demonstrates the system's decision regarding the case of ABAC with personalized complex context handlers, while Figure 5.14 illustrates the ability of the healthcare professional to bypass the system's Deny access decision so that the global result becomes Permit. As shown in Figure 5.13 and Figure 5.14, the visual environment of our web application is divided in three panes. In the first pane the patient's ID and age are demonstrated, while in the second pane the system's global access result is illustrated. Below this feature, the ABAC options with and without complex context handlers are presented in the respective two groups. The first group contains the three non-complex ABAC individual context handlers options regarding the health metrics of systolic and diastolic blood pressure and heart rate, as presented in our previous work (j1), while the second group contains the new ABAC with complex context handlers options, where the health metrics of systolic and diastolic blood pressure are combined by producing a single criticality result. The three respective non-complex / complex cases are the following: i) the baseline ABAC which handles basic thresholds as limits in order to permit or deny access, ii) the ABAC non-personalized non-complex / complex case which takes under consideration only the fuzzy inferencing process, and iii) the ABAC personalized non-complex / complex case which takes under consideration the fuzzy inferencing process as well as the personalization aspect of age. Below the ABAC selection options the button "Evaluate" exists regarding the system's decision (Figure 5.13) as well as the "Overwrite by ED" button, where the healthcare professional himself has the ability to alter the system's decision and bypass the deny access by gaining access to the system (Figure 5.14), or vice versa. In the third pane the patient's current health metrics are demonstrated along with the result of complex context handler as well as the individual access results per health metric, and the patient's current health history so that the healthcare professional has a broader scope.

It is worth mentioning, regarding all three test case scenarios, that the final decision regarding the emergency access of the healthcare professional is taken by the healthcare professional herself. Specifically, regarding the personalized case, the healthcare professional has at her disposal: i) the system's access result which takes under consideration if the requestor is an emergency department team member and the criticality of the fuzzy inferencing system, as stated in relation (5), ii) the current health metrics of systolic and diastolic blood pressure along with iii) the recent health metrics history retrieved by the IoT sensors, and iv) the patient's age. For example, the healthcare professional, by taking into consideration the patient's information of age and current health metrics values along with the recent health history, and the deny access result of our system as a recommendation, he still has the ability to bypass the system's recommendation and actually have access to the patient's EHR's, in case he judges that the patient's current health metrics in conjunction with the recent health history values are indeed critical. It is important to note that each patient's case is undoubtedly unique, and a personalized approach should always be implemented.

b) <u>Access Control Results</u>

In our evaluation, the PPG-BP (Photoplethysmograph – Blood Pressure) dataset [16] was used. This database contains health records of 219 patients whose age varies from 20 to 89 years. Three different critical cases have been considered, based on systolic and diastolic blood pressure.

We validate our method to detect emergency conditions by granting or denying access to medical information by leveraging the ABAC mechanism and we gauged the distribution of deny and permit results. We compared the context handlers of our approach of baseline ABAC, non-personalized complex conjunctive fuzzy context handler and personalized complex conjunctive context handler in order to evaluate their efficiency.

Permit and Deny Access Control Results Grouped per Age for each ABAC Method

Access control results of Permit and Deny by exploiting the three above-mentioned cases of: i) baseline ABAC method, ii) ABAC with non-personalized complex fuzzy context handler, and iii) ABAC with personalized complex context handler, along with the three cases of ABAC with non-complex context handlers of i) baseline ABAC, ii) ABAC with non-personalized non-complex fuzzy context handler, and iii) ABAC with personalized non-complex context handler, as thoroughly examined in our previous work (j1), according to age are depicted in Figure 5.15. As described above the complex context handlers take into consideration complex fuzzy rules, which consider multiple health metrics in the “if” part, where in this case there are the two health metrics of systolic and diastolic blood pressure.

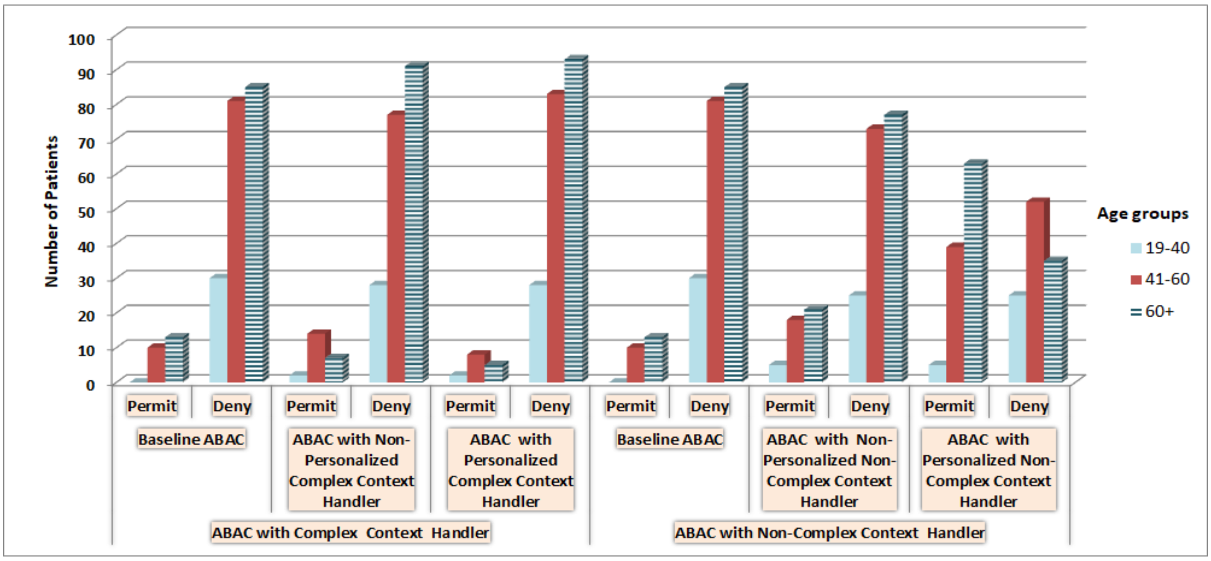


Figure 5. 15 Access control results according to each ABAC case..

It is worth mentioning that the number of permit cases regarding the ABAC with non-personalized complex context handler is lower compared to those in the equivalent case of ABAC with non-personalized non-complex context handler of our previous work (j1), for all age groups. Respectively, the number of permit cases regarding the ABAC with personalized complex context handler is lower compared to those in the equivalent case of ABAC with personalized non-complex context handler of our previous work (j1), in all age groups. We finally note that ABAC with personalized complex context handlers accomplishes the lower number of permit results in emergency conditions, notably regarding the two older age groups, in comparison with the other two cases of new baseline ABAC method, and ABAC with non-personalized complex fuzzy context handler.

False Positives and Negatives per ABAC Method and Age Group

Additionally, our comparison of all three above-mentioned cases of: i) baseline ABAC method, ii) ABAC with non-personalized complex fuzzy context handler, and iii) ABAC with personalized complex context handler, along with the three cases of ABAC with non-complex context handlers of i) baseline ABAC, ii) ABAC with non-personalized fuzzy context handler, and iii) ABAC with personalized complex context handler, as thoroughly examined in our previous work (j1) regarding false positives and false negatives, according to age, is illustrated in Figure 5.16.

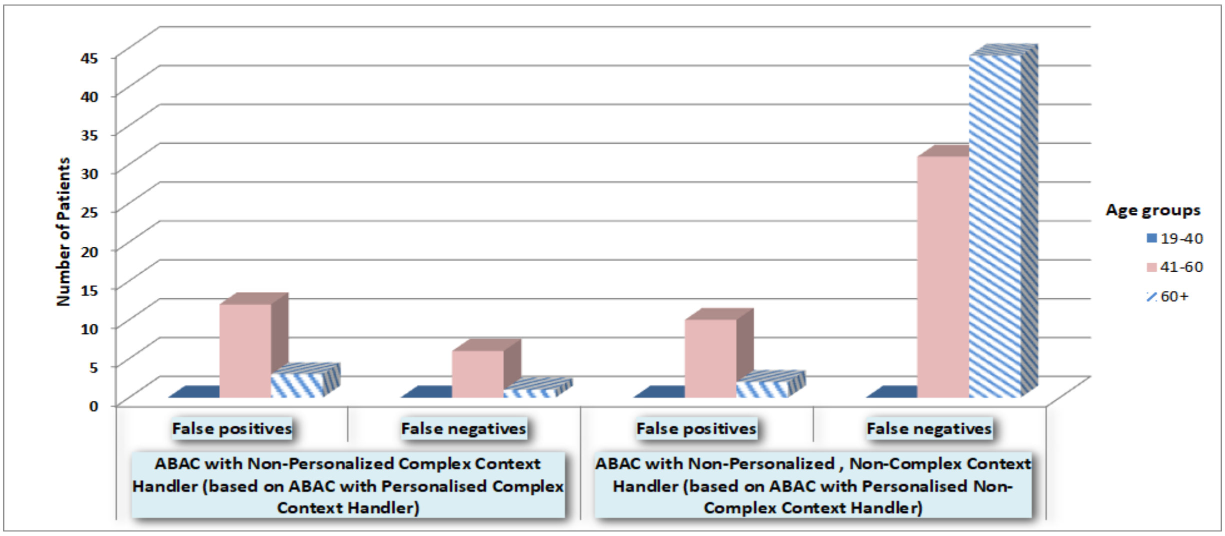


Figure 5. 16 False positives and negatives of ABAC with non-personilized complex context handler vs. ABAC with non-personilized non-complex context handler.

We notice that the numbers of false negatives, regarding the ABAC with personalized complex context handler case, are considerably lower, compared to those in the equivalent case of (j1) of ABAC with personalized non-complex context handler, in ages over 40, while they are almost equal as far as false positives are concerned.

Chapter 6

6. Prognostic-based Context Handlers

A. Motivation

Handling access to medical information is essential as the safeguarding of the patient's sensitive data privacy, e.g., her health history, is of prime importance. Access control models are related to the privileges an entity has upon handling particular data objects. Prevailing based on user identity access control models comprise Role-Based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [1]. Except for these static approaches, the Attribute-Based Access Control (ABAC) paradigm has been developed, which is dynamic [2]. In ABAC, there are connections snapshots that produced and dynamically altered based on the the current context, instead of no dynamic lists of permissions that link entities with objects.

In the medical sector, contextual information which characterizes an emergency in patient's healthcare state, should be deemed when controlling access to the healthcare sensitive information by guaranteeing the most efficient treatment. Accordingly, the implementation of access control models which integrate the context concept, such as the notion of dynamically changing contextual attributes which indicate a status, is needed. More specifically, context is considered as any information characterizing the status of an entity such as person, place, and object, related to the association between an application and a requestor [3]. Exploiting contextual data facilitates the implementation of access control policies by taking into account the conditions of access requests evaluation. For instance, in critical situations, an emergency healthcare professional intends to access partially the patient's healthcare data to encounter best a critical condition. The values of contextual information are obtained for instance from IoT devices, such as a wearable able to gauge the blood pressure. We report that context handlers are beneficial for implementing processes of dynamic authorization which consider the critical status of a specific medical acute care event before making a decision access control. In critical conditions the emergency medical teams should access immediately the patients' medical records.

The main research objective of our study is the development and application of machine learning techniques based on patients' health metrics and integrate them with an ABAC paradigm. This mechanism can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers in which raw contextual information e.g., data from IoT devices, can be used in order to identify acute care conditions and permit access to sensitive medical information. More specifically, we are going to use the patient's health history in order to predict the health metrics of the next couple of hours by implementing Long Short Term Memory (LSTM) Neural Networks (NNs). The prognosed health metrics values are to be evaluated by our personalized fuzzy context handlers, so as to estimate the criticality of the health condition of patient. Finally our objective is to develop a sufficient web application so as to evaluate our approach and compare with our previous work (j1).

1) Analytics

a) Analytics definitions and Categories

According to Simpao et al. [4], analytics is the way of developing insights through the efficient use of data and application of quantitative and qualitative analysis. Cortada et al. [5] report that analytics can generate fact-based decisions for "planning, management, measurement, and learning" purposes. Tomar et al. [6] claim that analytics assist healthcare professionals in disease prediction, diagnosis, and treatment, by improving service quality and results in reduction of dataset's cost information, predictive (i.e., prediction of upcoming events based on historical data) and prescriptive (i.e., utilization of scenarios to provide decision support). Additionally, according to Lustig et al. [7], analytics is categorized in descriptive, predictive, and prescriptive ones. More precisely, descriptive analytics describes past performance of existing systems, predictive analytics predicts future performance of systems, and prescriptive analytics prescribes interventions so as to improve future performance of systems. According to Khalifa [8] five main types of analytics could be identified: descriptive, diagnostic, predictive, prescriptive and discovery analytics.

Each one of them has its own distinct role in improving healthcare. More specifically, descriptive analytics works by categorizing, characterizing, aggregating and classifying data to be converted to valuable information to help healthcare professionals understand and analyze decisions, performance and results. According to Basu's definition [9], prescriptive analytics role comes into action when decisions have to be made regarding a wide range of feasible alternatives, and it enables executives not only to look into consequences and expected results of their decisions and see the opportunities or problems, but it also provides them with the best course of action so as to take advantage of that foresight in a timely manner. According to the authors, the success of prescriptive analytics depends mainly on the adoption of five basic elements: utilizing hybrid data, including both structured and unstructured data types, integrating predictions and prescriptions, considering all possible side effects, and using adaptive algorithms that can be tailored easily per situation along with the importance of robust and reliable feedback mechanisms. According to Bernstein [10], discovery analytics utilizes knowledge more than information or what can be considered as wisdom in discovering new medications or alternative treatments or detect new symptoms, signs or diseases or unknown side effects. According to Khalifa [11], descriptive analytics were used to explore different variables and test for any relations between these variables and admission probability of the patient so as to determine which variables could be utilized in order to build the suggested decision algorithm model. According to Simpao et al. [4] diagnostic health analytics works on answering why something happened. It needs extensive exploration and directed analysis of the existing data using tools such as visualization techniques to discover the root causes of a problem and help users realize nature and impact of problems. As an example, the increased waiting time in providing certain healthcare services could be tracked down to multiple influential factors including patient, provider or organization related factors.

b) Health Analytics definition and Categories

According to Cortada et al. [5], the Healthcare Information and Management Systems Society defines health analytics as the systemic use of medical data and related management information via the application of analytics methods and tools such as quantitative and qualitative statistics, context analysis and predictions to develop actionable insights and lead information based strategic and operational management for better healthcare.

According to Madsen [12] health analytics is a business driven term that encompasses a wide spectrum of aspects and dimensions of big data analysis. According to the authors, this analysis is based mainly on the availability and accessibility of data and information derived through the efficient integration and interoperability of a wide range of technologies and tools such as electronic health record systems, data warehouses, web applications, clinical decision support systems and other operational systems. According to Kohn [13], health analytics applications and tools can be considered as a collection of decision support systems for the healthcare providers, enabling knowledge professionals such as physicians, nurses, health administrators, health policy makers and pharmacists to acquire vision and make more effective evidence based on healthcare decisions. Chen et al. [14] report that health analytics could also be defined as a way of transforming data and information into plans and actions through analysis and insights in the context of the healthcare decision making and problem solving. Bates [15] reports that typically, hospitals and healthcare organizations have already implemented descriptive analytics to medical data and clinical cases. According to the authors, by using queries and reporting tools and technologies, the healthcare professionals usually collect data and information on past performance, enabling classification and categorization of normally structured data.

c) LSTM in healthcare

The Long Short Term Memory (LSTM) Neural Networks (NNs) were initially proposed by Hochreiter and Schmidhuber in 1997 [16], which address the over extended time intervals by recurrent back-propagation that takes a very long time, mostly because of insufficient, decaying error backflow. The LSTM NNs are widely used in the healthcare domain. Yin et al. [17] propose a 3D human action detection system for real-time inference for intelligent healthcare applications based on LSTM, which can be used in emergency warnings. Kadri et al. [18] propose an approach for forecasting of daily patient arrivals at the pediatric emergency department, based on LSTM-deep-learning. Tsai et al. [19] propose a framework in embedding bottleneck vocal features in a LSTM architecture to automatically recognize pain-level intensity for emergency room patients during triage. Mantas [20] uses LSTM recurrent NN to build a model to predict emergency department wait time in the next 2 hours using a randomly generated patient timestamp dataset of a typical patient hospital journey. Nwakanma et al. [21] proposed an IoT-based emergency detection LSTM-based system, where the sensor collects vibration data which assist in predicting emergency scenario. Reddy et al. [22] present that their deep learning methodology of Recurrent Neural Networks (RNN) with LSTM, which can utilize longitudinal EHR data as sequential data, shows significant promise in predicting rehospitalization in lupus patients. Zhang et al. [23] based on the Covolutional Neural Networks (CNN) LSTM model, rely on the COVID-19 emergency in Wuhan and analyze the influence mechanism on netizens' emotions. Mou and Yu [24] propose a CNN-LSTM blood pressure prediction method based on pulse wave data. Chae et al. [25] performed "particulate matter" prediction using the LSTM among others, where the "particulate matter" can cause various toxin-induced cancers, affected lungs, and worsened asthma. Mumtaz et al. [26] apply LSTM model, among others, for predicting the concentration of air pollutants and predicting the overall quality of an indoor environment, which is helpful for individuals who suffer from acute pulmonary disorders and COVID-19 patients.

B. *Methods and Tools*

In this study, we extend our previous work on context-aware access policies (j1), as analytically described in Chapter 5, by considering, apart from the patient's current health situation, the prognosis of the patient's future health status. The proposed methodology delivers an access control mechanism which relies on Attribute-based Access Control (ABAC). The methodology combines machine learning techniques to predict the patient's upcoming health condition along with fuzzy logic to reason about the context of the access request (Figure 6.1).

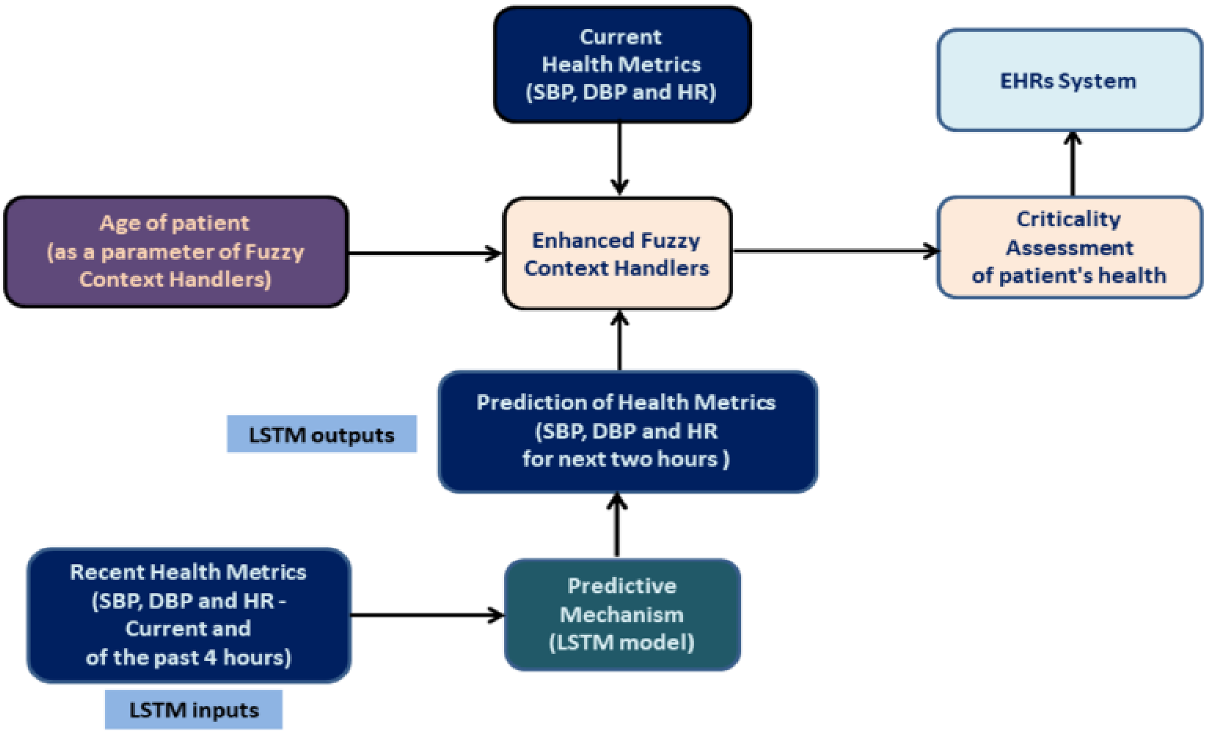


Figure 6. 1 Methodology

The predictive mechanism, implemented with LSTM, receives as input the recent health metrics and outputs the predictions of health metrics for the next two hours. Subsequently, the fuzzy context handler assesses the criticality of the future health status of the patient, by taking into consideration (i) the patient's age, (ii) the current health metrics and (iii) the predicted health metrics for the next two hours. The criticality assessment determines the decision about granting or not emergency access by healthcare professionals to the EHRs system.

1) __Fuzzy Context Handlers__

A context handler in XACML [27] is a system entity which transforms access requests from the initial format of requests to the canonical form of XACML [28]. Apart from using, or not, the XACML architecture, context handlers are exploited in ABAC to transform the attribute representations into mediums related to the environment of the application. Lower-level context is beneficial for uplifting context of higher level and understanding emergency conditions, for example in the situation of an acute care healthcare dispatcher case. This knowledge is responsible for determining if access to private medical information should be permitted or not.

In our earlier work (j1), as analytically presented in Chapter 5, we developed context handlers governed by fuzzy rules to identify critical situations. A fuzzy context handler uses fuzzy rules that associate contextual attributes with fuzzy values and generates as output an assessment of the criticality of the incident. The related contextual attributes, which are represented in a context model, are presented in detail in (c2), in Chapter 12. Here, we extend the fuzzy context handlers by taking into consideration apart from the patient’s current state her future one as well, by predicting the patient’s future health status.

2) ***Predicting Mechanism***

To implement the prediction mechanism, we rely on the long short term memory (LSTM) model [16], a variant of the recurrent neural network which is used to predict the patient’s future health metrics. LSTM networks have the capability of learning long-term dependencies. The LSTM network outperforms others in the prediction of the next sequence of process instances, because it predicts the next one by storing lengthy input sentences. The LSTM prediction exhibits a considerable rise and aligns with the actual time series data [29].

The basic structure (i.e., a cell) of an LSTM module, as illustrated in Figure 6.2, comprises three separate gates: input, output and forget. Each cell persists values over arbitrary time intervals while the three mentioned gates adjust the information flow coming into and out of the cell. There are three sigmoid gates, to protect and control the cell state. Each sigmoid gate decides what information should be ignored from the cell state. Calculating the output of a cell involves first the decision on which information to remove from the previous cell. Output “1” or “0” indicate that all previous information should be kept or discarded, respectively. Additionally, the tanh gate serves to convert values to be between −1 and 1. This special structure, apart from the input Xt, takes, additionally as input, the output of the previous block Ht−1 along with the memory from the previous LSTM block Ct−1. The final output Ht is given by Formula (1).

$$\mathrm{H_t} = \mathrm{O_t} * \tanh(\mathrm{C_t}) \tag{1}$$

where:

$$\mathrm{O_t} = \ \sigma\,(\mathrm{W_o} \cdot [\mathrm{H_{t-1}}, \mathrm{X_t}] + \mathrm{b_o}) \tag{2}$$

$$\mathrm{C_t} = \mathrm{F_t} * \mathrm{C_{t-1}} + \mathrm{I_t} * \mathrm{C_t} \tag{3}$$

$$\mathrm{C'}_{\mathrm{t}} = \tanh(\mathrm{W_c} \cdot [\mathrm{H_{t-1}}, \mathrm{X_t}] + \mathrm{b_c}) \tag{4}$$

$$\mathrm{I_t} = \ \sigma\,(\mathrm{W_i} \cdot \ [\mathrm{H_{t-1}}, \mathrm{X_t}] + \mathrm{b_i}) \tag{5}$$

$$F_t = \sigma(W_f \cdot \ [H_{t-1}, X_t] + b_f) \tag{6}$$

In the above equations, Wf, Wi, Wc and Wo are weights and bf, bi, bc and bo are biases, which are learned during the training phase of the network. We perform multi-step forecasting [30] of two next steps based on multivariate input time series.

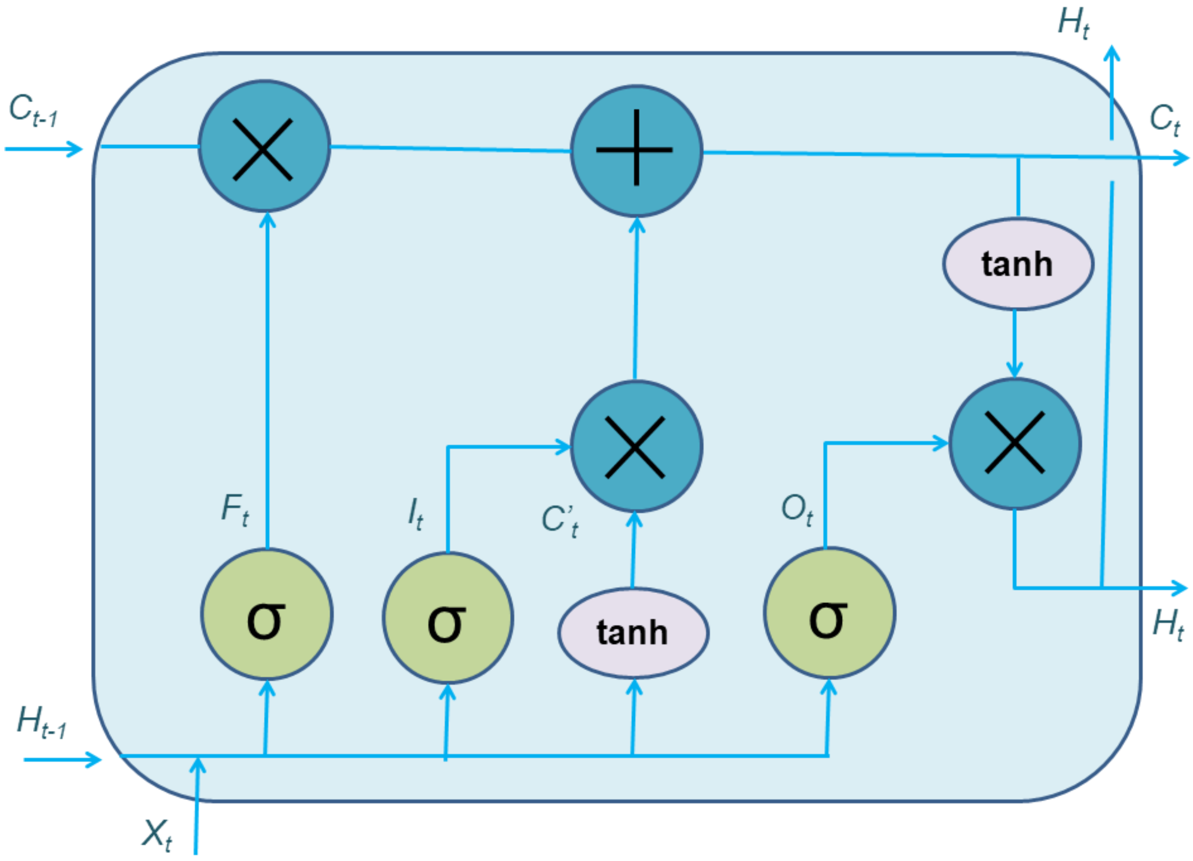


Figure 6. 2 LSTM block architecture.

As illustrated in Figure 6.3, the recent health metrics of SBP, DBP and HR are taken into consideration and constitute the input for the multivariate multi-step LSTM model we developed. The model outputs the prediction of these three health metrics for the next two hours.

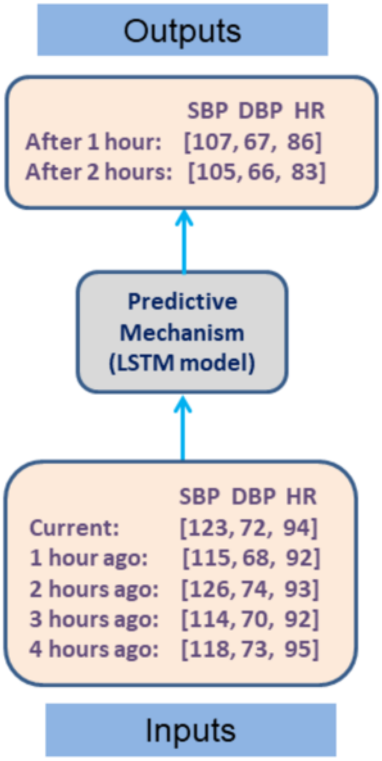

Outputs
SBP DBP HR
After 1 hour: [107, 67, 86]
After 2 hours: [105, 66, 83]
Predictive Mechanism (LSTM model)
SBP DBP HR
Current: [123, 72, 94]
1 hour ago: [115, 68, 92]
2 hours ago: [126, 74, 93]
3 hours ago: [114, 70, 92]
4 hours ago: [118, 73, 95]
Inputs

Figure 6. 3 LSTM model example.

Our predictive LSTM model that we developed for forecasting the output sequences of health metrics is an Encoder-Decoder model of multi-variate input and multi-variate multi-step output. The model is comprised of two sub-models: the encoder and the decoder. Both encoder and decoder comprise their own single layer which consists of 200 LSTM blocks respectively. The model was trained for each patient according to the real dataset from a hospital [31]. The training was based on samples of health metrics of the last four hours and additionally for the next two hours, throughout the health history of a patient. The relation of Loss Function (here the mean squared error) with the number of epochs in the training process is shown in Figure 6.4.

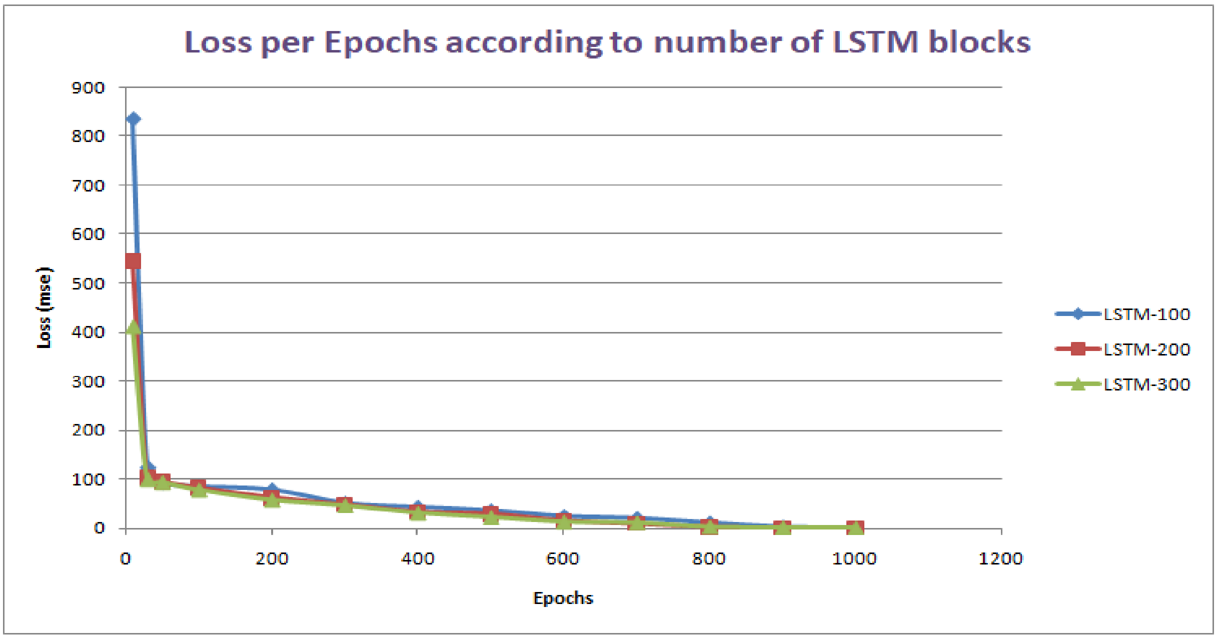


Figure 6. 4 Loss per Epochs according to number of LSTM blocks per layer.

Next, we discuss an example use case in which our proposed system is used to assess the overall health situation of a patient (i.e., its criticality) for driving the access control decision with respect to emergency access to a certain EHR. In our previous work (j1), as analytically described in Chapter 5, we developed a fuzzy context handler which is able to map the input fuzzy variables Systolic Blood Pressure (m1) and Diastolic Blood Pressure (m2) to fuzzy values 'Low', 'Normal', 'Elevated' and 'High', while the input fuzzy variable Heart Rate (m3) to fuzzy values 'Low', 'Medium' and 'High'. Last, the output fuzzy variable Criticality, is mapped to values 'Low', 'Medium' and 'High'.

In a general case, we can have the n health metrics m1 − mn. After having defined the fuzzy sets, the fuzzy rules per fuzzy variable are defined based on our previous work (j1), as analytically described in Chapter 5. An example of a fuzzy rule regarding the SBP is "If SBP is Low then Criticality is High". After this step, the fuzzy inferencing process is implemented, where the percentage of criticality is deduced per health metric.

For example, for the health metrics of SBPcurrent = 123 mmHg, DBPcurrent = 72 mmHg and HRcurrent = 94 bpm, as presented in the current values of the patient with ID 17, shown in Figure 6.3, we deduce the following respective criticalities of: (i) criticality(SBPcurrent = 123 mmHg) = 33%, (ii) criticality(DBPcurrent = 72 mmHg) =

38.61% and (iii) criticality(HRcurrent = 94 bpm) = 63.6%. In this particular example, neither case is critical, because, as stated in our work (j1), as analytically described in Chapter 5, for a case to be critical, it should meet the maximum criticality percentage, which is 67% according to the specific fuzzy inferencing process. Therefore, after having calculated if the current case is critical or not, we proceed to the calculation of the criticality for next two hours. In order to proceed to this particular calculation, we need to have at our disposal the values for the next two hours per each health metric. In order to achieve this goal, we predict these next two hours' health values by implementing LSTM NNs by taking into consideration the last four-hour health history and the current health metrics. This particular prediction is essential for the emergency doctor so that he has at his disposal a thorough perception of the patient's clinical profile, and, additionally, is considered as input for the fuzzy context handlers.

As seen throughout this example, the fuzzy context handlers, by having at their disposal the current health metrics of SBP, DBP and HR, will make the criticality assessment (Figure 6.1) of the respective future health metrics for the next two hours. For example, as seen in Figure 6.3, if the patient, has for the last five hours, the following values, regarding the health metrics of SBP, DBP and HR, respectively: (i) 118 mmHg, 114 mmHg, 126 mmHg, 115 mmHg and 123 mmHg; (ii) 73 mmHg, 70 mmHg, 74 mmHg, 68 mmHg and 72 mmHg; and (iii) 95 bpm, 92 bpm, 93 bpm, 92 bpm and 94 bpm, then our system predicts as their corresponding future two-hour SBP, DBP and HR values, respectively: (i) 107 mmHg and 105 mmHg, (ii) 67 mmHg and 66 mmHg and (iii) 86 bpm and 83 bpm.

After this specific step, we proceed to the criticality calculation of these future health metrics. Therefore, the criticality percentages for the next hour are: (i) criticality(SBPafter-1-h = 107 mmHg) = 60.2%, (ii) criticality(DBPafter-1-h = 67 mmHg) = 67% and (iii) criticality(HRafter-1-h = 86 bpm) = 36.4%. Therefore, in this case, for the next hour we conclude that the situation is critical, because the criticality of at least one of the health metrics case reaches the maximum percentage of 67% according to the fuzzy inferencing process. Therefore, regarding the next two hours' case, we have the following criticality percentages: (i) criticality(SBPafter-2-h = 105 mmHg) = 67%, (ii) criticality(DBPafter-2-h = 66 mmHg) = 67% and (iii) criticality(HRafter-2-h = 83 bpm) = 33%, where we conclude that similarly to the after one hour case the patient's situation is critical because at least one of the criticality percentages reaches its' maximum level.

The overall criticality result is deduced based on the three individual results of the patient's current and future state. In this case, even if regarding the current situation the patient's situation is not considered critical, it is critical for both after one and two hours. The overall critically result is deduced based on the equation (8) of Section 6.2 which states that even one of the current or future states is critical, then in case the requestor is an emergency doctor, he can be granted access to the patient's EHRs.

Our methodology regarding the prediction of the patient's future health metrics is presented in the following Algorithm 1.

Algorithm 1 Prediction of future health metrics.

```
CHOOSE NUMBER OF INPUT STEPS (health history of last 4 h)
    input_steps ← 5
CHOOSE OUTPUT STEPS (future health metrics of the next two hours)
    output_steps ← 2
CHOOSE FEATURES (number of health metrics)
    features ← 3
REPEAT FOR ALL DATA FILES
    READ EACH DATASET'S FILE PER PATIENT
    SELECT TRAIN AND TEST SETS
        data_train, data_test ← devide(dataset, 0.8)
    SPLIT DATA ACCODING TO INPUT AND OUTPUT STEPS
        X_train, Y_train ← split_dataset(data_train, input_steps)
        X_test, Y_test ← split_dataset(data_test, input_steps)
    RESHAPE X_train and X_test
        Reshape X_train, X_test into (samples, inpute_steps, features)
    DEFINE MODEL
        add(LSTM(200, activation = 'relu', input_shape = (input_steps, features)))
        add(RepeatVector(output_steps))
        add(LSTM(200, activation = 'relu', return_sequences = True))
        add(TimeDistributed(Dense(features)))
    COMPILE MODEL
        compile(optimizer = 'adam', loss = 'mse')
    FIT MODEL (to improve the weights and biases of the network)
        model.fit(X_train, Y_train, epochs = 200, verbose = 0)
    EVALUATE MODEL
    SAVE MODEL
        model.save(model_file)
```

```
END REPEAT
INPUT A PATIENT’S HEALTH METRICS FOR THE LAST 4 HOURS METRICS
    input_metrics:
        sbp_current, dbp_current, hr_current current health metrics
        sbp_before_1, dbp_before_1, hr_ before_1 health metrics before 1 h
        sbp_ before_2, dbp_ before_2, hr_before_2 health metrics before 2 h
        sbp_ before_3, dbp_ before_3, hr_before_3 health metrics before 3 h
        sbp_before_4, dbp_before_4, hr_before_4 health metrics before 4 h
PREDICT AND OUTPUT PATIENT’S FUTURE HEALTH METRICS
    output_metrcs:
        sbp_next_1, dbp_next_1, hr_next_1 predicted health metrics after 1 h
        sbp_next_2, dbp_next_2, hr_next_2 predicted health metrics after 2 h
output_metrics ← model_file.predict(input_metrics)
```

C. Evaluation/Validation

1) Technical Implementation

In our previous work (j1) developed and proposed context handlers.

We utilize the XACML architecture to implement the proposed context-based, predictive access control mechanism. XACML also known as a policy-based access control (PBAC) system, where attribute values associated with a resource, an action or a user are perceived as inputs into the access control decision, regarding a given user, a particular target resource and a specific way of access. RBAC can additionally be implemented in XACML as a specialization of ABAC. The XACML architecture contains: (a) the Policy Enforcement Point (PEP), able to protect data and applications, to intercept requests and to propagate authorization requests directed to the Policy Decision Point (PDP); (b) the Policy Information Point (PIP) that connects external attribute sources; and (c) the Policy Administration Point (PAP) responsible for handling access policies.

Policies in ABAC associate attributes, to characterize allowable or not actions, and to grant or deny access to personal information. For instance, when a requestor intends to be granted access to a particular medical information, PDP intercepts her request. PDP evaluates related policies handled by PAP and exploiting attributes retrieved from PIP. ABAC has been used to manage access to EHR platforms [32].

To evaluate our work, we implemented the context-based, predictive access control mechanism based on the XACML architecture and integrated it in EHRServer

[33]. EHRServer is a clinical information management system on the basis of the standard of openEHR [34]. An overview of the integrated system architecture is shown in Figure 6.5. The context handler communicates with the criticality evaluation mechanism, which, after having received the patient's current health metrics, recent health history, age and the prediction of the future health metrics' values for the next two hours, is able to calculate via the inferencing process the criticality level of the patient, by considering her current and future state for the two hours as well.

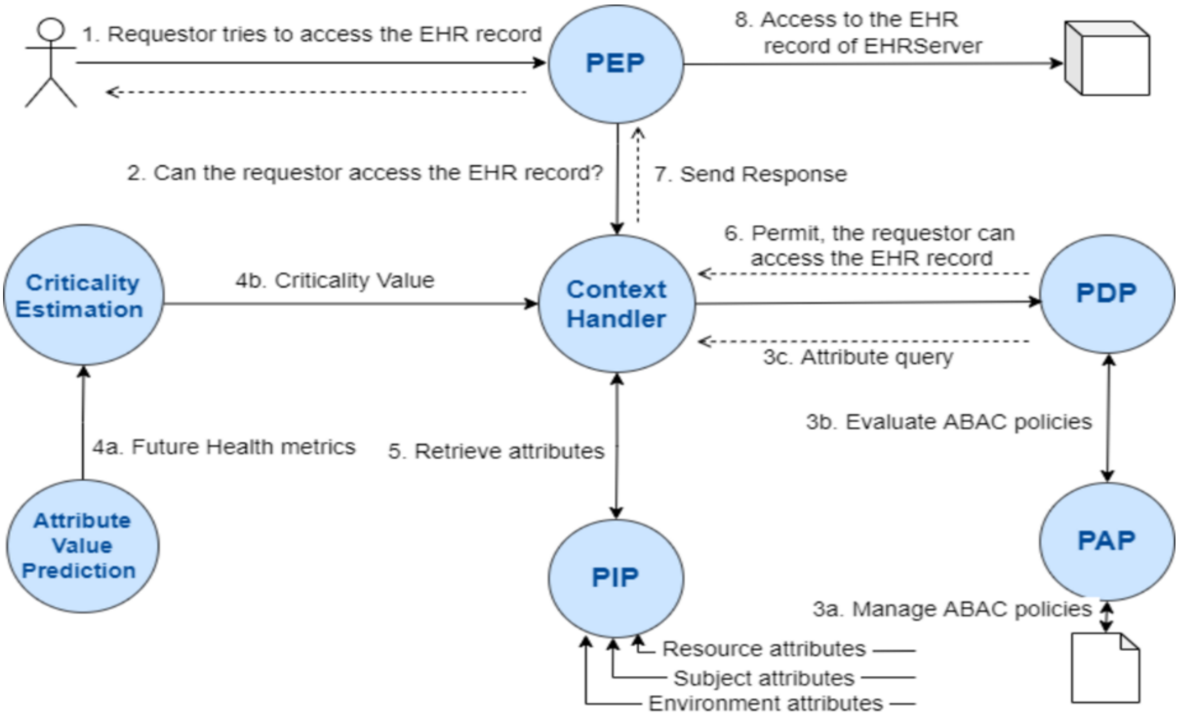
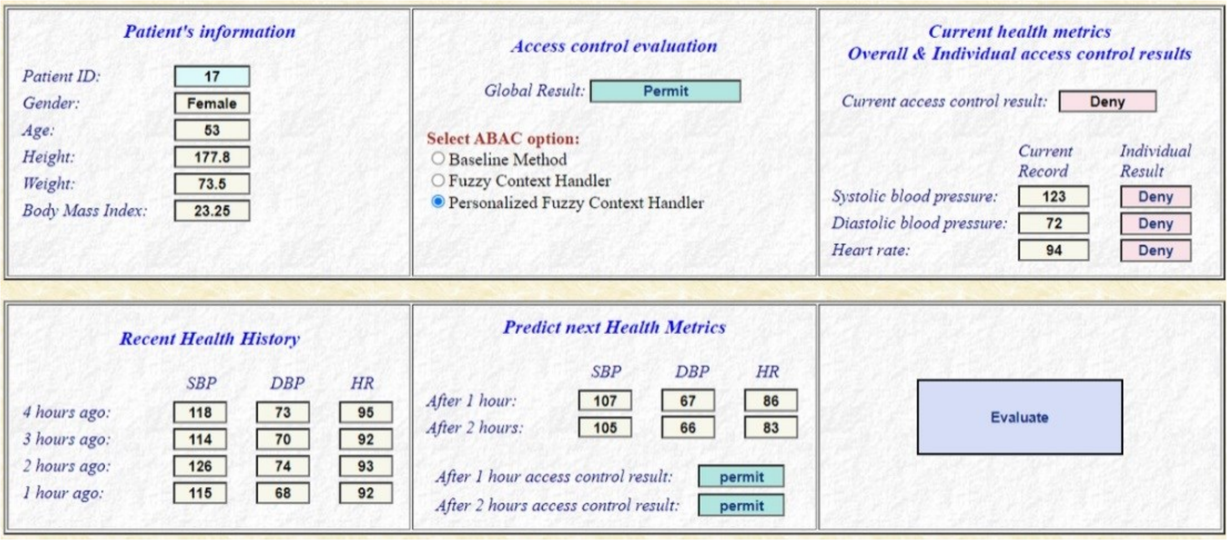

1. Requestor tries to access the EHR record
PEP
8. Access to the EHR record of EHRServer
2. Can the requestor access the EHR record?
7. Send Response
Criticality Estimation
4b. Criticality Value
Context Handler
6. Permit, the requestor can access the EHR record
PDP
3c. Attribute query
3b. Evaluate ABAC policies
4a. Future Health metrics
5. Retrieve attributes
Attribute Value Prediction
PIP
PAP
3a. Manage ABAC policies
Resource attributes
Subject attributes
Environment attributes

Figure 6. 5 Integrated context-based, predictive access control in the XACML Architecture.

We implemented python's tensorflow and keras in order to develop the LSTM RNNs trained model per patient which predicts her future health metrics based on her recent health history. All trained models were integrated in our web user interface (Figure 6.6) so as to output the respective predictions by implementing the trained models and to calculate the respective results per patient on the fly.



Patient's information

Patient ID:	17
Gender:	Female
Age:	53
Height:	177.8
Weight:	73.5
Body Mass Index:	23.25

Access control evaluation

Global Result: Permit

Select ABAC option:

○ Baseline Method
○ Fuzzy Context Handler
● Personalized Fuzzy Context Handler

Current health metrics
Overall & Individual access control results

Current access control result: Deny

	Current Record	*Individual Result*
Systolic blood pressure:	123	Deny
Diastolic blood pressure:	72	Deny
Heart rate:	94	Deny

Recent Health History

	SBP	*DBP*	*HR*
4 hours ago:	118	73	95
3 hours ago:	114	70	92
2 hours ago:	126	74	93
1 hour ago:	115	68	92

Predict next Health Metrics

	SBP	*DBP*	*HR*
After 1 hour:	107	67	86
After 2 hours:	105	66	83

After 1 hour access control result: permit
After 2 hours access control result: permit

Figure 6. 6 Web user interface of context-based, predictive access control.

The web user interface is divided into six panes. In the upper left pane, the patient‘s ID, gender, age, height, weight and BMI are presented, while in the upper center pane, the system’s global access decision is presented. Below this feature, the ABAC selectable options are illustrated, which are the following: (i) the baseline ABAC, which handles basic thresholds as limits so as to permit or not access; (ii) the ABAC non-personalized case, which considers only the fuzzy inferencing process; and (iii) the ABAC personalized case, which considers the fuzzy inferencing process as well as the personalization aspect of age. All the three ABAC methods above take into consideration the SBP, DBP and HR health metrics, as presented in our previous work (j1), as analytically described in Chapter 5, regarding the patient’s diagnosis of present medical status, and we extend it in our current approach by including the patient’s prognosed health metrics after one or two hours by leveraging LSTM NNs. In the upper right pane, the patient’s current health metrics are demonstrated along with the current health status result of the prognostic context handlers case, which has already been selected on the previous pane, as well as the individual access results per health metric regarding the patient’s current status. In the lower left pane, the patient’s current health history within the last five hours is presented. In the lower center pane, our LSTM NN mechanism predicts the health metrics values for the next two hours along with the corresponding access requests by leveraging the fuzzy inferencing system of our previous work (j1), as analytically described in

Chapter 5. Finally, in the lower right pane, there is the button "Evaluate" for the system's decision based on the chosen ABAC case.

2) Evaluation Scenarios and Datasets

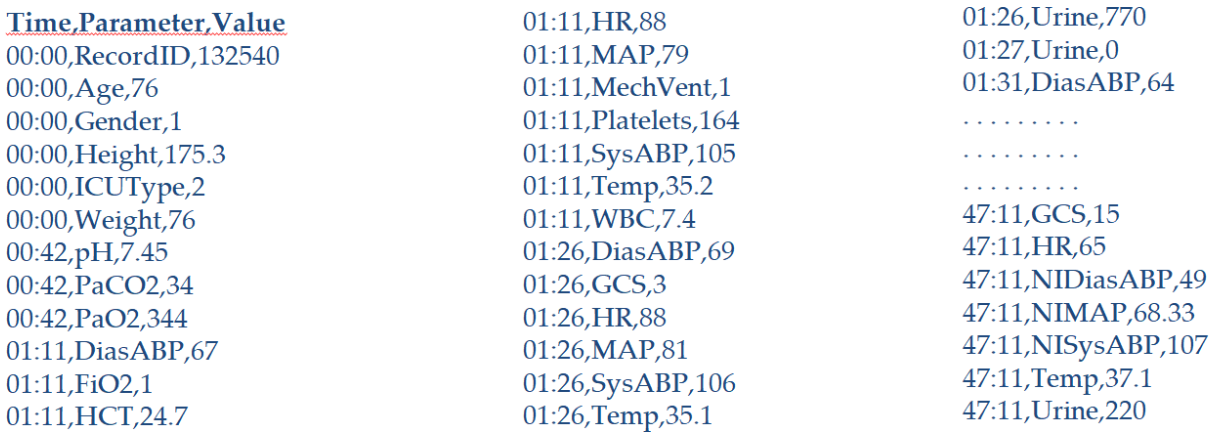
We tested three scenarios as follows: first, access control was handled by the baseline ABAC. In particular, if the requestor is an emergency department (ED) health professional and at least one of the patients' health metrics values is above the suggested threshold, then the patient's situation is critical and, thus, the health professional can have access to the patient's healthcare data. The policy rule is presented as follows:

$$\begin{gathered}
\text{If (requestor} = \text{ED Cilinician) AND} \\
\text{contextual expression (}\mathrm{SBP}_{\mathrm{CURRENT}} > \mathrm{SBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{DBP}_{\mathrm{CURRENT}} > \mathrm{DBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{HR}_{\mathrm{CURRENT}} > \mathrm{HR}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{SBP}_{\mathrm{AFTER\_1\_HOUR}} > \mathrm{SBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{DBP}_{\mathrm{AFTER\_1\_HOUR}} > \mathrm{DBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{HR}_{\mathrm{AFTER\_1\_HOUR}} > \mathrm{HR}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{SBP}_{\mathrm{AFTER\_2\_HOURS}} > \mathrm{SBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{DBP}_{\mathrm{AFTER\_2\_HOURS}} > \mathrm{DBP}_{\mathrm{THRESHOLD}}\ \mathrm{OR} \\
\mathrm{HR}_{\mathrm{AFTER\_2\_HOURS}} > \mathrm{HR}_{\mathrm{THRESHOLD}}) \\
\text{then (Critical Situation)}
\end{gathered} \tag{7}$$

In the second and third scenarios, we modified policy rule (7) with non-personalized and personalized context handlers, respectively. The policy rule now includes the patient's predicted health metrics after one or two hours. (For details about how personalization in context handlers is achieved, please refer to (j1), as analytically described in Chapter 5.)

$$\begin{gathered}\text{If }((\text{requestor} = \text{ED Clinician})\text{ AND}\\ \text{context expression }\;((\text{CRITICAL}_{\text{SITUATION\_CURRENT}}\\ = \text{true})\text{ OR}\\ (\text{CRITICAL}_{\text{SITUATION\_AFTER\_1\_HOUR}} = \text{true})\text{ OR}\\ (\text{CRITICAL}_{\text{SITUATION\_AFTER\_2\_HOURS}} = \text{true})))\\ \text{then }(\text{Critical Situation})\end{gathered} \tag{8}$$

We tested the three scenarios using the publicly available dataset [31], comprising 4000 patients and including one file per patient. Each patient file, among others, includes SBP, DBP and HR health metrics history. These time-series sequential data are taken sporadically every ten minutes, or twenty minutes or even 1 h or more. The raw format of the dataset is shown in Figure 6.7.

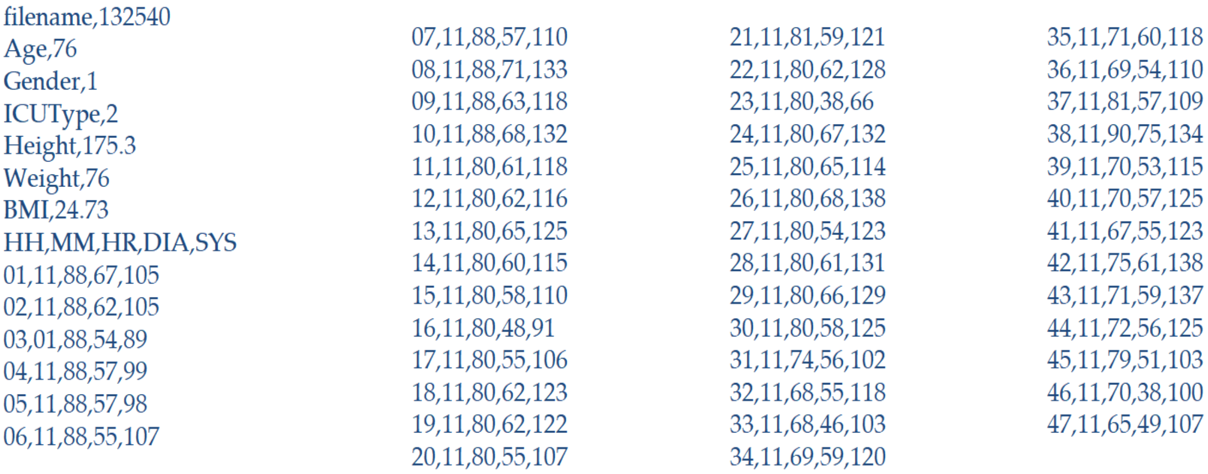


```
Time,Parameter,Value
00:00,RecordID,132540
00:00,Age,76
00:00,Gender,1
00:00,Height,175.3
00:00,ICUType,2
00:00,Weight,76
00:42,pH,7.45
00:42,PaCO2,34
00:42,PaO2,344
01:11,DiasABP,67
01:11,FiO2,1
01:11,HCT,24.7
01:11,HR,88
01:11,MAP,79
01:11,MechVent,1
01:11,Platelets,164
01:11,SysABP,105
01:11,Temp,35.2
01:11,WBC,7.4
01:26,DiasABP,69
01:26,GCS,3
01:26,HR,88
01:26,MAP,81
01:26,SysABP,106
01:26,Temp,35.1
01:26,Urine,770
01:27,Urine,0
01:31,DiasABP,64
. . . . . . . . .
. . . . . . . . .
. . . . . . . . .
47:11,GCS,15
47:11,HR,65
47:11,NIDiasABP,49
47:11,NIMAP,68.33
47:11,NISysABP,107
47:11,Temp,37.1
47:11,Urine,220
```

Figure 6. 7 Initial data file before processing of patient with ID 132540.

The first lines of each file, annotated with time “00:00”, indicate the beginning of the metrics’ recording. The first lines denote the characteristics of each patient including age, gender, height or weight. Subsequent lines contain time-series measurements, recorded in chronological order, and the related timestamps from the beginning of the measurements. These measurements were reported at regular intervals ranging from hourly to daily, or at non-frequent timestamps. The metrics of interest to our study are Systolic Arterial Blood Pressure (SysABP), Diastolic Arterial Blood Pressure (DiaABP) and Heart Rate (HR).

We developed an additional software component to extract the health metrics of every hour, and we excluded all the files that had time gaps more than one hour. An example file is shown in Figure 6.8.



```
filename,132540
Age,76
Gender,1
ICUType,2
Height,175.3
Weight,76
BMI,24.73
HH,MM,HR,DIA,SYS
01,11,88,67,105
02,11,88,62,105
03,01,88,54,89
04,11,88,57,99
05,11,88,57,98
06,11,88,55,107
07,11,88,57,110
08,11,88,71,133
09,11,88,63,118
10,11,88,68,132
11,11,80,61,118
12,11,80,62,116
13,11,80,65,125
14,11,80,60,115
15,11,80,58,110
16,11,80,48,91
17,11,80,55,106
18,11,80,62,123
19,11,80,62,122
20,11,80,55,107
21,11,81,59,121
22,11,80,62,128
23,11,80,38,66
24,11,80,67,132
25,11,80,65,114
26,11,80,68,138
27,11,80,54,123
28,11,80,61,131
29,11,80,66,129
30,11,80,58,125
31,11,74,56,102
32,11,68,55,118
33,11,68,46,103
34,11,69,59,120
35,11,71,60,118
36,11,69,54,110
37,11,81,57,109
38,11,90,75,134
39,11,70,53,115
40,11,70,57,125
41,11,67,55,123
42,11,75,61,138
43,11,71,59,137
44,11,72,56,125
45,11,79,51,103
46,11,70,38,100
47,11,65,49,107
```

Figure 6. 8 Data file after processing of patient with ID 132540.

After data pre-processing, 2086 patient files remained. For each patient, a trained prediction model was developed and used for the prediction of the criticality for the next couple of hours.

3) ***Results***

Table 6.1 presents the error in criticality prediction after one and two hours, for the three previously-mentioned cases of: (i) baseline ABAC method, (ii) ABAC with non-personalized fuzzy context handler and (iii) ABAC with personalized context handler as described in our previous work (j1), as analytically described in Chapter 5.

Table 6. 1 Error of the predicted criticality.

Access Control Case	Criticality Prediction Error
ABAC with Personalized Fuzzy context handler.	6.86%
ABAC with non-Personalized Fuzzy context handler.	17.31%
Baseline ABAC.	17.74%

The total number of patients whose future health state is falsely predicted per ABAC case is calculated using Formula (9). This number comprises the patients who are: (i) in non-critical state based on both of the predictions of the next two hours, but in a critical situation based on the real next two-hour situation where at least one the situations of the next two hours is critical, and (ii) in critical state based on at least one of the next two hours prediction, but in a non-critical situation based on both health states of the real next two hours. Formula (10) computes the falsely predicted criticality percentage (criticality prediction error).

$$\begin{aligned}&\text{Number\_of\_Patients\_Total\_Error} = \text{Number of patients where contextual expression } (((\text{CRITICAL}_{\text{PREDICTED\_SITUATION\_AFTER\_1\_HOUR}} = \text{false AND} \\ &\text{CRITICAL}_{\text{PREDICTED\_SITUATION\_AFTER\_2\_HOURS}} = \text{false) AND} \\ &(\text{CRITICAL}_{\text{REAL\_SITUATION\_AFTER\_1\_HOUR}} = \text{true OR} \\ &\text{CRITICAL}_{\text{REAL\_SITUATION\_AFTER\_2\_HOURS}} = \text{true)) AND} \\ &((\text{CRITICAL}_{\text{PREDICTED\_SITUATION\_AFTER\_1\_HOUR}} = \text{true OR} \\ &\text{CRITICAL}_{\text{PREDICTED\_SITUATION\_AFTER\_2\_HOURS}} = \text{true) AND} \\ &(\text{CRITICAL}_{\text{REAL\_SITUATION\_AFTER\_1\_HOUR}} = \text{false AND} \\ &\text{CRITICAL}_{\text{REAL\_SITUATION\_AFTER\_2\_HOURS}} = \text{false)))}\end{aligned} \tag{9}$$

$$\text{Criticality\_Prediction\_Error} = \frac{\text{Number\_of\_Patients\_Total\_Error}}{\text{Number\_of\_all\_patients}} * 100 \tag{10}$$

The criticality prediction in the ABAC with personalized context handler case exhibits the lowest percentage error (6.86%) while the corresponding errors of the ABAC with non-personalized context handler and the baseline method are 17.31% and 17.74%, respectively.

Chapter 7

7. Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records

A. *Motivation*

1) Introduction

Access control to healthcare data is vital as the protection of the patient's sensitive data privacy, e.g. the health history, is of great importance. Access control models are associated with the rights an entity has upon managing particular data objects. These are based on user identity access control models, such as Role-Based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [1]. Contrarily to these static approaches, the Attribute-Based Access Control (ABAC) paradigm has been introduced, which is dynamic in nature [2]. In ABAC, there are connections' snapshots that are produced and dynamically altered based on the current context, instead of statically-defined lists of permissions that link entities with objects.

As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient's health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. A major challenge in this area is to enable trustworthiness and to achieve traceability of access control to personal health data in emergency situations.

In our previous work (j2), as analytically described in Chapter 6, we applied machine learning methods to the patient's recent health history so as to predict key health metrics of the next couple of hours and used the predicted values to evaluate the criticality of the patient's medical state with fuzzy logic (j1), as analytically described in Chapter 5. The research objective of our work is to develop a proactive access control method that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party. We build a proactive access control mechanism within the blockchain system that exploits smart contracts of our private and permissioned Hyperledger Fabric-based blockchain network, which, based on our predictive model, and combined with our personalized fuzzy approach, examines recent health metrics of a patient and outputs the patient's health criticality assessment, effectively managing access to the patient's EHRs.

2) ***Blockchain technologies in the medical sector***

Blockchain based technologies implemented in the medical sector hold various benefits, but also many challenges as well regarding the acceptance by the medical community. Even if the technology of blockchain has benefits such as system performance, collaborative ecosystem, or innovative technological features, its applications in healthcare are in their early stage [3]. The perceptions of the individual issues such as the lack of knowledge, the organizational issues such as the implementation, the technological issues such as the blockchain model types, and market-related issues such as regulatory concerns indicate that blockchain-based applications in healthcare constitute an emerging field. This study points out the practical implications and thus is capable to assist developers and medical managers in identifying possible issues in implementing, developing, and planning blockchain-based health information exchange systems. According to the author, tackling these barriers can assist the widespread usage of blockchain-based health information exchanges in various medical settings and facilitate connectivity and interoperability in community and regional health information networks. Additionally, barriers of acceptance include among others, usability constraints, lack of management commitment, lack of a security-oriented culture, lack of awareness regarding legislations and health information technology risks [4]. Nevertheless, blockchain is being explored by stakeholders to enable better use of healthcare-related data, enhance compliance, improve patient outcomes, lower costs, and optimize business processes [5]. Nonetheless, in assessing if blockchain can fulfill the hype of a technology described as disruptive and revolutionary, it is important to ensure that blockchain design elements take under consideration the actual medical needs of regulators, providers, patients, and consumers. It is worth mentioning that the authors point out that the most praiseworthy advantages of blockchain are yet to be realized. However, the efforts of blockchain pilots will finally lead to the promise of patient-driven medical systems in the form of open health data markets and precision medicine, finally reaching the patient.

3) ***Hyperledger Fabric Blockchain Platform***

Hyperledger Fabric is an open source enterprise-based permissioned distributed ledger technology platform, designed for utilization in business contexts, which delivers key differentiating capabilities over other popular blockchain platforms. The Hyperledger Fabric project is governed by maintainers of multiple organizations and has a configurable and modular architecture, enabling optimization, versatility and innovation for several industry use cases such as healthcare, or banking. Fabric is the first distributed ledger platform which supports smart contracts authored in general-purpose programming languages such as Node.js, Go and Java, instead of constrained domain-specific languages. Fabric platform is additionally permissioned, which means that, contrary to a public permissionless network, the users are known to one another, instead of anonymous and thus fully untrusted. More specifically, even if the participants may not entirely trust each other, a network can be operated under a governance model which is constituted of what trust does exist among users, like a legal agreement or framework for managing disputes. Fabric is able to utilize consensus protocols which don't require a native cryptocurrency to fuel smart contract execution or to incent costly mining.

Hyperledger's first project, Fabric, is a permissioned blockchain platform. It operates similarly to most blockchains, which maintains a ledger of digital events. The ledger events are structured as transactions and shared among users. These transactions are executed without a cryptocurrency, and are confidential, private, and secured. Fabric is able to exclusively be updated by consensus of the participants. At the time the records have been inputted, they cannot be modified. Fabric is a solution, focused on compliance with regulations and scalability. Each user must register proof of identity to membership services so as to yield system's access.

B. Methods and Tools

1) Proactive Access Control Mechanism

In this section, we describe how we extend our previous works on context-aware access control policies in healthcare (c3), as analytically described in Chapter 12, by considering context-aware access policies for identifying the patient's current situation (j1), as analytically described in Chapter 5, and predicting the patient's future state based on the resent health history of the last five hours (j2), as analytically described in Chapter 6, where the data regarding the recent health history, were obtained from the publicly available online database [6]. We couple the proactive access control mechanism (j1), as analytically described in Chapter 5, with a private and permissioned blockchain network by leveraging the Hyperledger Fabric blockchain platform.

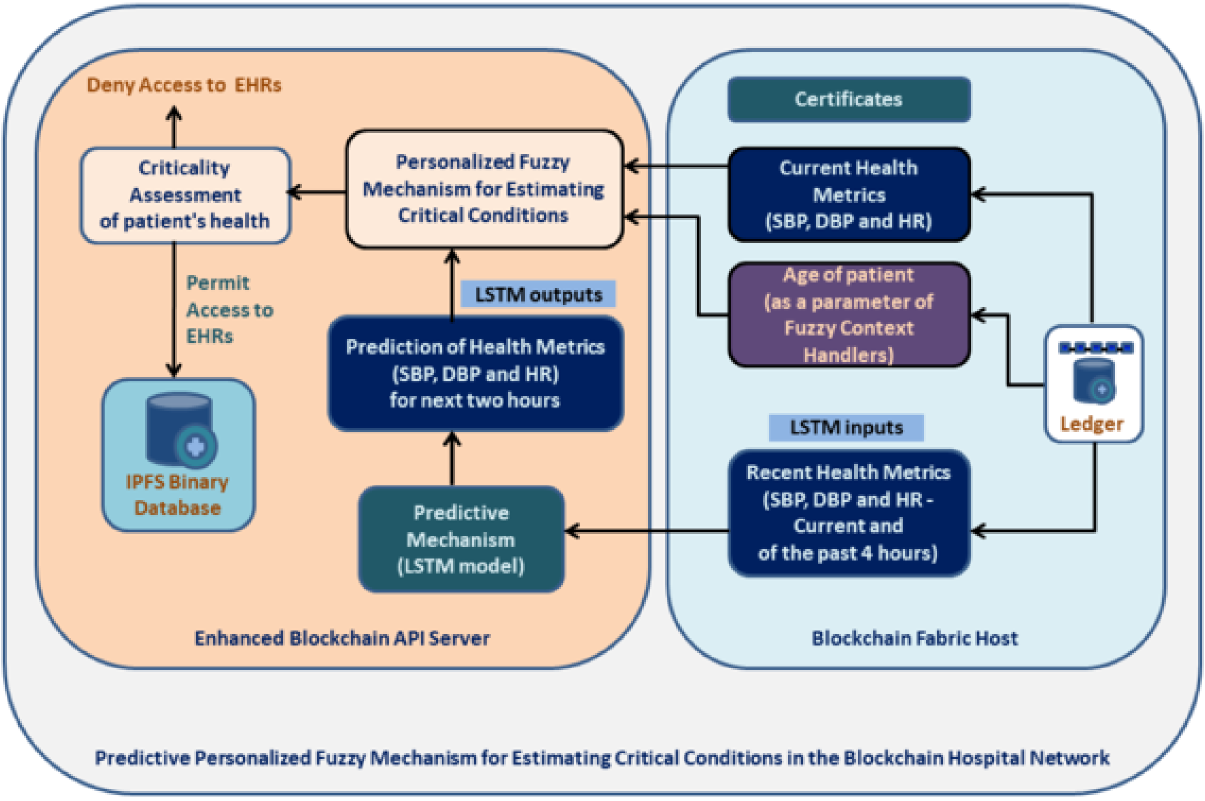
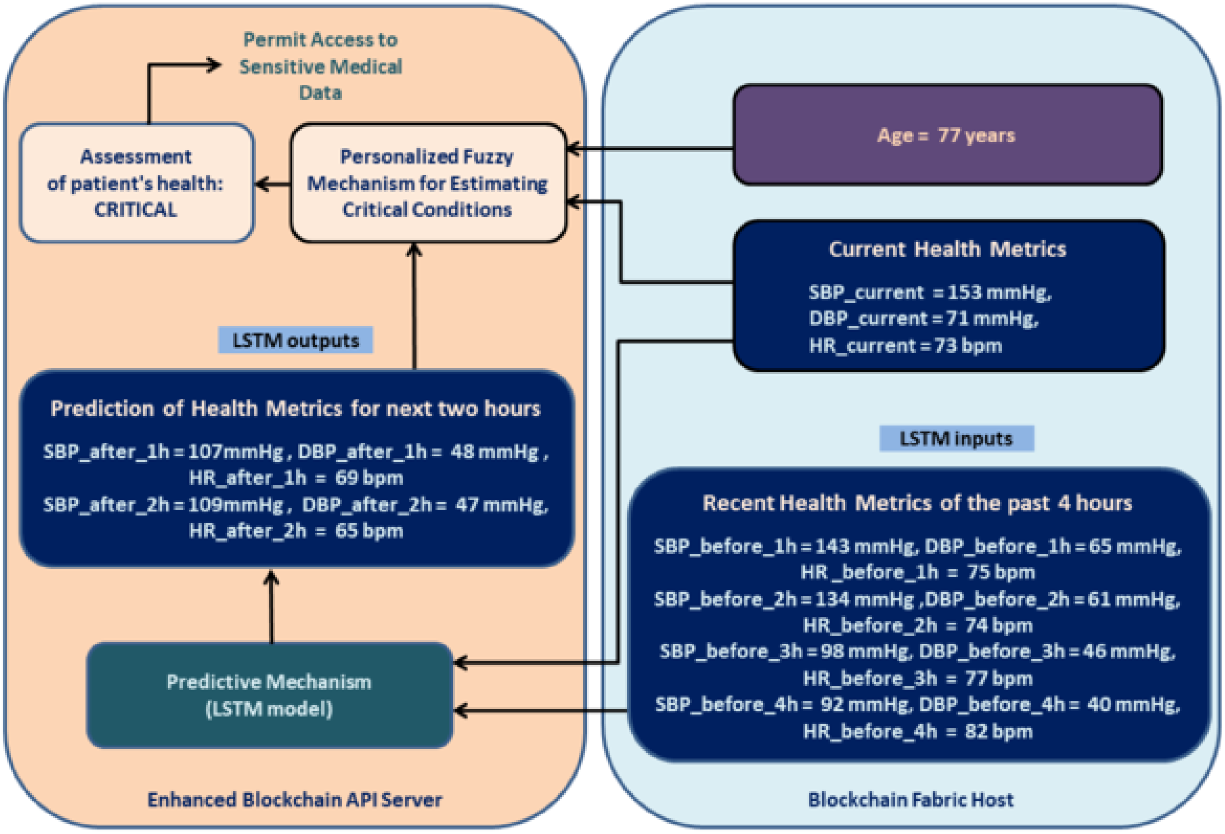

Deny Access to EHRs
Criticality Assessment of patient's health
Personalized Fuzzy Mechanism for Estimating Critical Conditions
Permit Access to EHRs
LSTM outputs
Prediction of Health Metrics (SBP, DBP and HR) for next two hours
IPFS Binary Database
Predictive Mechanism (LSTM model)
Enhanced Blockchain API Server
Certificates
Current Health Metrics (SBP, DBP and HR)
Age of patient (as a parameter of Fuzzy Context Handlers)
Ledger
LSTM inputs
Recent Health Metrics (SBP, DBP and HR - Current and of the past 4 hours)
Blockchain Fabric Host
Predictive Personalized Fuzzy Mechanism for Estimating Critical Conditions in the Blockchain Hospital Network

Figure 7. 1 Conceptual Approach

The proactive mechanism (Figure 7.1) queries the ledger of the blockchain, where the history of these metrics' transactions are stored. It receives the current health metrics of Systolic Blood Pressure (SPB), Diastolic Blood Pressure (DBP), and Heart Rate (HR), along with the same health metrics of the past four hours, and after predicting the health metrics for the next two hours, it forwards the results to the fuzzy mechanism for assessing the criticality of the patient's situation. The mechanism receives the current heath metrics (SBP, DBP, and HR) from the ledger along with parameter of patient's age and it makes a decision about the criticality of the patient's health, by taking into consideration both the current and the predicted health metrics. Afterwards, if the assessment of patient's health is "Critical", the access to the medical binary database is permitted, else the access to patient's sensitive private health metrics is prohibited. This binary database, is an off-chain InterPlanetary File System (IPFS) [7], where each file's encrypted data are stored in multiple nodes, in case of large file volumes.



Permit Access to Sensitive Medical Data
Assessment of patient's health: CRITICAL
Personalized Fuzzy Mechanism for Estimating Critical Conditions
Age = 77 years
Current Health Metrics
SBP_current = 153 mmHg,
DBP_current = 71 mmHg,
HR_current = 73 bpm
LSTM outputs
Prediction of Health Metrics for next two hours
SBP_after_1h = 107mmHg , DBP_after_1h = 48 mmHg ,
HR_after_1h = 69 bpm
SBP_after_2h = 109mmHg , DBP_after_2h = 47 mmHg,
HR_after_2h = 65 bpm
LSTM inputs
Recent Health Metrics of the past 4 hours
SBP_before_1h = 143 mmHg, DBP_before_1h = 65 mmHg,
HR_before_1h = 75 bpm
SBP_before_2h = 134 mmHg ,DBP_before_2h = 61 mmHg,
HR_before_2h = 74 bpm
SBP_before_3h = 98 mmHg, DBP_before_3h = 46 mmHg,
HR_before_3h = 77 bpm
SBP_before_4h = 92 mmHg, DBP_before_4h = 40 mmHg,
HR_before_4h = 82 bpm
Predictive Mechanism (LSTM model)
Enhanced Blockchain API Server
Blockchain Fabric Host

Figure 7. 2 Illustrative Example.

A numeric example of the functionality of the mechanism is illustrated in Figure 7.2. The example is a case study of a 77 year old patient with his health metrics (SBP, DBP, and HR) of the past four hours, as illustrated. In this example, the overall criticality result is deduced dependent on the three individual results of the patient's current and future status. In this case, even if based on the current situation the patient’s condition is not deemed critical, it is critical for both after one and two hours. The overall critically result is deduced based on the equation (2) which states that even one of the current or future situations is critical, then if the requestor belongs in the emergency team, he can be granted access to the patient’s sensitive EHRs.

C. *Evaluation/Validation*

1) *Implementation*

a) *Architecture of Blockchain-based Access Control Mechanism*

In Figure 7.3 the architecture of blockchain-based access control mechanism is illustrated. The certificates administrator issues and grants a personal identity card which includes the credentials, the role, and the digital signature of each specific user. In case of an emergency incident, a certified user, e.g. a member of the emergency team, by using this identity card by a client application, requests access to a patient’s sensitive medical data (IPFS database). Then the identification control of “Enhanced Blockchain Application Programming Interface (API) Server” confirms the user’s identity features and rejects or proceeds the request accordingly. In case of successful identification the request proceeds to the predictive personalized fuzzy mechanism for estimating critical situations, and triggers the relating algorithm of personalization. Finally, if the ultimate estimation about the patient’s health is not critical then the request if finally rejected. On the contrary, if the ultimate estimation is critical then the requestor is granted access to IPFS database.

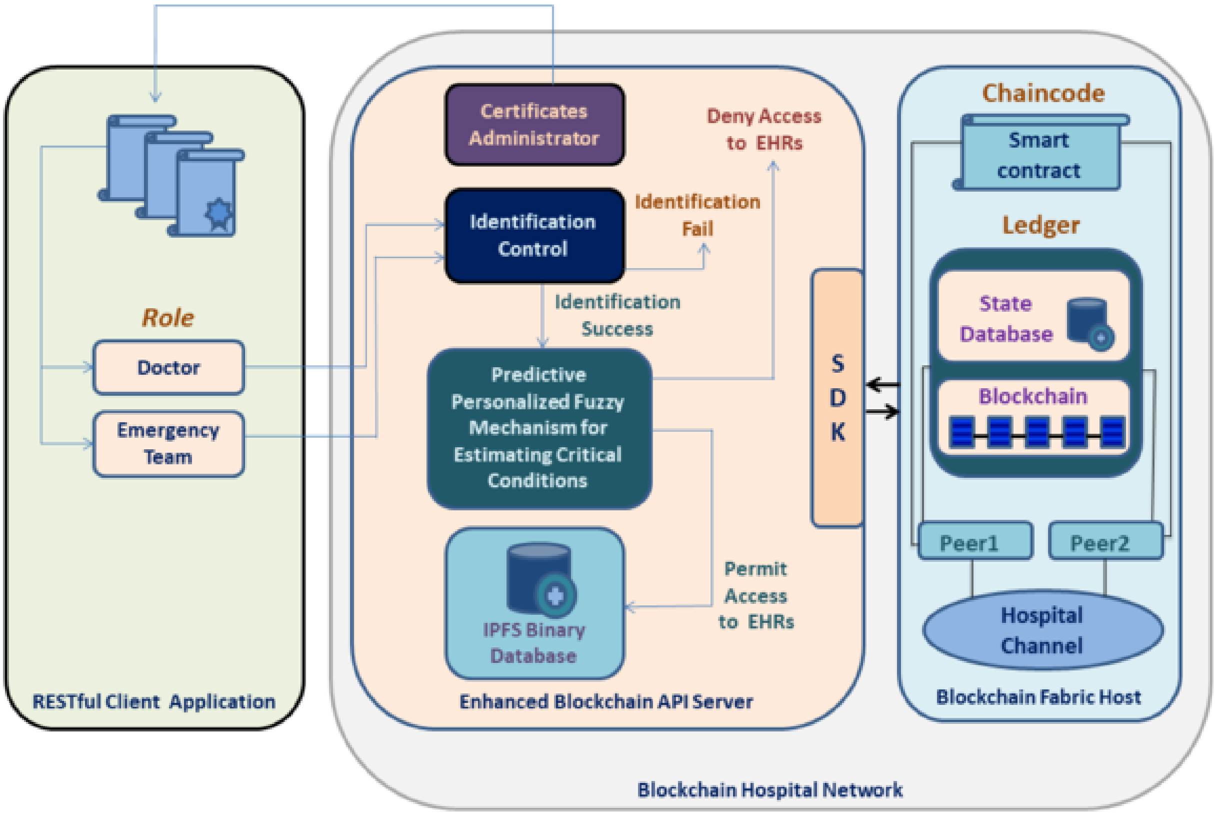


Figure 7. 3 Architecture of Blockchain-based Access Control Mechanism.

b) *Technical Implementation*

Hyperledger Fabric doesn't have by default its own API Server in order to communicate with front-end applications, so we had to create an appropriate one, incorporated in the "Blockchain Network". An overview of the integrated system architecture is shown in Figure 7.4. At the right, the "Blockchain Hospital Network" is illustrated which runs in Linux operating system and consists of the following two sub-components: i) "Blockchain Fabric Host" and ii) "Enhanced Blockchain API Server". Specifically, the "Blockchain Fabric Host" contains: a) the "Hospital Channel" which services the users of the network, b) the "Smart contract" where the rules of transactions are defined, and c) the ledger where the transactions are recorded. The changes in the health metrics (SBP, DBP, and HR) of patients are always registered as transactions in the ledger, and thus, we can query all patients' health history from the ledger. Respectively, the "Enhanced Blockchain API Server" i) incorporates all the rules of the smart contract, ii) runs the blockchain network and handles the appropriate user certificates of blockchain network, iii) encompasses our "Predictive Personalized Fuzzy Mechanism for Estimating Critical Conditions", and iv) provides and handles the communication between our "RESTful Client Application" with the "Blockchain Fabric Host". Additionally, at the left we see our "RESTful Client Application", which runs in Windows operating system, communicates with the blockchain network, and sends the adequate access control request and receives the respective response.

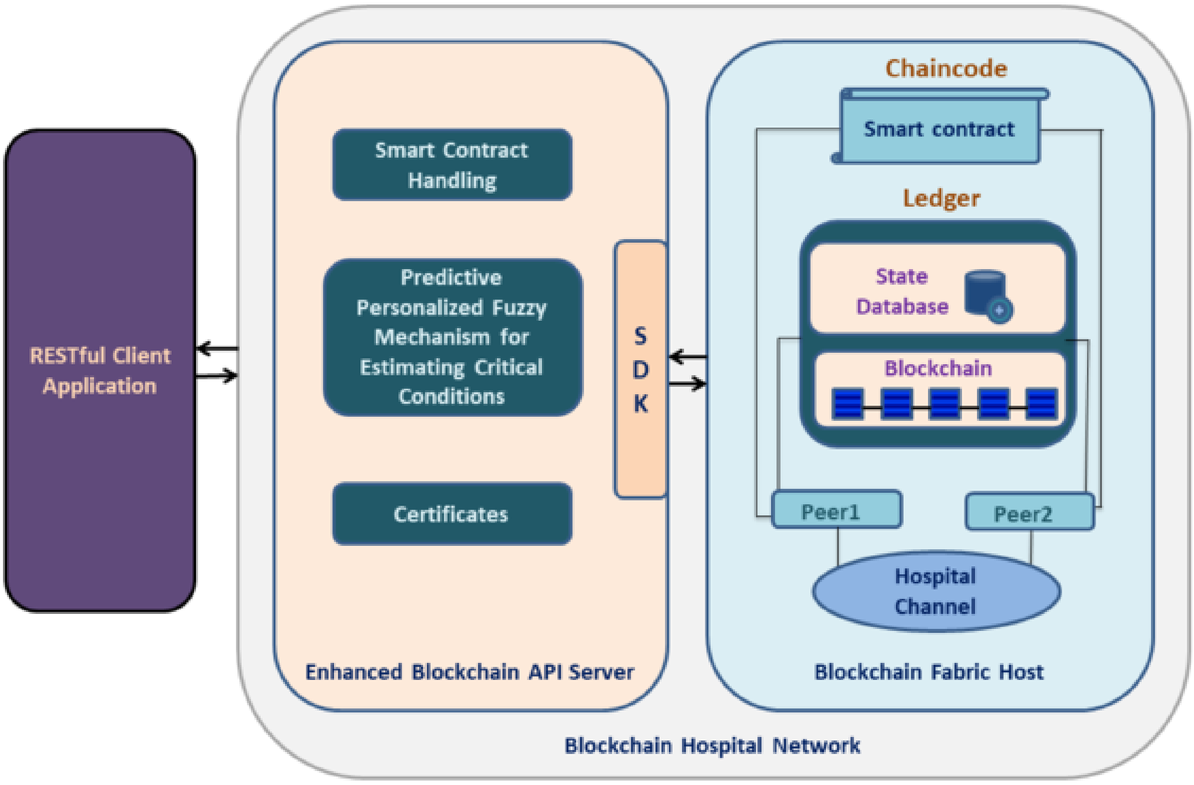

RESTful Client Application
Smart Contract Handling
Predictive Personalized Fuzzy Mechanism for Estimating Critical Conditions
Certificates
S D K
Enhanced Blockchain API Server
Chaincode
Smart contract
Ledger
State Database
Blockchain
Peer1
Peer2
Hospital Channel
Blockchain Fabric Host
Blockchain Hospital Network

Figure 7. 4 Blockchain Implementation (Custom API and Fabric Server).

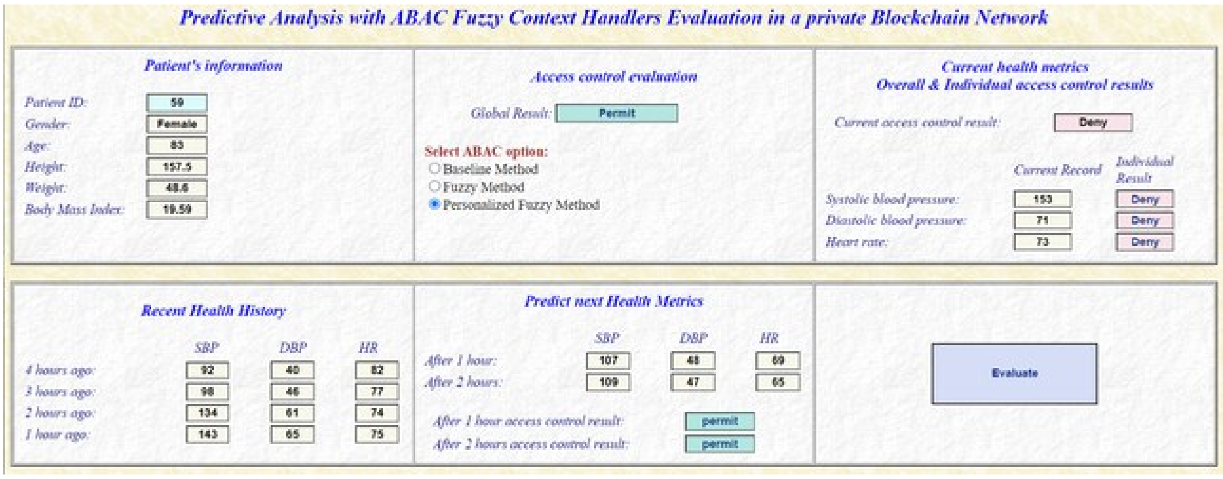
Contextual policies utilize context attributes to characterize allowable or not access requests and to permit or deny access to private information. Specifically, when a user requests access to specific healthcare data, the policy–based access control mechanism evaluates the related contextual policies exploiting attributes. In our current research, we encompass the context-based, predictive access control mechanism of our previous work (j2), as analytically described in Chapter 6, in the Hyperledger Fabric platform, so as to enrich the blockchain network.

If a requestor who belongs in the emergency team needs to submit a query along with her appropriate credentials, in order to access the recent health history of a specific patient, and if the “Enhanced Blockchain API Server” deduces that the patient is indeed in danger, then the person who handles the front-end application receives in the “RESTful Client Application” is sent the patient’s personal information as well as recent health history.

The several methods, which handle the read or write rights to the ledger of blockchain fabric hosts, are handled by the smart contract, which is known as chaincode. The smart contract of the blockchain fabric host is responsible for granting read or write access to the ledger along with implementing suitable related queries on its’ data. The “Smart Contract Handling” mechanism of the “Enhanced Blockchain API Server” encapsulates the smart contract rules and is integrated with the predictive, personalized fuzzy mechanism so as evaluate the criticality of the patient’s health by considering her current and predicted future health metrics, as well.

In case the access control response which has been sent to our client application is “Permit”, then the requestor is granted access to patient’s sensitive medical data and the patient’s respective information is illustrated to the appropriate panes, as explained analytically in Figure 7.5, so that the user such as the emergency doctor has a thorough initial view.

To build the LSTM RNNs trained model, we implemented components of tensorflow and keras in Linux. All trained models are integrated in our “Enhanced Blockchain API Server”, so as to calculate on the fly the health metrics predictions by the corresponding incorporated trained neural network model per patient.



Predictive Analysis with ABAC Fuzzy Context Handlers Evaluation in a private Blockchain Network

Patient's information

Patient ID: 59
Gender: Female
Age: 83
Height: 157.5
Weight: 48.6
Body Mass Index: 19.59

Access control evaluation

Global Result: Permit

Select ABAC option:
○ Baseline Method
○ Fuzzy Method
● Personalized Fuzzy Method

Current health metrics
Overall & Individual access control results

Current access control result: Deny

	Current Record	Individual Result
Systolic blood pressure:	153	Deny
Diastolic blood pressure:	71	Deny
Heart rate:	73	Deny

Recent Health History

	SBP	DBP	HR
4 hours ago:	92	40	82
3 hours ago:	98	46	77
2 hours ago:	134	61	74
1 hour ago:	143	65	75

Predict next Health Metrics

	SBP	DBP	HR
After 1 hour:	107	48	69
After 2 hours:	109	47	65

After 1 hour access control result: permit
After 2 hours access control result: permit

Figure 7. 5 RESTful client application, for communication with the blockchain network, for contextual predictive access control.

The RESTful client application comprises six panes (Figure 7.5). In the upper left pane, the patient‘s Body Mass Index (BMI), weight, height, age, gender, and ID are demonstrated, whereas in the upper center pane, the overall access result is demonstrated. Below this component, the access control selectable options are illustrated, which are the following: i) the baseline method, which considers basic thresholds as limits in order to grant access; ii) the non-personalized method, which considers only the fuzzy inferencing process; and iii) the personalized method, which takes into account the fuzzy inferencing process and the personalization aspect of age. All the three already mentioned access control cases consider the health metrics of SBP, DBP and HR, based on the patient’s diagnosis of present medical status. In the upper right pane, the patient’s current health metrics are presented as well as the current medical state result of the prognostic access control case, which has already been checked on the previous pane, along with the individual access results per health metric referring to the patient’s current medical state. In the lower left pane, the patient’s recent medical history within the last five hours is demonstrated. In the lower center pane, the LSTM NNs mechanism predicts the health metrics’ values for the following two hours as well as the respective access requests by using the fuzzy inferencing system (j1), as analytically described in Chapter 5. Finally, in the lower right pane, the button ‘Evaluate’ provides the system’s decision according to the chosen access control case.

2) Evaluation

a) Evaluation Scenarios and Datasets

We tested the three predictive scenarios of baseline method, personalized fuzzy method, and personalized fuzzy method which inference the criticality of patient’s health state. More information about how all three methods are implemented can be found in (j2), as analytically described in Chapter 6. In this work, in all three scenarios the requestor is a member of the emergency medical team and wants to have an immediate and privileged access to sensitive data of a patient who is probably is a critical situation. The whole access control policy rules are implemented as follows in equation (1) and equation (2).

$$\begin{gathered}\text{If (((role\_of\_requestor = "Doctor") OR} \\ \text{(role\_of\_requestor = "Emergency Team")) AND} \\ \text{(requestor\_credentials = "Valid"))} \\ \text{then (Identification Success)}\end{gathered} \tag{1}$$

$$\begin{gathered}\text{If ((Identification Success) AND} \\ \text{context expression ((}\mathrm{CRITICAL}_{\mathrm{SITUATION\_CURRENT}} = \text{true) OR} \\ \text{(}\mathrm{CRITICAL}_{\mathrm{SITUATION\_AFTER\_1\_HOUR}} = \text{true) OR} \\ \text{(}\mathrm{CRITICAL}_{\mathrm{SITUATION\_AFTER\_2\_HOURS}} = \text{true)))} \\ \text{then (Critical Situation)}\end{gathered} \tag{2}$$

In this work we tested the three scenarios utilizing the public dataset [6], including four thousand patients and comprising one file per patient. Each patient file, among others, includes SBP, DBP and HR health metrics history. These time-series sequential data are taken sporadically every ten minutes, or twenty minutes or even one hour or more. We built an additional software component, in (j2), as analytically described in Chapter 6, to extract the health metrics of every hour, and we excluded all the files that had time gaps more than one hour. For more information regarding the data pre-processing, please refer to (j2), as analytically described in Chapter 6. In this research we integrated the health metrics data used in our previous work (j2), as analytically described in Chapter 6, by incorporating their health metric values in the smart contract as initial values. More particularly, we inserted programmatically the EHRs per patient, in adequate format in the smart contract file. We handle this file in Go programming language, which is the default language for creating the smart contracts in Hyperledger Fabric.

b) *Evaluation Results*

We measured the response time of the system from the moment an emergency team member, by communicating with API server using the client application, asks permission to access the patient's sensitive medical data, until he is finally granted this access or not, which is considered as a query transaction. This response time of committing a query transaction so that the "Enhanced Blockchain API Server" responds to the RESTful client application in milliseconds (ms) is demonstrated in Table 7.1. Three cases are taken under consideration. In the first case we examine the "Non-Predictive Personalized Fuzzy Method" of our previous work (j1), as analytically described in Chapter 5, where only the fuzzy mechanism is integrated in the blockchain network, by considering only the current situation and without taking into consideration the prediction of the patient's future state. In the second case, we examine the "Predictive Personalized Fuzzy Method - with trained LSTM models" where the LSTM models we use for the prediction are trained in advance by using a considerable amount of data, and are then implemented in the predictive mechanism for the evaluation. In the third case, we examine the "Predictive Personalized Fuzzy Method - with training LSTM models" where these models are trained by the whole amount of available data, "on the fly" at the exact moment of the access request and they are right away implemented and incorporated in the predictive mechanism which proceeds to the estimation of the patient's state. We deduce from Table 7.1 that the first blockchain access control case of the "Non-Predictive Personalized Fuzzy Method" has the shortest response time for committing a query transaction, while the third case of the "Predictive Personalized Fuzzy Method - with training LSTM models" corresponds to the longest response time. To our knowledge not a scientific work was published up till now that incorporates predictive fuzzy techniques in estimating a patient's critical health state in order to provide access control on a blockchain network system and thus there is not time comparison with similar access control cases. Nevertheless, our mechanism enhances trustworthiness and achieves traceability of access control to personal health data in emergency situations. Our work could contribute to the review work of Sookhak et al.

[8] by introducing the latency due to the integration of a predictive fuzzy personalized mechanism within the hyperledger-based blockchain network.

Table 7. 1 Latency for committing a query transaction to our client application from the blockchain network per access control case.

Blockchain Access Control Case	Time (ms)
Non-Predictive Personalized Fuzzy Method (integrating the fuzzy mechanism, without the LSTM prediction)	1887
Predictive Personalized Fuzzy Method (with trained LSTM models)	5104
Predictive Personalized Fuzzy Method (with training LSTM models)	14736

3) Discussion

a) Access Control Schemes in Critical Medical Conditions

Yielding access to patient's medical information constitutes a sensitive concept due to the fact that there is the danger for patient's private information to be exposed to malicious subjects. Granting access to EHRs in critical conditions improves medical decision-making and increases the quality of patient's life [9]. Povey et al. [10] suggest a retrospective access control method so that the system isn't misused, and where transactions are used to assure the integrity of the system is able to be recovered during a data breach case. The authors suggest an informative break-glass approach regarding misuse before its activation. They state that in an emergency case, the users are able to operate the tool but, after the event, they must inform the system's administrator to avoid a penalty.

Saberi et al. [11] present a synthesis of IPFS with blockchain technology. Blockchain is used as a secure incorporated system for ABAC break-glass mechanisms, and as an IPFS that creates a distributed file storage infrastructure to store big files of medical data. Furthermore, the conceptual model of Saberi et al. [12] was based on the blockchain technology, on an IPFS and on ABAC, that doesn't necessitate circumventing the access control system so as to constitute the patient's healthcare data. Particularly in emergencies, the medical professionals are permitted access to the EHRs in time based on the attribute-related security rights that are decided by the patients.

Manasa et al. [13] introduced an access control scheme for patient-centric privacy regarding medical data in critical states. The model of Tsegaye et al. [14] assures the EHRs confidentiality based on ABAC and RBAC, whereas ensuring integrity by the exploitation of Clark–Wilson model for safeguarding the EHRs from both unauthorized entities and authorized medical professionals. Additionally, by implementing their paradigm, the EHRs are protected and any access problems are dealt with whereas yielding access of medical records in emergencies.

Farinha et al. [15] introduced an implementation of the break-glass paradigm in a real life scenario to enhance the legislation regarding genetics. In addition to this, the authors evaluated the process of encompassing legislation into the healthcare practice and the impact of break-glass usage by reaching a consensus that the break - glass features were able to filter the non-authorized accesses that wouldn't be prevented otherwise. Georgakakis et al. [16] created the spatio-temporal Emergency RBAC scheme dependent on spatiotemporal context of location, time, and roles' hierarchy to grant exception access in emergencies. In their scheme, users are able to access resources either through the common process of assigned roles based on the security policy of the organization or demand access to a resource through the emergency access procedure.

Marinovic et al. [17] suggested a break-glass paradigm which builds a break-glass policy by determining the reason why the access wasn't granted. Their scheme represented missing and conflicting data, allowing the policy to produce a more informed decision when faced with inconsistent or missing knowledge. Maw et al. [18] introduced an access control scheme, in networks of body area and wireless sensor networks that supports a flexible emergency access control of accessing data. Guan et al. [19] suggested a paradigm leveraging the patients' fingerprints to assist doctors to have temporary access of medical information. If a patient is in a coma, the doctor needs to access the patient's medical records immediately to take efficient aid measures. Künzi et al. [20] introduced an access mechanism in critical conditions for EHR systems which encompass digital rights protection of health records. Their approach for emergency situations, they mitigate the emergency key distribution problem and can be integrated in distributed environments.

b) *Contextual Attributes for Access Control in Critical Medical Conditions*

Context identifies a specific condition by considering the circumstances where an event arises. Each contextual attribute serves as a quantitative primitive, like the location of the requestor. Attributes in ABAC are divided in the four following categories [21]: i) subject attributes identify the user requesting access, like age; ii) action attributes identify the requested action like read; (c) object attributes identify the resource of access like a medical record; and (d) environment attributes are related with factors of dynamic access control, like time.

In the healthcare domain, contextual information that identifies a patient's medical critical condition should be characterized in managing access to the medical sensitive data so as to assure the most effective treatment. Correspondingly, the implementation of access control models that incorporate the context notion, like the concept of dynamically altering contextual attributes that characterize the current status, is needed. More particularly, context is deemed as any information identifying the status of an entity, like an object, place or person, based on the relation between a requestor and an application [22]. Using contextual information assists the implementation of access control policies by considering the conditions of access requests' evaluation. As an example, in emergency cases, an emergency medical professional intends to access the patient's medical information to efficiently address a critical situation. The values of contextual information are collected, for example, from IoT devices, like a wearable which measures blood pressure. In emergency situations, the emergency healthcare teams must be able to gain access instantly to the patients' healthcare records.

We reviewed the following works to identify context-based information for facilitating the evaluation of critical healthcare conditions. Nomikos et al. [23]

examined patients’ conditions using attributes, like the time when the stroke happened, the age, the DBP, the SBP, the Glasgow and the Scandinavian coma scales that characterize the patient’s consciousness level. Mahmood et al. [24] estimated the crisp values of blood pressure parameters from the HR. Djam et al. [25] proposed a fuzzy expert system for the hypertension management utilizing the fuzzy logic paradigm. As fuzzy inputs, BMI, age, DBP, and SBP were deemed to estimate the risk for hypertension.

Manasa et al. [13] considered contextual attributes like the patient’s medical history, allergies, prescriptions, and basic profile. Furthermore, an emergency attribute is considered for emergency access. A fuzzy expert system for estimation of heart diseases, that utilizes the approach of cuckoo search, is suggested by Moameri et al. [26] by considering the attributes of age, type of chest pain, blood pressure, electrocardiogram results, maximum HR, and cholesterol level.

Few studies take under consideration users’ specificities for the evaluation of access policies. For instance, the increased HR is considered as critical for a specific patient in case that his healthcare situation, his activity levels or his age are taken into account. Zerkouk et al. [27] suggested an adaptable access control paradigm and its related architecture, where the security policy is based on an analysis of the user’s monitored behavior. Røstad et al. [28] introduced a mechanism for personalized access control in health records. Their scheme combines properties and concepts of RBAC and DAC to manage the desired properties. Additionally, they deem a set of common policies that cannot be edited by the patient, along with a set of personal policies updated by the patient. Petković et al. [29] suggested security and privacy enhancements in a RBAC paradigm. Their system includes personalized access control which is a combination of user-managed and role-based access control, along with a cryptographic enforcement, that includes effective key management for accessing medical data.

Son et al. [30] suggested a dynamic access control paradigm, for preserving the personal health information security in a cloud environment by considering contextual attributes for dynamic access. Their model utilizes the ontological concept of 5W1H to process context-based attributes for dynamic access. Their approach refers to the dynamic access control in medical sector.

c) Hyperledger Fabric Blockchain for Access Control in Critical Medical Conditions

Various implementations have been proposed which utilize the Hyperledger Fabric blockchain for managing the access control in emergency medical situations. First of all, Son et al. [31] propose an emergency access control management framework to safeguard the patients' data. Their framework is formed dependent on permissioned blockchain Hyperledger Fabric, and defines regulations and rules by utilizing smart contracts and time duration to manage emergencies. Additionally, in their system the patients restrict the time to access the data in emergency conditions. Additionally, Le et al. [32] propose a Hyperledger Fabric-based system which deals with the problem of yielding access to patients' sensitive information when emergency situations arise and deals with the problems of setting appropriate rules for accessing the emergency control management of personal health records. Furthermore, Morelli et al. [33] present an audit-based framework which leverages the Hyperledger Fabric distributed ledger in order to increase accountability and decentralize the authorization decision process of Attribute-Based Access Control policies by using smart contracts ,and implementing it in the use case of EHR access control.

Additionally, various research works refer to the inclusion of blockchain for medical access control in non-emergency cases by leveraging the Hyperledger Fabric blockchain platform. Firstly, Chenthara et al. [34] develop a privacy-preserving framework called "Healthchain" based on blockchain technology which maintains integrity, security, privacy, and scalability of the e-health information. More specifically, the blockchain is built on Hyperledger Fabric, which is a permissioned distributed ledger solution by utilizing Hyperledger composer and stores EHRs by using IPFS to implement their "Healthchain" framework. Additionally, Zhan et al. [35] propose a paradigm which encourages the growth of healthcare data by enabling stakeholders to collaborate and share EHR trust. More specifically, they recommend a Hyperledger Fabric-based strategy to support the exchange of EHR models. By leveraging the Hyperledger Fabric blockchain, EHR stakeholders can be brought into the channel to facilitate data sharing. ABAC permits users to design the data access control policy, which can improve security. All the records stored in the blockchain are viewed utilizing the Hyperledger Fabric feature and they can't be destroyed or altered, supporting data traceability. Last but not least, Malamas et al. [36] propose, a distributed fine-grained access control model for shared and dynamic multi-authority and multi-domain environments, along with Janus, a practical system for policy enforcement. Their model supports: i) dynamic trust management between different authorities, ii) flexible access control policy enforcement, defined at the domain and cross-domain level, iii) a global source of truth for all entities, supported by an immutable, audit-friendly mechanism. Janus implements the model and relies on the effective fusion of two core components. First, a Hierarchical Multi-Blockchain architecture that acts as a single access point that cannot be bypassed by users or authorities. Second, a Multi-Authority Attribute-Based Encryption protocol that supports flexible shared multi-owner encryption, where attribute keys from different authorities are combined to decrypt data distributedly stored in different authorities. Their methodology was implemented using Hyperledger Fabric as the underlying blockchain, with the system components placed in Kubernetes Docker container pods.

d) <u>Non-Hyperledger Fabric Blockchain-based for Access Control in Critical Medical Conditions</u>

However, various blockchain-based implementations rely on different blockchain platforms, which aren't based on the Hyperledger Fabric platform, for medical access control. Firstly, in the work of Sultana et al. [37] blockchain was utilized to keep an audit trail of medical data transmissions. Their suggested model comprises two users who share health data. In medical image sharing, the medical technologist who generates X-ray files etc. is the sender, patient is the receiver, and the data in question are the medical image files. Additionally, the patient can share information with a doctor by having the patient as the sender and doctor as the receiver. More specifically, their model uses a public blockchain such as Ethereum that utilizes proof-of-work consensus mechanism in order to validate nodes. Their work provides an overview of their decentralized trustless model that aims to deal with security issues based on storing and sharing of health records and images in an EHR system. More specifically, their work enhances the security of health images and medical records transmission based on a combination of zero trust principles and blockchain. Furthermore, according to Ma et al. [38] blockchain is able to be utilized to query genomic dataset audit trail and build a space and time efficient log. Thus, it provides a promising solution for distributing genomic information with accountability requirement across various sites. Additionally, Gursoy et al. [39] develop a particular smart contract to query and store gene-drug interactions utilizing a multi-mapping index-based method by leveraging the Ethereum blockchain. Their smart contract stores each pharmacogenomics observation, a gene-variant-drug triplet with outcome, in a mapping by a unique identifier, permitting for space and time adequate query and storage. Last but not least, Malamas et al. [40] propose a hierarchical multi expressive blockchain architecture. The testing environment of the proposed system, is set on a local Ethereum-based private blockchain with six Smart Contracts simulating the system functionalities. At the top layer, a proxy blockchain enables independently managed trust authorities to interoperate. End-users from different health care domains, such as hospitals or device manufacturers are able to access and securely exchange medical data, provided that a commonly agreed domain-wise access policy is enforced. At the bottom layer, one or more domain blockchains allow each domain (e.g. a hospital or device manufacturer) to enforce their policy and allow fine-grained access control with attribute-based encryption. Their architecture is designed to provide the autonomous management of trusted medical data/devices and the transactions of mutually untrusted stakeholders, as well as an inherent forensics mechanism tailored for granular auditing. Smart contracts are used to enforce decentralized policies. Ciphertext-policy attribute based encryption (CP-ABE) is used to distribute the decryption process among end users and the system, as well as support an efficient credential revocation mechanism.

e) Comparison between ABAC and ABE paradigms

ABE Definition and Categories

Attribute-Based Encryption (ABE) schemes allow a user to encrypt a file based on a certain policy and a public key. In order to share this encrypted file with a set of users, the data owner can generate a unique key for each user that wishes to share the file with. These keys are generated based on a list of attributes. More precisely, the attributes are bound to the identity of the owner of the key (e.g. name, surname, date of birth, department in the company etc.). Then, a user is able to decrypt the file encrypted with a certain policy only if the attributes of her key satisfy the underlying policy. ABE was first introduced by Sahai and Waters [41] in order to solve the problem of encrypted access control. ABE schemes are classified into two main categories: (1) Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and (2) Key-Policy Attribute-Based Encryption (KP-ABE). In CP-ABE, every secret key is generated along with a policy P while ciphertexts are generated with a set of attributes U. Decryption is possible if the list of attributes satisfies the underlying policy (i.e. P(U) = True). KP-ABE works similar. More precisely, the generated ciphertexts associated with a set of attributes while the secret keys are associated with a policy. Similarly, decryption works if at least a threshold number of attributes overlap between the ciphertext and the secret key of the user who is trying to perform the decryption.

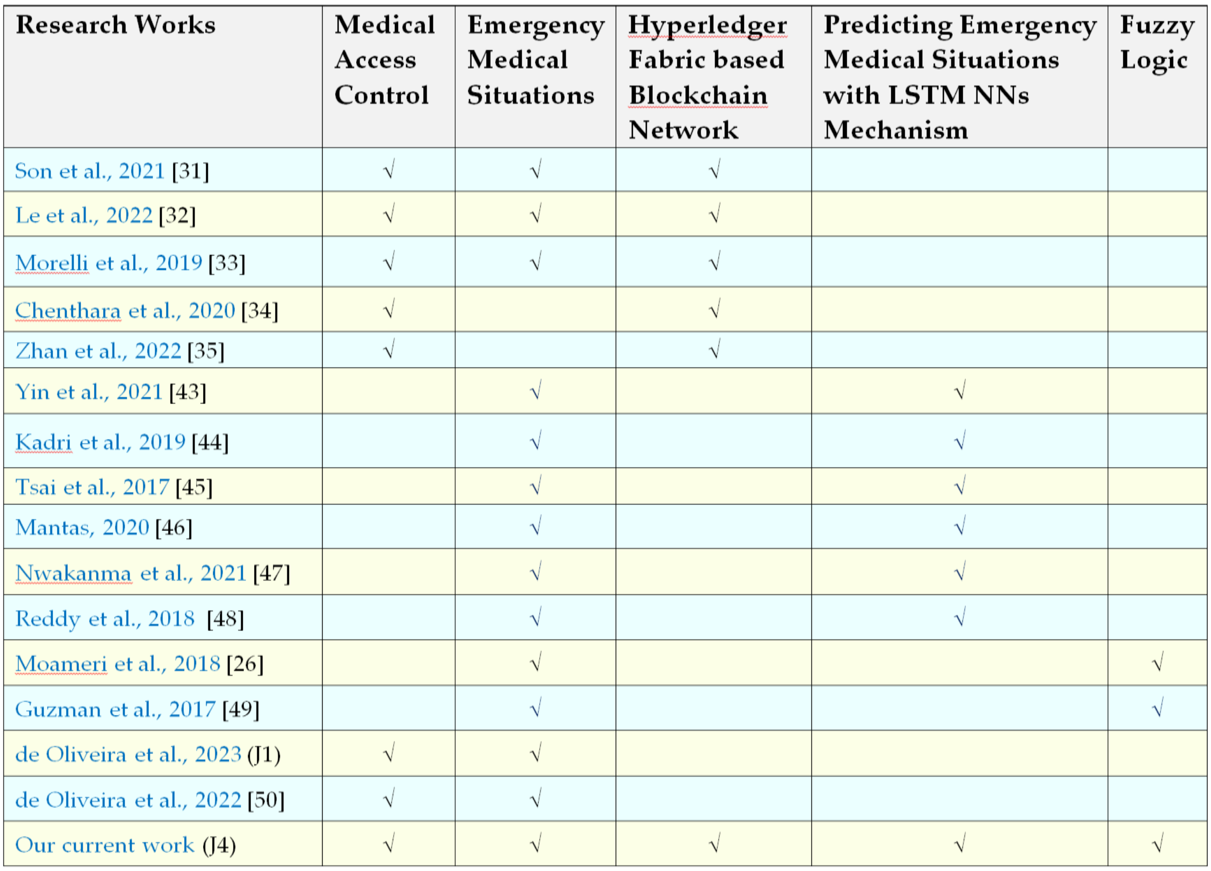
ABE VS ABAC - Advantages and Disadvantages

First of all, ABE has the following advantages of: (i) data confidentiality (encryption before uploading in cloud), (ii) fine-grained access control (using attributes and access policies), (iii) scalability (the number of authorized users do not affect performance), (iv) key traceability and user accountability, (v) user revocation, and (vi) collusion-resistance (users cannot combine their keys to decrypt data). On the other hand, ABE has the following disadvantages: i) KP-ABE scheme does not allow the encryptor to decide who can decrypt the encrypted data, while CP-ABE schemes do not fully satisfy enterprise-grade access control requirements, in terms of flexibility and efficiency. ii) Moreover, nonmonotonic CP-ABE methods involve increased key length and higher complexity since it encompasses the negations attributes and most Hierarchical ABE and Multi-Authority ABE methods require that each attribute is administered by one authority. iii) In general, ABE methods involve increased complexity compared to other access control methods (this is due to their cryptographic nature). iv) Furthermore, they entail higher costs when adding or removing attributes from already encrypted data, since such operations usually require re-encryption of the data, which in a cloud setting might be quite high.

On the contrary, ABAC has the following benfits: i) The policy model encourages the separation of the access decisions from the points of use. This will pave the way for the development of an interpreter for dynamically interpreting authorization policies in healthcare scenarios and also for developing a healthcare-oriented enabling the context-aware. ii) Additionally, ABAC enforcement raises the involved actors' security awareness by indicating the logic of each authorization decision. context-aware ABAC enforcement mechanism. On the other hand, the context handlers of the ABAC mechanism, used for quantifying contextual circumstances might be compromised and thus they might seriously interfere with the legitimate context-aware access control enforcement. In this dissertation, the policy-based access control has been chosen instead of the cryptographic-based approach for controlling access to sensitive medical data because the benefits outweight the risks.

f) <u>Positioning</u>

As seen in the research papers' comparison in Figure 7.6, we examined research articles by considering the following criteria: i) medical access control, ii) emergency Medical Situations, iii) Hyperledger Fabric based blockchain network, iv) predicting emergency medical situations with LSTM NNs mechanism, and v) fuzzy logic. To our knowledge up till now only our work fulfills all the above-mentioned criteria, which encompasses the integration of a predictive fuzzy personalized mechanism within a Hyperledger based blockchain network by predicting emergencies in the healthcare sector.



Research Works	Medical Access Control	Emergency Medical Situations	Hyperledger Fabric based Blockchain Network	Predicting Emergency Medical Situations with LSTM NNs Mechanism	Fuzzy Logic
Son et al., 2021 [31]	√	√	√		
Le et al., 2022 [32]	√	√	√		
Morelli et al., 2019 [33]	√	√	√		
Chenthara et al., 2020 [34]	√		√		
Zhan et al., 2022 [35]	√		√		
Yin et al., 2021 [43]		√		√	
Kadri et al., 2019 [44]		√		√	
Tsai et al., 2017 [45]		√		√	
Mantas, 2020 [46]		√		√	
Nwakanma et al., 2021 [47]		√		√	
Reddy et al., 2018 [48]		√		√	
Moameri et al., 2018 [26]		√			√
Guzman et al., 2017 [49]		√			√
de Oliveira et al., 2023 (J1)	√	√			
de Oliveira et al., 2022 [50]	√	√			
Our current work (J4)	√	√	√	√	√

Figure 7. 6 Positioning of proposed method.

Chapter 8

8. Dynamic and Personalized Access Control to Electronic Health Records

A. Motivation

1) Introduction

Permitting access to health-related information is crucial as the safety of patients' sensitive data privacy, such as the medical history which is of major significance. Access control paradigms are associated with the rights of an entity in controlling specific data objects. These are dependent on requestor's identity access control paradigms, e.g., Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Mandatory Access Control (MAC) [1]. In addition to these fixed methods, the Attribute-Based Access Control (ABAC) mechanism has been proposed, that is flexible and dynamic [2]. In ABAC, links' snapshots exist, which are dynamically altered, and produced dependent on current context, contrary to statically defined permissions' lists which associate objects with entities.

In the healthcare domain, context-based information that identifies an emergency in patients' medical condition should be considered when permitting access to the health-related private information to secure the most efficient medical care. Respectively, the implementation of access control paradigms that integrate the context concept, such as the notion of actively changing context-based attributes which indicate the current state, is required. Specifically, context is any information describing an entity's state, such as person, place or object, dependent on the link between an application and a requestor [3]. Leveraging context-based information facilitates the application of access control policies by taking under consideration the conditions of the evaluation of the access requests. More specifically, in critical conditions, an emergency doctor aims to partially access the patient's health-related information to accurately handle an emergency situation. The contextual information's values could be collected from IoT devices, e.g., a wearable that can track the heart rate. We note that context handlers are valuable for implementing actions of dynamic authorization that take under consideration the emergency state of a particular healthcare critical event before deciding an access control result. In emergency cases, the emergency health-related staff must access instantly the patients’ healthcare data.

The research objective of this study is the examination of the possibility of having real-time medical information, such as from sensors and health-related devices, and its usage to characterize emergency cases and grant access to critical healthcare data. We investigate the use of machine learning techniques to derive personalized and dynamic access control policies for accessing EHRs depending on the current contextual information. Particularly, we will utilize the patients’ current medical metrics so as to estimate if the patient risks to suffer from cerebral infarction, cerebrovascular diseases or hypertension by implementing Artificial Neural Networks (ANNs) and utilize the predictive mechanism to evaluate the criticality of patients’ medical state for permitting access or not to the EHR-system.

2) ***Access Control in Critical Medical Cases***

Yielding access to patients’ sensitive information is an important topic due to the fact that exist the risk for patients’ private information to be exposed to malevolent requesters. Permitting access to EHRs in critical situations ameliorates the patients’ life and betters decision-making in healthcare [4]. Povey et al. [5] introduced a retrospective access control paradigm so that the system isn’t corrupted, and where transactions are used to assure that the integrity can be recovered in a system’s violation episode.. The authors present a break-glass paradigm that notifies for possible corruption of the system before its activation. The authors explain that in a critical situation, the requesters can handle the system but, after this incident, they should explain to the administrator of the system in order to prevent the associated penalty.

Manasa et al. [6] introduced an access control protocol to accomplish patient-centric privacy related to medical-related data in critical cases. The paradigm proposed by Tsegaye et al. [7] enhances the confidentiality of the EHRs via ABAC and RBAC, while ensuring integrity by leveraging the Clark–Wilson paradigm which safeguards the EHRs from both unauthorized entities and authorized medical actors. In addition to this, by implementing their model, the EHRs can be protected and any access issues could be managed while permitting EHRs access in an emergency situation. Li et al. [8] presented an access control model for personal health-related information within the cloud computing servers. They used the Attribute-based Encryption (ABE) paradigm to encrypt patients' medical information. Furthermore, the introduced paradigm strengthens requesters' on-demand revocation and break-glass access in emergency cases.

Jagdale et al. [9] incorporated a system for yielding data access to health-related in-formation in cloud environment. Their paradigm supports ABE encryption to encrypt the medical records. Their paradigm permits break-glass access for emergency conditions, and modification of access policies or attributes. Brucker et al. [10] proposed a break-the-glass paradigm by enabling a SecureUML extension. They introduced a security paradigm enabling break-the-glass which contains a transformation from break-the-glass SecureUML policies to eXtensible Access Control Markup Language (XACML). Georgakakis et al. [11] introduced a spatio-temporal emergency RBAC paradigm dependent on spatio-temporal contextual information of hierarchy of roles, location, and time in order to grant exception access in emergency cases. Kabbani et al. [12] introduced the integration of situation-based authorization policies by leveraging XACML that supports policy-based management architecture and an attribute-based policy language. By leveraging XACML, they incorporate attributes which are aggregated and utilized in rules, while they pass on the policy the dynamicity of values.

Marinovic et al. [13] presented a break-glass approach that creates a break-glass policy by proving why the access isn't granted. The authors' paradigm presents missing and conflicting data, permitting the policy to make a knowledgeable decision when tackles in-consistent or missing information. Maw et al. [14] introduced an access control paradigm in networks of body area and wireless sensor networks that supports a flexible control of permitting access to data in critical situations. Guan et al. [15] presented a model using the patient's fingerprints to assist healthcare actors to have temporary authorization access of private medical data. If the patient suffers from coma, the healthcare actor must access the patient's private medical information urgently so as to take efficient aid measures.

3) ***Context-based Information for Access Control***

Context identifies a specific case by considering the circumstances where an incident happens. Each context-based attribute is a quantitative primitive, e.g., the requestor's location. Contextual information in ABAC is divided in the four subcategories, as follows [16]: (i) subject attributes which define the requestor, e.g., the attribute of age; (ii) action attributes that define the requested action e.g. the read action; (iii) object attributes which define the access resource e.g., a medical file; and (iv) environment attributes that are connected to dynamic access control aspects, e.g., time.

To identify context-based information which is able to assist the prediction of critical healthcare conditions, we examined the studies, as follows. Nomikos et al. [17] inspected patients' status, utilizing attributes, e.g., the stroke's occurrence time, the Scandinavian coma scale and the Glasgow coma scale value, that identify the patient's consciousness level, the Diastolic Blood Pressure (DBP), the Systolic Blood Pressure (SBP), and the age Mahmood et al. [18] evaluated the blood pressure's crisp values parameters from Heart Rate (HR). Djam et al. [19] presented a fuzzy expert system for the hypertension handling by leveraging the fuzzy logic method. As fuzzy inputs, the Body Mass Index (BMI), age, DBP, and SBP were taken into account to estimate the risk of hypertension.

Manasa et al. [6] introduced contextual information such as the patients' prescriptions, allergies, and history. In addition to this, an emergency attribute is defined for break-the-glass access. Several works consider the user's specificities for the access policies assessment. More specifically, the increased HR can be deemed as critical for a patient, only if his age, health condition, or levels of activity are considered. Zerkouk et al. [20] introduced an access control paradigm, in which the security policy is dependent on requestor's monitored behavior. Røstad et al. [21] presented a paradigm for personalized access control in medical information. The model associates concepts and properties of RBAC and DAC. In addition to this, the authors take into account a group of policies that can't be changed by the patients, along with a personal policies' group that can be altered by the patients. Petković et al. [22] introduced security and privacy advancements in a RBAC system. The authors' paradigm includes personalized access control that is a synthesis of user-managed and role-based access control, along with a cryptographic application, that includes effective key management for personalized role-based access control in medical data.

4) Health Analytics Using ANNs

Standard ANNs comprise the following layers: i) the input, ii) the hidden, and iii) the output one. The number of the hidden layers defines the network's depth. In fully connected NNs, all the nodes per layer are linked with the nodes of the next layer. More specifically, each layer's output is used as input for the next one, by implementing in every neuron the appropriate activation function, which is generally non-linear. Additionally, each node is weighted and there is also a bias factor that is taken into consideration per layer. The outputs of layers are calculated as follows:

$$a_l = (W_l h_{l-1} + b_l) \qquad (1)$$

$$h_l = f(a_l) \qquad (2)$$

In the formulas above, l represents the layer number, f indicates the activation function such as sigmoid, softmax, or relu. Wl represents the matrix of weights of layer l, while hl represents the activation function's output and bl represents the bias factor of layer l. If P(α) is taken under consideration as the estimated output from the NNs, α indicates parameters of NN, while y represents the actual value. The loss function of a network with N output nodes, is as follows in formula (3):

$$L = \frac{1}{N}\sum_{i=1}^{N}(y_i - P(\alpha))^2 \qquad (3)$$

The fundamental objective is to optimize the NN parameters. Likewise, the loss function must be minimized. A regularization penalty term is commonly needed in order to avoid overfitting, as seen in the following formula (4):

$$L = \frac{1}{N}\sum_{i=1}^{N}(y_i - P(\alpha))^2 + \Omega(\alpha) \qquad (4)$$

In one of our previous works (j2), we leveraged ANNs for clustering a particular health situation among the available group. We use Ω(α) = λ||α||2 , a hyperparameter and norm-2 in order to manage the regularization strength. Regarding the learning processing, different algorithms exist like ADAM, or SGD.

Nevertheless, ADAM a suitable option based on its capability to process non-stationary data.

The architecture of the ANNs is illustrated in Figure 8.1 For example, a ANN which has: i) three neurons as input, ii) one hidden layer with four neurons, and iii) one neuron as output, is presented as 3-4-1.

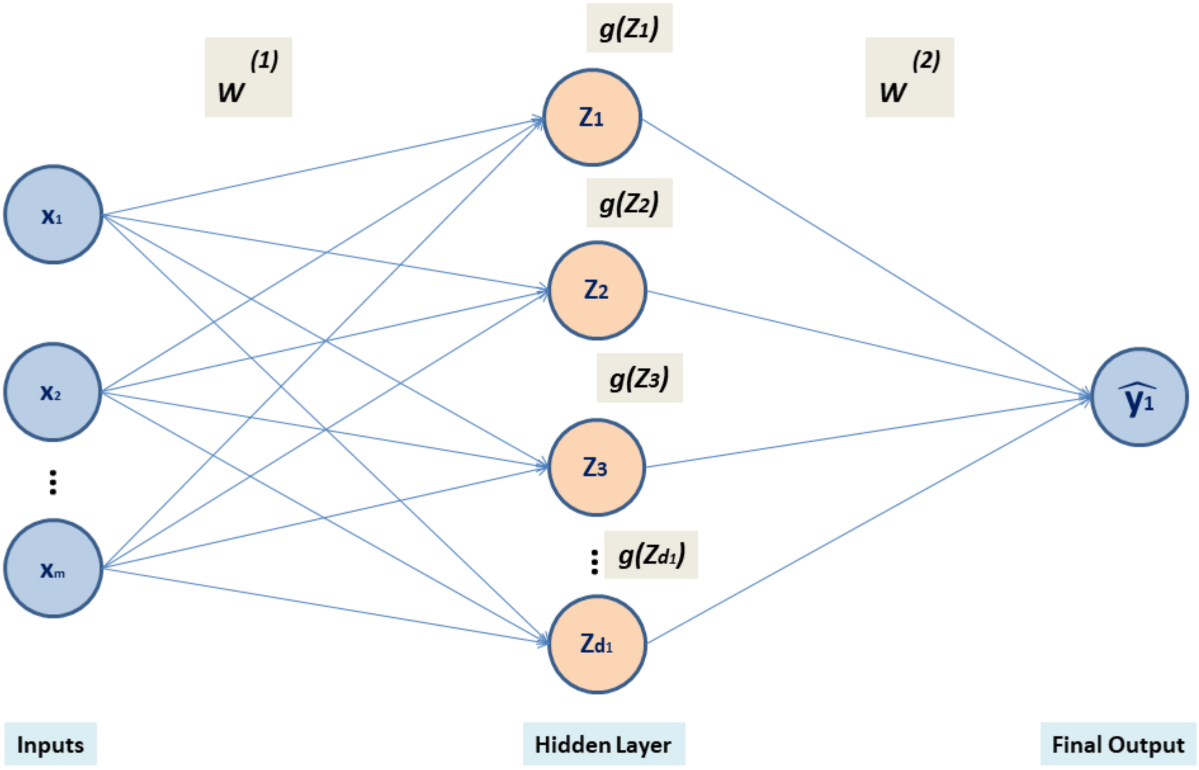


Figure 8. 1 ANNs architecture

ANNs are widely used in the medical sector for the assistance of medical professional for detection of emergency situations or diseases. Khatri et al. [23] developed and tested an ANN-based classifier utilizing Multi-Layer Perceptron with back propagation algorithm, which estimates peak events for respiratory diseases in Dallas, Texas, and they deduced that this classifier could be utilized as a forecasting tool for emergency departments actors. An et al. [24] estimate the onset of high-risk cardiovascular diseases for patients hyperlipidaemia, hypertension, or diabetes histories without the assistance of any healthcare professional, based on deep neural networks, by having at their disposal patients' premorbid information extracted from their EHRs. Singh et al. [25] use convolutional neural networks to categorize the possibly COVID-19 patients as infected or not by leveraging the patients' chest computed tomography images. Roquette et al. [26] compare predictive models for patient's admission to the hospital by using unstructured and structured information at triage time. Additionally, the authors state that among their predictive models, their best model consisted of a double-step process with a deep neural network so as to extract information from text-based data continued by a gradient boosting classifier.

Irfan et al. [27] developed hybrid deep neural networks, utilizing computed tomography and X-ray images, to estimate the risk of the onset of disease in COVID-19 patients. More specifically, the subjects were characterized in the three groups of "COVID-19", "Pneumonia", and "Normal". Ganesan et al. [28] leveraged neural networks for lung cancer diagnosis to assist oncologists to provide the patients with early diagnosis, and to plan for a better medication. Launay et al. [29] conducted a brief geriatric assessment which predicts prolonged length hospital stay, using the ANN multilayer perceptron method. According to the authors, the accuracy of the prediction is primarily based on the existence of life-long conditions. In the work of Kiliçarslan et al. [30] deep learning mechanisms are introduced to results in better classifying pneumonia. Additionally, the authors tested various activation functions and a convolutional NN classifier with two different convolution layers were utilized for pneumonia detection by leveraging chest X-ray imaging.

B. Methods and Tools

1) Diagnostic Context Handlers

A context handler in XACML [31] is a mechanism which converts access requests from the initial format of requests to the canonical form of XACML [32]. Regardless of utilizing or not, the XACML paradigm, context handlers are leveraged in ABAC to convert the attribute representations into mediums based on the application's environment. Lower-level contextual information is advantageous for uplifting higher level contextual information and detecting critical situations. This knowledge is important to determine whether access to sensitive health-related information must be granted or not.

In our previous works (j1), (j2), (j4), we created context handlers based on fuzzy rules to determine emergency cases. The associated contextual attributes that are presented in the context-based model, are demonstrated analytically in (c2). In this work, we use machine learning-based context handlers. A machine learning-based context handler utilizes rules which connect context-based information and generate as output the criticality risk, using machine learning. Specifically, we use machine learning to evaluate the patient's health state criticality.

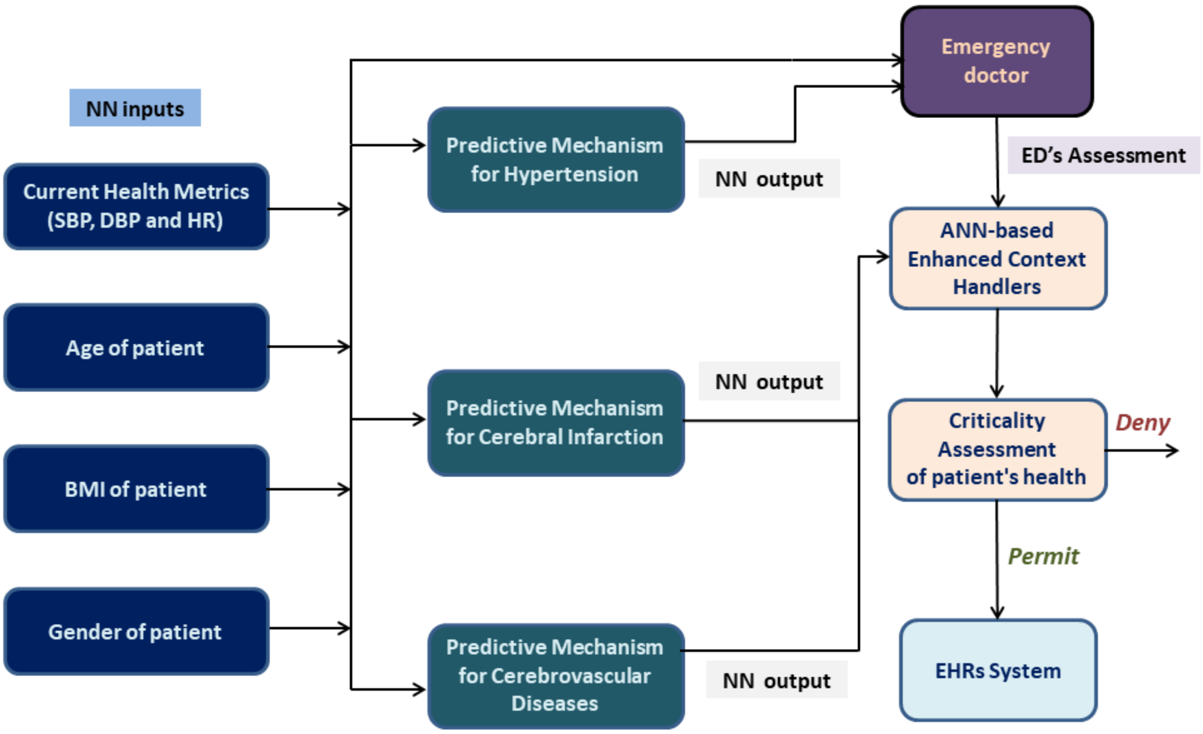
2) ***ANNS for Predicting Health State***

We leverage the computational method of standard ANNs we achieve to diagnose if a patient risks suffering from hypertension, cardiac infarction, or cardiovascular diseases, based on her current health metrics, age, gender, and BMI. Regarding these three pre-dictions, we make the following distinction: The prediction of cerebral infarction and the prediction of cerebrovascular diseases are taken under consideration from the contextual policies, without the intervention of the doctor, whereas the prediction of hypertension is directed by the system to the emergency healthcare professional, so that he has at his disposal a detailed image of the patient's medical profile, and based on this information to be able to decide if the patient suffers from a hypertension crisis based on the personalized profile. The system deduces a critical condition if the evaluation system estimates that the patient risks of suffering from cerebrovascular diseases or cerebral infarction, or if the doctor who receives the result from the hypertension diagnosis, deduces that the patient based on his personalized clinical profile suffers from hypertension.

For example, if the patient has for the medical metrics of HR, DBP, and SBP the values 94 bpm, 72 mmHg, and 123 mmHg, respectively, then our system deduces that he isn't positive either to hypertension or cardiovascular diseases.

3) ***Methodology***

A predictive mechanism is combined with an access control policy, as it is illustrated in Figure 8.2. Our predictive mechanism receives as inputs the following parameters: i) the medical metrics of HR, DBP, SBP ii) the patient's age, iii) the patient's BMI and iv) the patient's gender and after predicting the risk for cerebral infarction, cerebrovascular diseases, and hypertension, and especially by incorporating the additional opinion of the emergency doctor regarding a potential hypertensive crisis, it forwards by the enhanced context handler these three partial estimations to the mechanism of criticality assessment of patient's health status. More specifically, this mechanism decides about the criticality of the patient's medical state, by considering all the above mentioned inputs received from the predictive mechanisms. Finally, if the evaluation of patient's medical state is "Critical", the access to the EHRs system is granted, else this access is denied.



NN inputs
Current Health Metrics (SBP, DBP and HR)
Age of patient
BMI of patient
Gender of patient
Predictive Mechanism for Hypertension
Predictive Mechanism for Cerebral Infarction
Predictive Mechanism for Cerebrovascular Diseases
NN output
NN output
NN output
Emergency doctor
ED's Assessment
ANN-based Enhanced Context Handlers
Criticality Assessment of patient's health
Deny
Permit
EHRs System

Figure 8. 2 Methodology

The policy which determines the functionality of the criticality assessment mechanism is defined by the following rule 5, where the patient's overall criticality estimation is relied on the individual predictions upon the mentioned diseases, along with the final assessment by the emergency staff:

$$\begin{aligned}&\text{If (requestor} = \text{Member of Emergency Staff) AND}\\ &\text{contextual expression (prediction}_{Cerebral\_infarction}\text{ is positive OR}\\ &\text{prediction}_{Cerebrovascular\_diseases}\text{ is positive OR}\\ &\text{doctor\_criticality\_assessment}_{\text{hypertension}}\text{ is positive)}\\ &\text{then (Critical Situation)}\end{aligned} \tag{5}$$

A numeric example is depicted in Figure 8.3. The parameters of a patient with ID = 1113, such as SBP=174 mmHg, DBP=50 mmHg, HR= 88 bps, age=22, BMI=38.26, gender=male, are forwarded simultaneously to the three above mentioned predictive mechanisms. As it is shown, the predictive mechanism for hypertension outputs a positive assessment, the predictive mechanism for cerebral infarction outputs a positive assessment too, and the predictive mechanism for cerebrovascular diseases outputs a negative assessment. All these partial assessments are directed to the ANNs enhanced context handlers where the criticality assessment mechanism takes into consideration all the above mentioned inputs and grants access to the EHRs system.

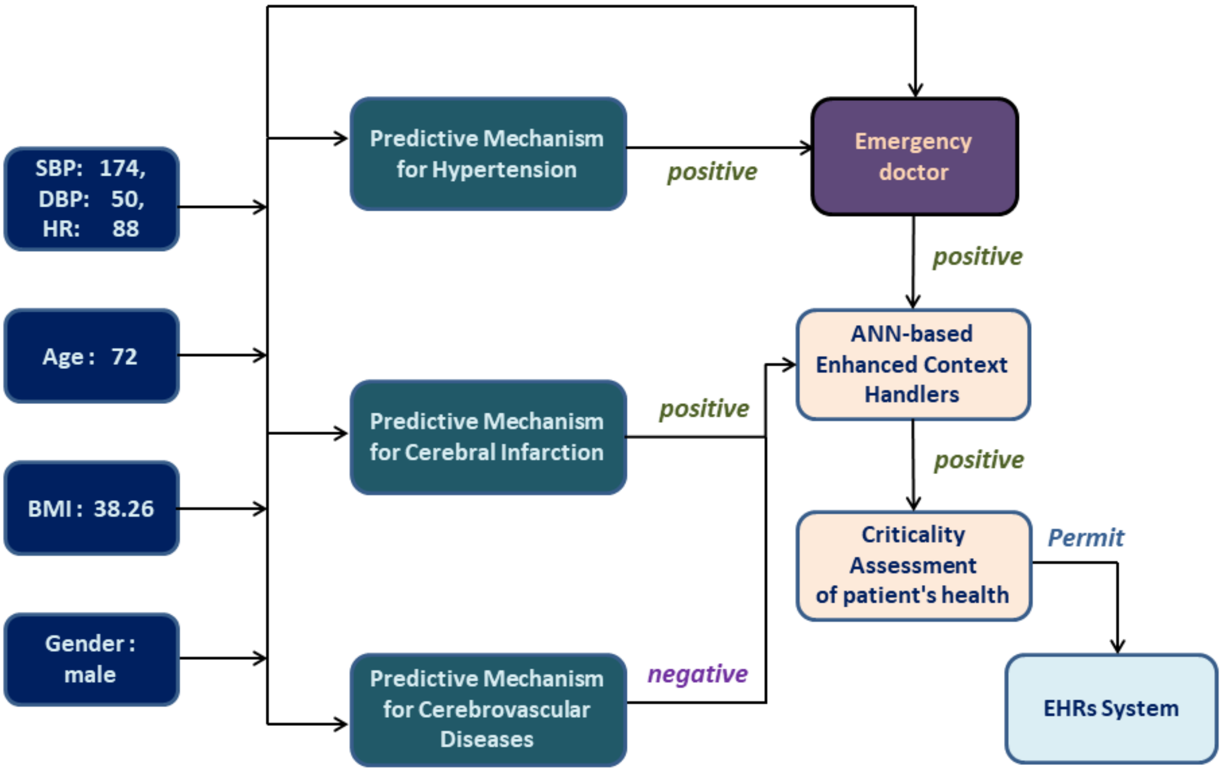

SBP: 174,
DBP: 50,
HR: 88
Age : 72
BMI : 38.26
Gender : male
Predictive Mechanism for Hypertension
Predictive Mechanism for Cerebral Infarction
Predictive Mechanism for Cerebrovascular Diseases
positive
positive
negative
Emergency doctor
positive
ANN-based Enhanced Context Handlers
positive
Criticality Assessment of patient's health
Permit
EHRs System

Figure 8. 3 Illustrative Example

We developed, trained and tested Neural Network models which estimate the risk of: i) Hypertension, ii) Cerebral infarction, iii) Cerebrovascular diseases respectively. For the training purposes of our developed Neural Network we used a dataset [33] which comprises the health records of 219 patients. As inputs we used six variables derived from corresponding fields of this dataset like gender, age, SBP, DBP, HR and BMI. As outputs we used the three variables related to the diseases hypertension, cerebral infarction and cerebrovascular disease respectively, and thus we developed three separate predictive models.

The methodology regarding the estimation of risk of the diseases under examination is shown in Algorithm 1.

```
READ THE APPROPRIATE CHARACTERISTICS FROM DATASET FILE
SPLIT DATA ACCODING TO INPUTS AND OUTPUT
    X = dataset [ gender, age, SBP, DBP, HR, BMI ]
    Y = dataset [ diagnosis of respective disease ]
SPLITTING DATA INTO TRAIN AND TEST SETS
    Xtrain, Xtest, Ytarain, Ytest = split(X, Y, test_size = 0.20)
DEFINE MODEL
    add(Dense(30, input_dim=6, activation='relu'))
    add(Dense(30, activation='relu'))
    add(Dense(1, activation='sigmoid'))
COMPILE MODEL
    compile(loss='binary_crossentropy', optimizer='adam',
metrics=['accuracy'])
FIT MODEL
    model.fit(Xtrain, Ytrain, epochs = 100)
EVALUATE MODEL
SAVE MODEL
```

Algorithm 1. **Web user interface of context-based, predictive access control.**

Next, by using our software, as demonstrated in section 8.3., we found those patients who are at risk of the various mentioned diseases. The methodology regarding the estimation of the patients at risk is shown in the following algorithm 2.

```
REPEAT FOR ALL DISEASES
    LOAD RESPECTIVE DISEASE TRAINED MODEL
    REPEAT FOR EACH PATIENT
        READ THE PATIENT’S DATA
                PREDICT THE RESPECTIVE RISK
                IF RISK >= 0.5
            ADD TO LIST OF PATIENTS AT RISK (OF THE RESPECTIVE
                                        DISEASE)
        END IF
    END REPEAT
END REPEAT
```

Algorithm 2. Estimation of risk for all (2086) patients.

All these results are illustrated in section 8.3, in several figures below which show the variation of the patients at risk with their age and BMI.

4) ***Implementation***

The XACML architecture was used for the implementation of our introduced diagnostic context-based access control paradigm. XACML is additionally a policy-based access control (PBAC) paradigm, where the values of attributes which are related with a user, an action, and a resource are inserted as inputs into the access control evaluation, for a specific requester, a given resource and a particular way of access. The architecture of XACML consists of: 1) the Policy Enforcement Point (PEP), which protects data and applications, intercepts requests and propagates authorization requests which are directed to the Policy Decision Point (PDP); 2) the Policy Information Point (PIP) that associates attribute sources; and 3) the Policy Administration Point (PAP) which handles the access policies.

Policies in ABAC link attributes, to grant or deny access to personal information, and to identify permissible or not actions. For example, if a requester intends to be permitted access to specific healthcare data, PDP intercepts his request. PDP evaluates related policies handled by PAP and exploiting attributes retrieved from PIP. ABAC has been utilized to control access to EHR-systems [34].

To evaluate this work, we developed the context-based, diagnostic access control paradigm dependent on the XACML paradigm and integrated it in EHRServer [35]. EHRServer provides a system for management of medical information based on the openEHR protocol [36]. A thorough view of the architecture of our integrated system is depicted in Figure 8.4. Our context handler communicates with the mechanism of the criticality evaluation, that after having received the patient's current health metrics of SBP, DBP and HR, age, BMI, gender and the prediction of cerebrovascular diseases and cerebral infarction, and the emergency team's assessment regarding a potential hypertension crisis based on the our system's evaluation, is able to calculate the patient's level of criticality, by considering the predictive mechanism diagnosis as well as the doctor's assessment for the final evaluation.

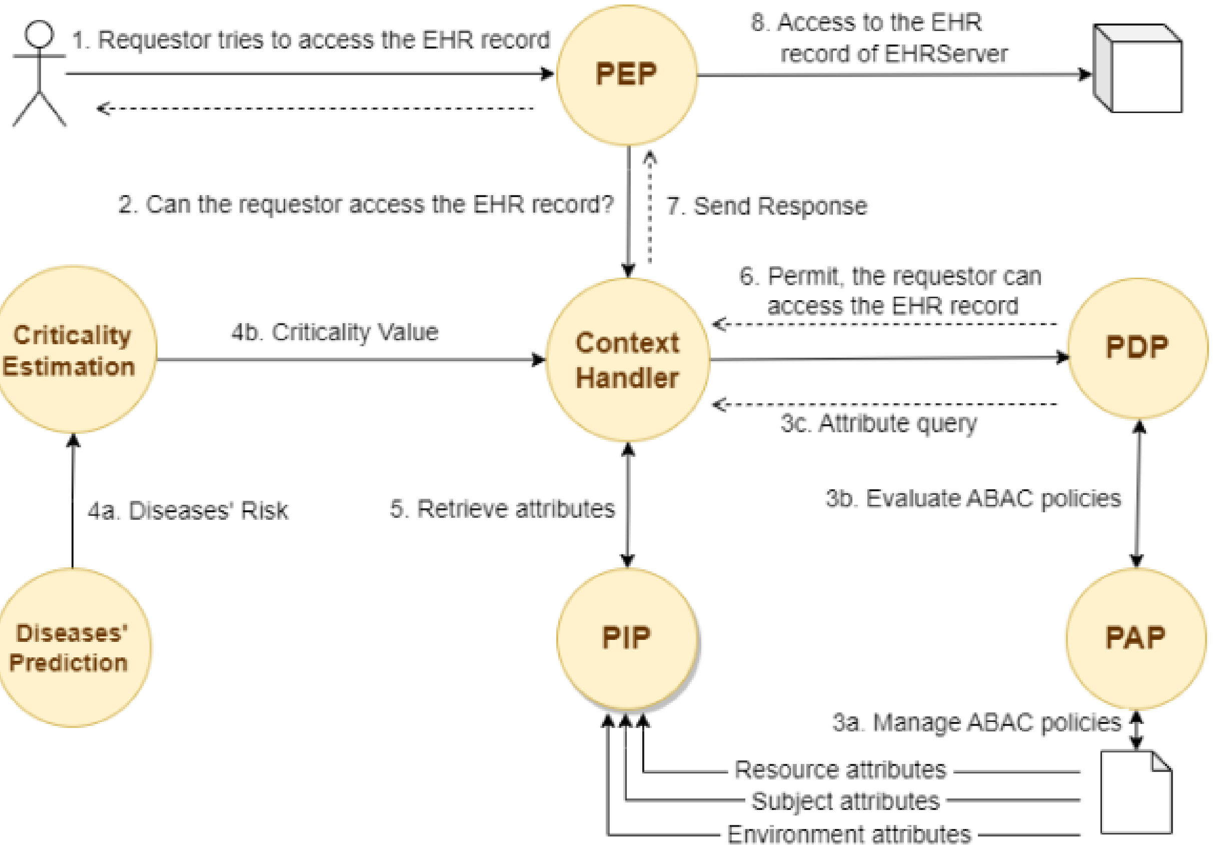
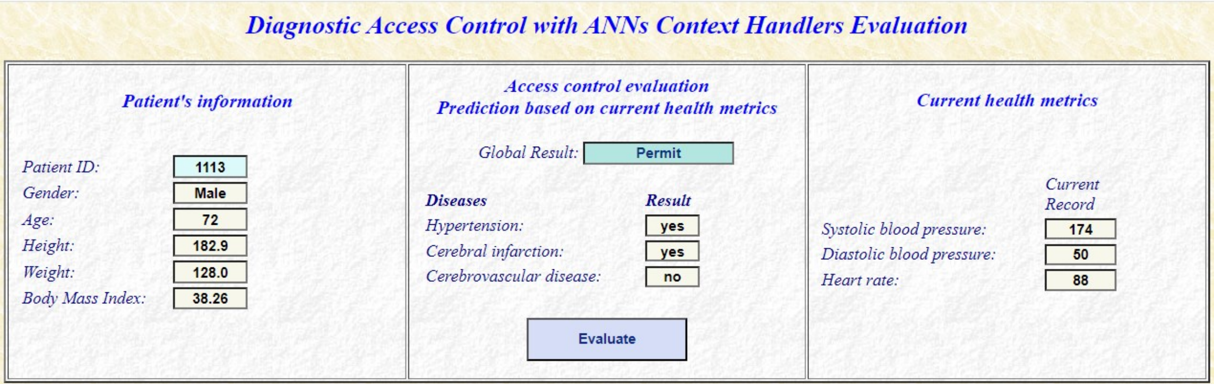


Figure 8. 4 Integrated diagnostic, context-based access control based on XACML Architecture

The predictive mechanism, which predicts if the patient suffers or not from hypertension, cerebral infarction of cerebrovascular diseases, is based on a Neural Network, which is developed in tensorflow and keras. For the training purposes of our developed Neural Network we used a dataset [33] which comprises the health records of 219 patients. The medical metrics of HR, DBP, and SBP, along the patient's personal information of gender, age, and BMI, are used as inputs so as get as output the risk per each disease of the hypertension, cerebral infarction and cerebrovascular disease.

For evaluation purposes, we developed a client-server application in order to implement and validate the whole access control mechanism as illustrated in Figure 8.5. More specifically, in this figure the estimation of the patient's health state with the ID 1113 is show. We notice that the system activates messages for positive risks of hypertension, cerebral infarction and cerebrovascular diseases, and finally permits access to the EHRs System. This web user interface is divided into three panes. In the left pane, the patient's ID, gender, age, height, weight and BMI are demonstrated, while in the center pane, the system's estimation of risk of each corresponding disease, along with system's global access decision are presented, and we notice that in this case the system grants access based on the ABAC context handlers' evaluation. In the right pane, the patient's current medical metrics are presented.



Diagnostic Access Control with ANNs Context Handlers Evaluation

Patient's information

Patient ID: 1113
Gender: Male
Age: 72
Height: 182.9
Weight: 128.0
Body Mass Index: 38.26

Access control evaluation
Prediction based on current health metrics

Global Result: Permit

Diseases	Result
Hypertension:	yes
Cerebral infarction:	yes
Cerebrovascular disease:	no

Current health metrics

	Current Record
Systolic blood pressure:	174
Diastolic blood pressure:	50
Heart rate:	88

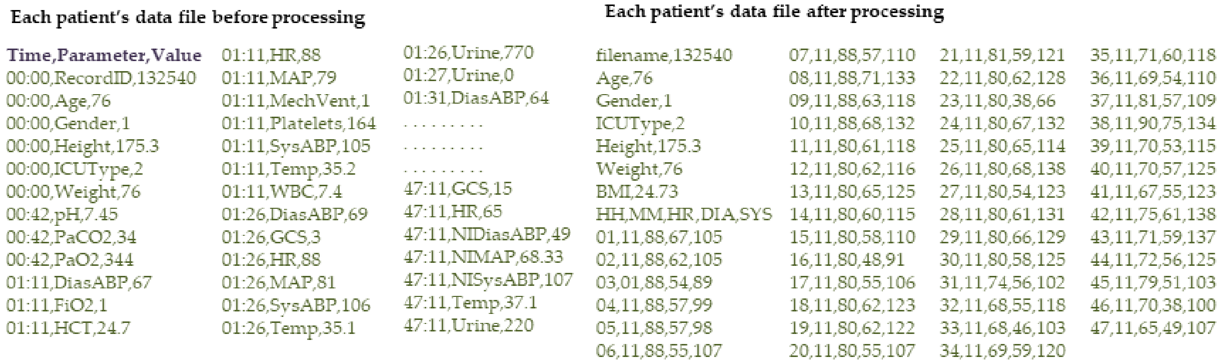
Figure 8. 5 Web user interface of diagnostic, context-based access control

C. Evaluation/Validation

1) Evaluation Scenario, Datasets, and Positioning

In the scenario of our predictive access control mechanism, if the requester is an emergency department (ED) medical professional and if the predictive mechanism deduces that the patient suffers from cerebral infarction or cerebrovascular diseases, or the emergency healthcare professional deduces based on the hypertension prediction that the patient suffers from a hypertensive crisis, then the patient's situation is critical and thus, the medical actor can be granted access to the patient's medical information. The policy rule (5) is demonstrated in section 8.2.

We tested our scenario utilizing the publicly available dataset [37], which comprises 4000 patients and includes one file per patient. Each patient file, among others, contains the SBP, DBP and HR medical metrics. We created an additional software component, as presented in our previous work (j2) to extract these health metrics. After data pre-processing, 2086 patient files remained. The data pre-processing per patient's file is depicted in Figure 8.6. In each file the patient's current health metrics along with the recent medical history, are demonstrated. Additionally, per each patient's file we programmatically created a file which comprises all the 2086 patients' current health metrics, as demonstrated in Figure 8.7.



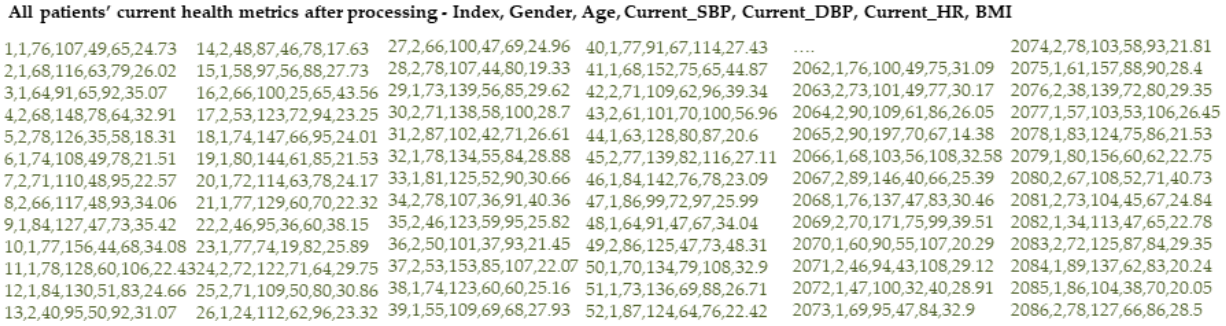
Each patient's data file before processing

```
Time,Parameter,Value
00:00,RecordID,132540
00:00,Age,76
00:00,Gender,1
00:00,Height,175.3
00:00,ICUType,2
00:00,Weight,76
00:42,pH,7.45
00:42,PaCO2,34
00:42,PaO2,344
01:11,DiasABP,67
01:11,FiO2,1
01:11,HCT,24.7
01:11,HR,88
01:11,MAP,79
01:11,MechVent,1
01:11,Platelets,164
01:11,SysABP,105
01:11,Temp,35.2
01:11,WBC,7.4
01:26,DiasABP,69
01:26,GCS,3
01:26,HR,88
01:26,MAP,81
01:26,SysABP,106
01:26,Temp,35.1
01:26,Urine,770
01:27,Urine,0
01:31,DiasABP,64
. . . . . . . . .
. . . . . . . . .
. . . . . . . . .
47:11,GCS,15
47:11,HR,65
47:11,NIDiasABP,49
47:11,NIMAP,68.33
47:11,NISysABP,107
47:11,Temp,37.1
47:11,Urine,220
```

Each patient's data file after processing

```
filename,132540
Age,76
Gender,1
ICUType,2
Height,175.3
Weight,76
BMI,24.73
HH,MM,HR,DIA,SYS
01,11,88,67,105
02,11,88,62,105
03,01,88,54,89
04,11,88,57,99
05,11,88,57,98
06,11,88,55,107
07,11,88,57,110
08,11,88,71,133
09,11,88,63,118
10,11,88,68,132
11,11,80,61,118
12,11,80,62,116
13,11,80,65,125
14,11,80,60,115
15,11,80,58,110
16,11,80,48,91
17,11,80,55,106
18,11,80,62,123
19,11,80,62,122
20,11,80,55,107
21,11,81,59,121
22,11,80,62,128
23,11,80,38,66
24,11,80,67,132
25,11,80,65,114
26,11,80,68,138
27,11,80,54,123
28,11,80,61,131
29,11,80,66,129
30,11,80,58,125
31,11,74,56,102
32,11,68,55,118
33,11,68,46,103
34,11,69,59,120
35,11,71,60,118
36,11,69,54,110
37,11,81,57,109
38,11,90,75,134
39,11,70,53,115
40,11,70,57,125
41,11,67,55,123
42,11,75,61,138
43,11,71,59,137
44,11,72,56,125
45,11,79,51,103
46,11,70,38,100
47,11,65,49,107
```

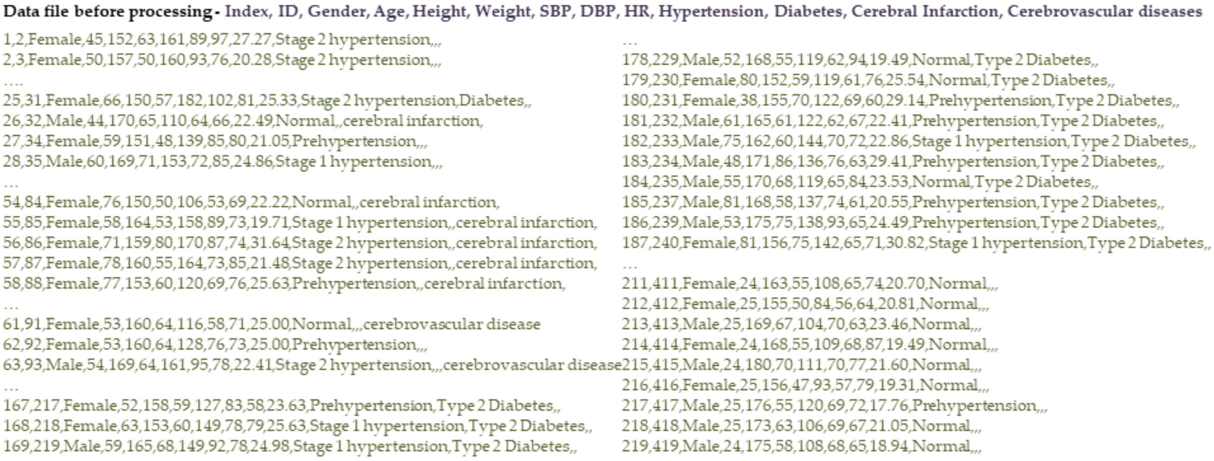
Figure 8. 6 Pre-processing per patient's file, of the 2086 patients



```
All patients' current health metrics after processing - Index, Gender, Age, Current_SBP, Current_DBP, Current_HR, BMI

1,1,76,107,49,65,24.73   14,2,48,87,46,78,17.63   27,2,66,100,47,69,24.96   40,1,77,91,67,114,27.43   ....                         2074,2,78,103,58,93,21.81
2,1,68,116,63,79,26.02   15,1,58,97,56,88,27.73   28,2,78,107,44,80,19.33   41,1,68,152,75,65,44.87   2062,1,76,100,49,75,31.09    2075,1,61,157,88,90,28.4
3,1,64,91,65,92,35.07    16,2,66,100,25,65,43.56  29,1,73,139,56,85,29.62   42,2,71,109,62,96,39.34   2063,2,73,101,49,77,30.17    2076,2,38,139,72,80,29.35
4,2,68,148,78,64,32.91   17,2,53,123,72,94,23.25  30,2,71,138,58,100,28.7   43,2,61,101,70,100,56.96  2064,2,90,109,61,86,26.05    2077,1,57,103,53,106,26.45
5,2,78,126,35,58,18.31   18,1,74,147,66,95,24.01  31,2,87,102,42,71,26.61   44,1,63,128,80,87,20.6    2065,2,90,197,70,67,14.38    2078,1,83,124,75,86,21.53
6,1,74,108,49,78,21.51   19,1,80,144,61,85,21.53  32,1,78,134,55,84,28.88   45,2,77,139,82,116,27.11  2066,1,68,103,56,108,32.58   2079,1,80,156,60,62,22.75
7,2,71,110,48,95,22.57   20,1,72,114,63,78,24.17  33,1,81,125,52,90,30.66   46,1,84,142,76,78,23.09   2067,2,89,146,40,66,25.39    2080,2,67,108,52,71,40.73
8,2,66,117,48,93,34.06   21,1,77,129,60,70,22.32  34,2,78,107,36,91,40.36   47,1,86,99,72,97,25.99    2068,1,76,137,47,83,30.46    2081,2,73,104,45,67,24.84
9,1,84,127,47,73,35.42   22,2,46,95,36,60,38.15   35,2,46,123,59,95,25.82   48,1,64,91,47,67,34.04    2069,2,70,171,75,99,39.51    2082,1,34,113,47,65,22.78
10,1,77,156,44,68,34.08  23,1,77,74,19,82,25.89   36,2,50,101,37,93,21.45   49,2,86,125,47,73,48.31   2070,1,60,90,55,107,20.29    2083,2,72,125,87,84,29.35
11,1,78,128,60,106,22.4324,2,72,122,71,64,29.75   37,2,53,153,85,107,22.07  50,1,70,134,79,108,32.9   2071,2,46,94,43,108,29.12    2084,1,89,137,62,83,20.24
12,1,84,130,51,83,24.66  25,2,71,109,50,80,30.86  38,1,74,123,60,60,25.16   51,1,73,136,69,88,26.71   2072,1,47,100,32,40,28.91    2085,1,86,104,38,70,20.05
13,2,40,95,50,92,31.07   26,1,24,112,62,96,23.32  39,1,55,109,69,68,27.93   52,1,87,124,64,76,22.42   2073,1,69,95,47,84,32.9      2086,2,78,127,66,86,28.5
```

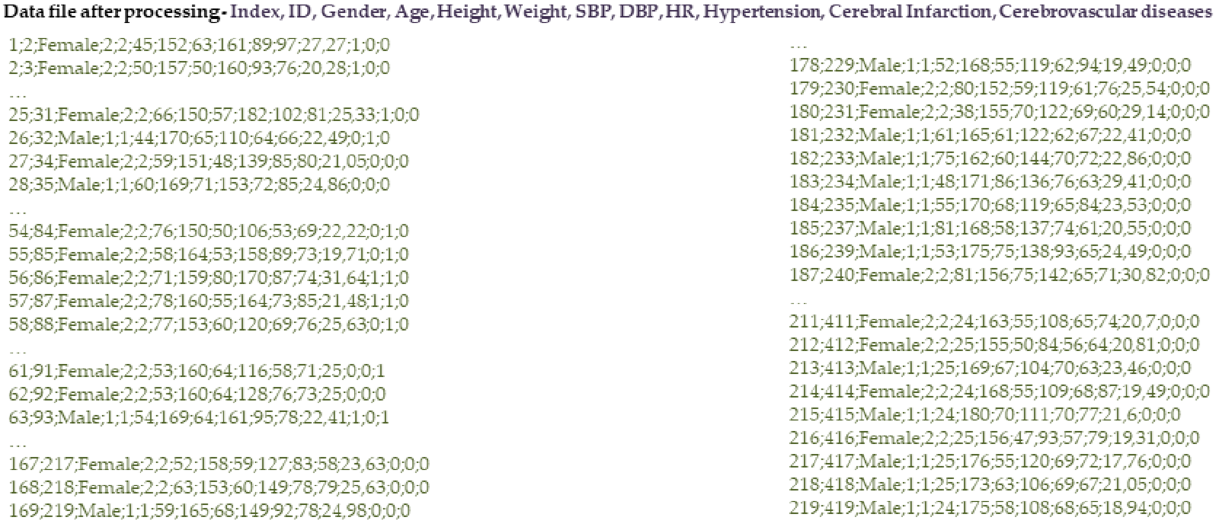
Figure 8. 7 Dataset of the current health metrics of the 2086 patient's in a single file

For each patient, a trained prediction model was created and utilized for the criticality's evaluation. Regarding the training, we utilized the dataset of PPG-BP (Photoplethysmograph – Blood Pressure) [33] that comprises 219 patient medical records. The patients' age varies from 20 to 89 years, with an average of 58 years. The dataset's fields per health record are the following: ID, Gender, Age, Height, Weight, SBP, DBP, HR, BMI, and diseases (cerebrovascular diseases, cerebral infarction, diabetes, and hypertension). The original dataset, along with the dataset file, after pre-processing are depicted in Figure 8.8 and Figure 8.9, respectively. Specifically, it should be mentioned that the differences between the before and after processing versions are specifically the following: i) The field of the Diabetes disease has been removed. ii) Regarding the field of the disease of hypertension, programmatically, we considered as positive result, or "1", the state where the patient suffers from "Stage 2 hypertension", else the result is considered negative or "0". iii) Regarding the field of the disease of "Cerebral Infarction", programmatically, we considered as positive result or "1" the state where the patient suffers from "cerebral infarction", else the result is considered negative or "0". iv) Regarding the field of the "Cerebrovascular diseases", programmatically, we considered as positive all the patients who suffer from "cerebrovascular disease" or "insufficiency of cerebral blood supply".



```
Data file before processing - Index, ID, Gender, Age, Height, Weight, SBP, DBP, HR, Hypertension, Diabetes, Cerebral Infarction, Cerebrovascular diseases
1,2,Female,45,152,63,161,89,97,27.27,Stage 2 hypertension,,,
2,3,Female,50,157,50,160,93,76,20.28,Stage 2 hypertension,,,
….
25,31,Female,66,150,57,182,102,81,25.33,Stage 2 hypertension,Diabetes,,
26,32,Male,44,170,65,110,64,66,22.49,Normal,,cerebral infarction,
27,34,Female,59,151,48,139,85,80,21.05,Prehypertension,,,
28,35,Male,60,169,71,153,72,85,24.86,Stage 1 hypertension,,,
…
54,84,Female,76,150,50,106,53,69,22.22,Normal,,cerebral infarction,
55,85,Female,58,164,53,158,89,73,19.71,Stage 1 hypertension,,cerebral infarction,
56,86,Female,71,159,80,170,87,74,31.64,Stage 2 hypertension,,cerebral infarction,
57,87,Female,78,160,55,164,73,85,21.48,Stage 2 hypertension,,cerebral infarction,
58,88,Female,77,153,60,120,69,76,25.63,Prehypertension,,cerebral infarction,
…
61,91,Female,53,160,64,116,58,71,25.00,Normal,,,cerebrovascular disease
62,92,Female,53,160,64,128,76,73,25.00,Prehypertension,,,
63,93,Male,54,169,64,161,95,78,22.41,Stage 2 hypertension,,,cerebrovascular disease
…
167,217,Female,52,158,59,127,83,58,23.63,Prehypertension,Type 2 Diabetes,,
168,218,Female,63,153,60,149,78,79,25.63,Stage 1 hypertension,Type 2 Diabetes,,
169,219,Male,59,165,68,149,92,78,24.98,Stage 1 hypertension,Type 2 Diabetes,,
…
178,229,Male,52,168,55,119,62,94,19.49,Normal,Type 2 Diabetes,,
179,230,Female,80,152,59,119,61,76,25.54,Normal,Type 2 Diabetes,,
180,231,Female,38,155,70,122,69,60,29.14,Prehypertension,Type 2 Diabetes,,
181,232,Male,61,165,61,122,62,67,22.41,Prehypertension,Type 2 Diabetes,,
182,233,Male,75,162,60,144,70,72,22.86,Stage 1 hypertension,Type 2 Diabetes,,
183,234,Male,48,171,86,136,76,63,29.41,Prehypertension,Type 2 Diabetes,,
184,235,Male,55,170,68,119,65,84,23.53,Normal,Type 2 Diabetes,,
185,237,Male,81,168,58,137,74,61,20.55,Prehypertension,Type 2 Diabetes,,
186,239,Male,53,175,75,138,93,65,24.49,Prehypertension,Type 2 Diabetes,,
187,240,Female,81,156,75,142,65,71,30.82,Stage 1 hypertension,Type 2 Diabetes,,
…
211,411,Female,24,163,55,108,65,74,20.70,Normal,,,
212,412,Female,25,155,50,84,56,64,20.81,Normal,,,
213,413,Male,25,169,67,104,70,63,23.46,Normal,,,
214,414,Female,24,168,55,109,68,87,19.49,Normal,,,
215,415,Male,24,180,70,111,70,77,21.60,Normal,,,
216,416,Female,25,156,47,93,57,79,19.31,Normal,,,
217,417,Male,25,176,55,120,69,72,17.76,Prehypertension,,,
218,418,Male,25,173,63,106,69,67,21.05,Normal,,,
219,419,Male,24,175,58,108,68,65,18.94,Normal,,,
```

Figure 8. 8 Dataset of 219 patients, before processing

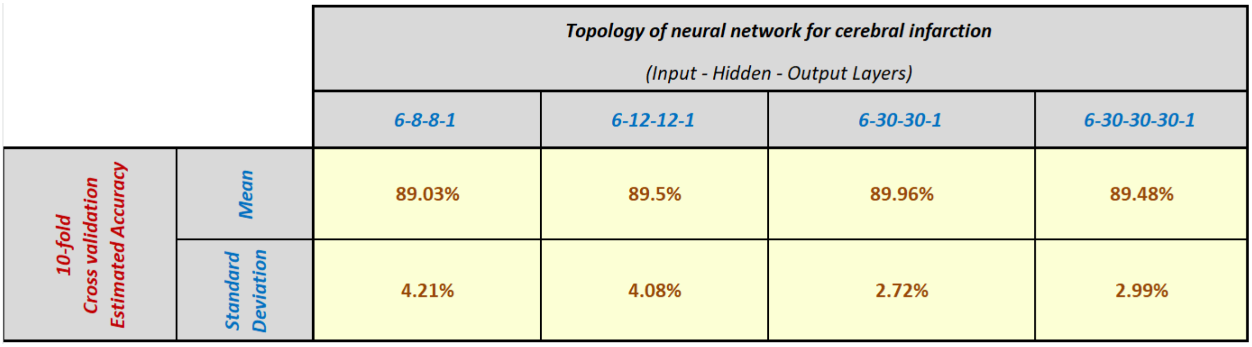


```
Data file after processing - Index, ID, Gender, Age, Height, Weight, SBP, DBP, HR, Hypertension, Cerebral Infarction, Cerebrovascular diseases
1;2;Female;2;2;45;152;63;161;89;97;27,27;1;0;0
2;3;Female;2;2;50;157;50;160;93;76;20,28;1;0;0
…
25;31;Female;2;2;66;150;57;182;102;81;25,33;1;0;0
26;32;Male;1;1;44;170;65;110;64;66;22,49;0;1;0
27;34;Female;2;2;59;151;48;139;85;80;21,05;0;0;0
28;35;Male;1;1;60;169;71;153;72;85;24,86;0;0;0
…
54;84;Female;2;2;76;150;50;106;53;69;22,22;0;1;0
55;85;Female;2;2;58;164;53;158;89;73;19,71;0;1;0
56;86;Female;2;2;71;159;80;170;87;74;31,64;1;1;0
57;87;Female;2;2;78;160;55;164;73;85;21,48;1;1;0
58;88;Female;2;2;77;153;60;120;69;76;25,63;0;1;0
…
61;91;Female;2;2;53;160;64;116;58;71;25;0;0;1
62;92;Female;2;2;53;160;64;128;76;73;25;0;0;0
63;93;Male;1;1;54;169;64;161;95;78;22,41;1;0;1
…
167;217;Female;2;2;52;158;59;127;83;58;23,63;0;0;0
168;218;Female;2;2;63;153;60;149;78;79;25,63;0;0;0
169;219;Male;1;1;59;165;68;149;92;78;24,98;0;0;0
…
178;229;Male;1;1;52;168;55;119;62;94;19,49;0;0;0
179;230;Female;2;2;80;152;59;119;61;76;25,54;0;0;0
180;231;Female;2;2;38;155;70;122;69;60;29,14;0;0;0
181;232;Male;1;1;61;165;61;122;62;67;22,41;0;0;0
182;233;Male;1;1;75;162;60;144;70;72;22,86;0;0;0
183;234;Male;1;1;48;171;86;136;76;63;29,41;0;0;0
184;235;Male;1;1;55;170;68;119;65;84;23,53;0;0;0
185;237;Male;1;1;81;168;58;137;74;61;20,55;0;0;0
186;239;Male;1;1;53;175;75;138;93;65;24,49;0;0;0
187;240;Female;2;2;81;156;75;142;65;71;30,82;0;0;0
…
211;411;Female;2;2;24;163;55;108;65;74;20,7;0;0;0
212;412;Female;2;2;25;155;50;84;56;64;20,81;0;0;0
213;413;Male;1;1;25;169;67;104;70;63;23,46;0;0;0
214;414;Female;2;2;24;168;55;109;68;87;19,49;0;0;0
215;415;Male;1;1;24;180;70;111;70;77;21,6;0;0;0
216;416;Female;2;2;25;156;47;93;57;79;19,31;0;0;0
217;417;Male;1;1;25;176;55;120;69;72;17,76;0;0;0
218;418;Male;1;1;25;173;63;106;69;67;21,05;0;0;0
219;419;Male;1;1;24;175;58;108;68;65;18,94;0;0;0
```

Figure 8. 9 Dataset of 219 patients, after processing

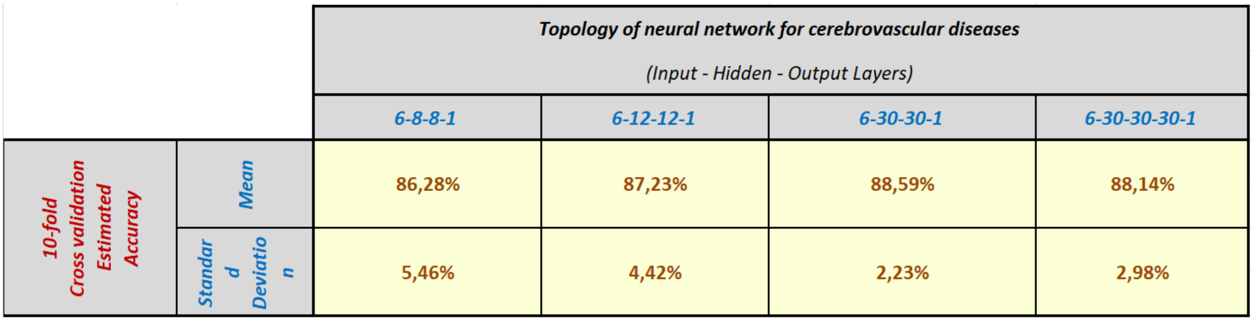
Several experiments were conducted so as to optimize the architecture of the Neural Network for predicting cerebral infarction, cerebrovascular diseases and hypertension, as shown in Figure 8.10, Figure 8.11, and Figure 8.12. We evaluated the network performance by implementing a k-fold cross validation, by considering 10 folds. Additionally, we considered a stratified cross validation so that while splitting the data into folds, each fold has approximately the same proportion of observations of the corresponding disease.

Specifically, in order to predict i) the cerebral infarction, ii) the cerebrovascular diseases, and iii) the hypertension, respectively, we chose the architecture 6-30-30-1 which means that we selected a neural network with an input layer with 6 neurons (equal to the six input variables) two hidden layers with 30 neurons each, and an output layer with a single neuron which represents the risk under examination. After tuning the architecture of the model for 100 epochs, we notice that the mean value and the standard deviation of the average estimated accuracy of the selected structure are 89.96 % and 2.72 %, for predicting the cerebral infarction, 88.59 % and 2.23 %, for cerebrovascular diseases, and 92.68 % and 5.08 %, for hypertension, respectively.



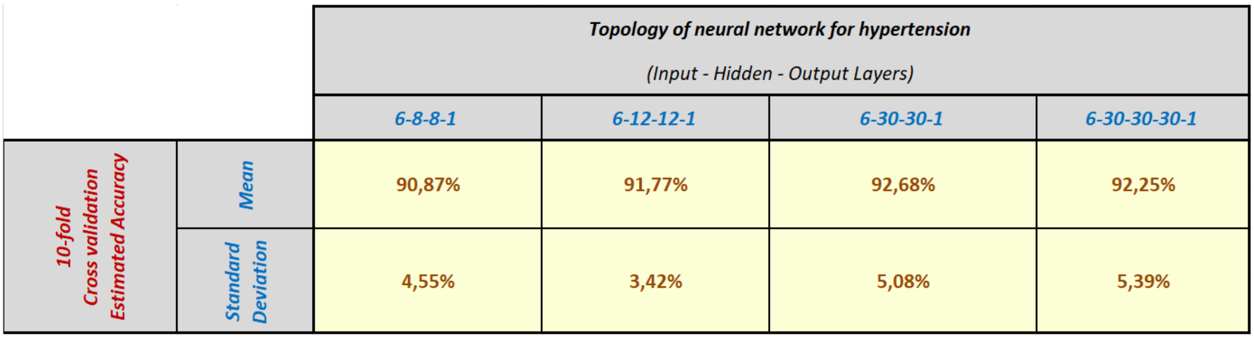
		Topology of neural network for cerebral infarction *(Input - Hidden - Output Layers)*			
		6-8-8-1	*6-12-12-1*	*6-30-30-1*	*6-30-30-30-1*
10-fold Cross validation Estimated Accuracy	*Mean*	89.03%	89.5%	89.96%	89.48%
	Standard Deviation	4.21%	4.08%	2.72%	2.99%

Figure 8. 10 Tuning the topology of the neural network by k-fold cross validation for cerebral infarction



		Topology of neural network for cerebrovascular diseases *(Input - Hidden - Output Layers)*			
		6-8-8-1	*6-12-12-1*	*6-30-30-1*	*6-30-30-30-1*
10-fold Cross validation Estimated Accuracy	*Mean*	86,28%	87,23%	88,59%	88,14%
	Standar d Deviatio n	5,46%	4,42%	2,23%	2,98%

Figure 8. 11 Tuning the topology of the neural network by k-fold cross validation for cerebrovascular diseases



		Topology of neural network for hypertension *(Input - Hidden - Output Layers)*			
		6-8-8-1	*6-12-12-1*	*6-30-30-1*	*6-30-30-30-1*
10-fold Cross validation Estimated Accuracy	*Mean*	90,87%	91,77%	92,68%	92,25%
	Standard Deviation	4,55%	3,42%	5,08%	5,39%

Figure 8. 12 Tuning the topology of the neural network by k-fold cross validation for hypertension

As demonstrated in the research papers' comparison in Table 8.1, we examined research papers by taking under consideration the following criteria: i) medical access control, ii) emergency Medical Situations, and iii) Predicting Emergency Medical Situations with MultiLayered Perceptron (MLP) Recurrent NNs Mechanism. To our knowledge until now only our study fulfills all these criteria that encompass the integration of a diagnostic personalized mechanism by predicting emergency situation in the medical domain.

Table 8. 1 Comparison with other research works.

Research Works	Medical Access Control	Emergency Medical Cases	Predicting Emergency Medical Cases with MLP RNNs Mechanism
Son et al., 2021 [38]	√	√	
Le et al., 2022 [39]	√	√	
Zhan et al., 2022 [40]	√		
Khatri et al., 2017 [23]		√	√
An et al., 2019 [24]		√	√
Singh et al., 2020 [25]		√	√
Roquette et al., 2020 [26]		√	√
Irfan et al., 2021 [27]		√	√
Ganesan et al., 2010 [28]		√	√
Launay et al., 2015 [29]		√	√
Kiliçarslan et al., 2023 [30]		√	√
de Oliveira et al., 2023 (j3)	√	√	
de Oliveira et al., 2022 [41]	√	√	
Psarra et al., 2021 (j1)	√	√	
Psarra et al., 2022 (j2)	√	√	
Psarra et al., 2023 (j4)	√	√	
This work	√	√	√

2) Results

As presented analytically in Table 8.2, from all 2086 patients, only 180 patients risk suffering from cerebral infarction, 201 from cerebrovascular diseases, and 151 from hypertension, based on our prediction. The patients' BMI, regarding the dataset of the 2086 patients, varies from 10 to 99.63. It should be mentioned that regarding all the patients, the patient who has the min BMI of 10 has height of 147.3 cm and weights 21.7 kg, while the patient who has the max BMI of 99.63 has 148.6 cm height, and 220 kg weight. Additionally, the patients' age varies from 17 to 90 years old. The following Figure 8.13, Figure 8.14, Figure 8.15, Figure 8.16, Figure 8.17, and Figure

8.18, describe the variation per each disease regarding the risk of suffering from cerebral infarction, cerebrovascular diseases, or hypertension, and the risk's variation based on age, BMI and gender.

Table 8. 2 Statistical analysis per disease, based on our system's prediction.

	Cerebral Infarction	Cerebrovascular Diseases	Hypertension	All patients
Number of patients	180	201	151	2086
Minimum age	34	18	18	17
Maximum age	90	90	90	90
Minimum BMI	14.38	10	14.38	10
Height of min BMI (cm)	182.9	147.3	182.9	147.3
Weight of min BMI (kg)	48.1	21.7	48.1	21.7
Maximum BMI	49.17	53.42	40.18	99.63
Height of max BMI (cm)	188.0	144.8	170.2	148.6
Weight of max BMI (kg)	173.8	112	116.4	220

In Figure 8.13 the variation of cerebral infarction risk with the patient's age is illustrated. We notice that the age of men who suffer from cerebral infarction varies from 47 to 90 years old, while the women's age varies from 34 to 90 years. So, we notice that women begin suffering from a cerebral infarction from a younger age than men. We notice that the risk of this disease generally increases in ages near 80 years for both genders. Additionally, for the age group of 70 – 80 we notice that men reach the highest risk of a cerebral infarction occurrence. On the contrary, the women's highest risk of a cerebral infarction occurs at the age group of 80 – 90. Furthermore, we notice that above the age of 80, men have lower risk of cerebrovascular infarction, than women.

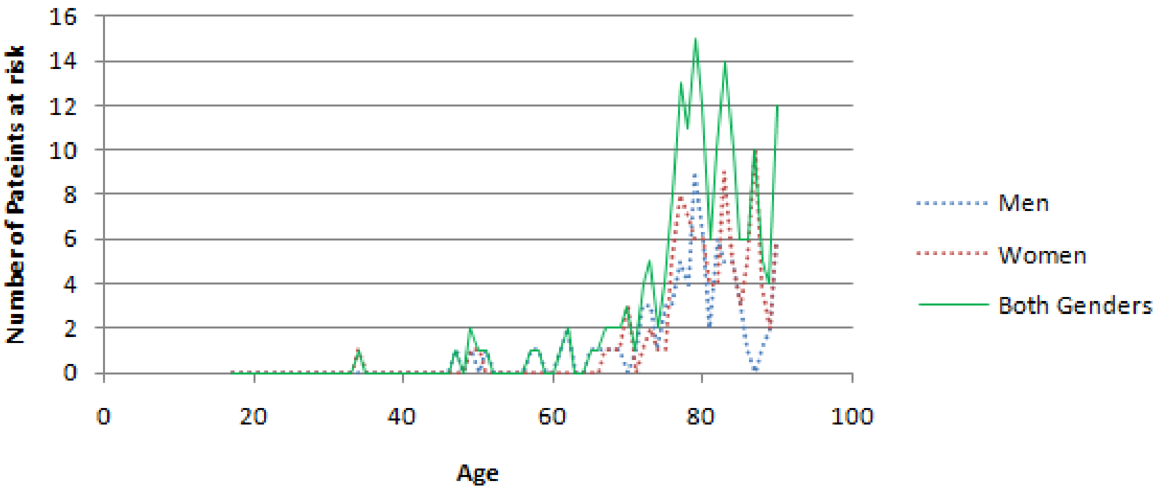


Figure 8. 13 Relation between patients' age and the risk of cerebral infarction

In Figure 8.14 the variation of cerebral infarction risk with the patients' BMI is presented. We notice that men's BMI who risk suffering from cerebral infarction varies from 16 to 49, while the women's BMI varies 14 to 45. So, we notice that women begin suffering from a cerebral infarction from a lower BMI than men, by having as starting point the underweight category (BMI < 18.5). We notice that the majority of those, whose the risk for cerebral infarction is high, are overweight or obese, by having BMI >= 25. Additionally, based on our prediction from the 180 patients who were considered positive to cerebral infarction: i) 12 patients were from the underweight BMI category (BMI < 18.5), ii) 80 patients belonged to the normal category (18.5 <= BMI < 25), iii) 46 patients were from the overweight category (25 <= BMI < 30), and iv) 42 patients were included in the obese category.

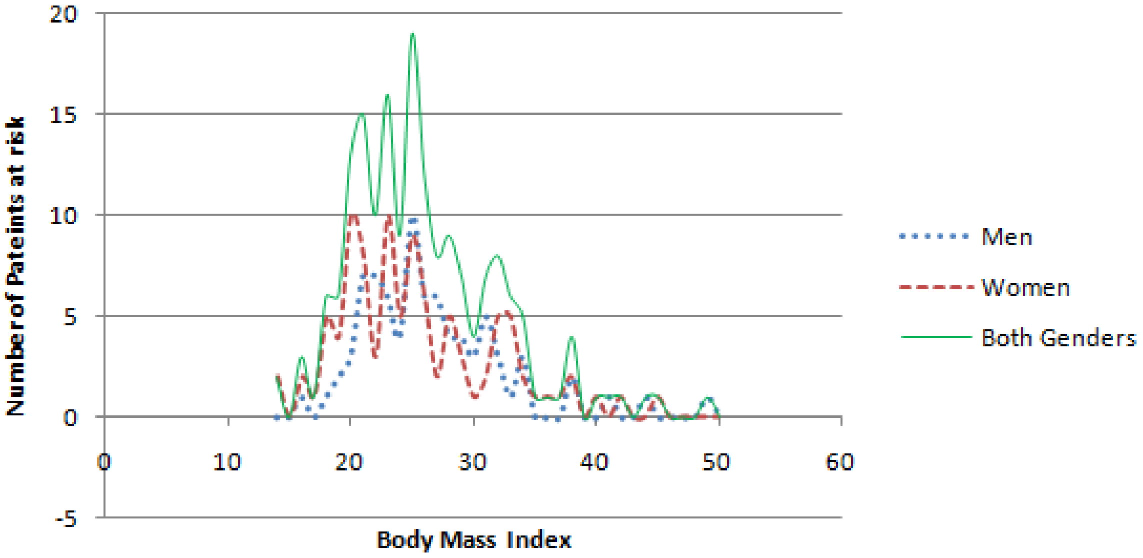


Figure 8. 14 Relation between patients' BMI and the risk of cerebral infarction

In Figure 8.15 the variation of cerebrovascular diseases risk with the patients' age is illustrated. We notice that the age of men who suffer from cerebrovascular diseases varies from 19 to 90 years old, while the women's age varies 18 to 90 years old. So, we notice that women begin suffering from cerebrovascular diseases from a younger age than men. We also notice that the risk of these diseases generally increases from the age of 60 years for both genders. Additionally, for the age group of 65 – 75 we notice that men reach the highest risk of cerebrovascular diseases. On the contrary, the women's highest risk of a cerebral infarction occurs at the age group of

75 – 85. Furthermore, we notice that above the age of 80, men have lower risk of cerebrovascular diseases, than women.

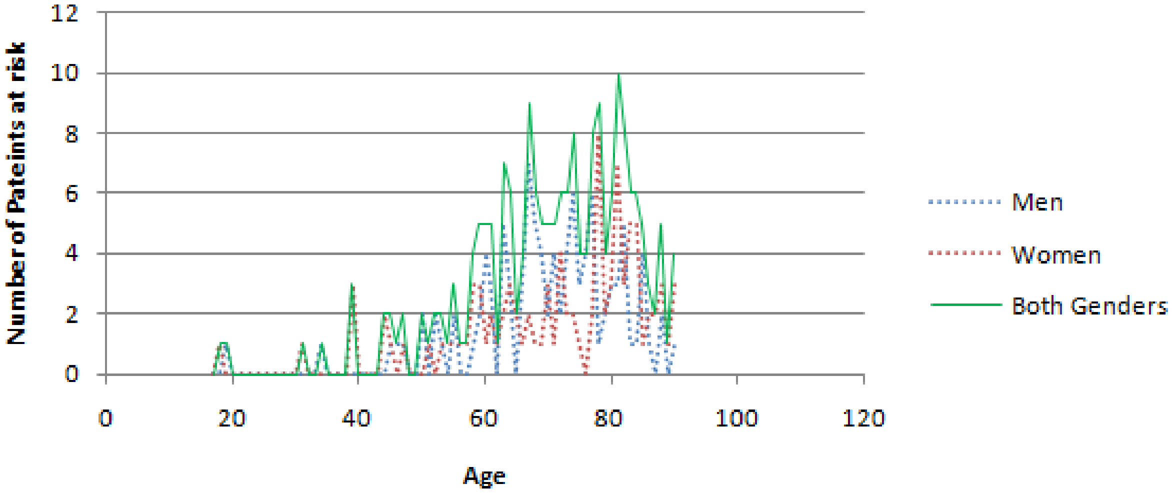


Figure 8. 15 Relation between patients' age and the risk of cerebrovascular diseases

In Figure 8.16 the variation of cerebrovascular diseases risk with the patients' BMI is illustrated. We notice that the men's BMI who risk suffering from cerebrovascular diseases varies from 15 to 45, while the women's BMI varies from 10 to 53.42. So, we conclude that women begin suffering from cerebrovascular diseases from a lower BMI than men, by having as starting point the underweight category. We also notice that the majority of those, whose the risk for cerebrovascular diseases is high, are overweight or obese. Additionally, based on our prediction from the 201 patients who were prone to cerebrovascular diseases: i) 12 patients were classified into the underweight BMI category, ii) 61 patients belonged to the normal category, iii) 75 patients belonged to the overweight category, and iv) 53 patients were considered from the obese category.

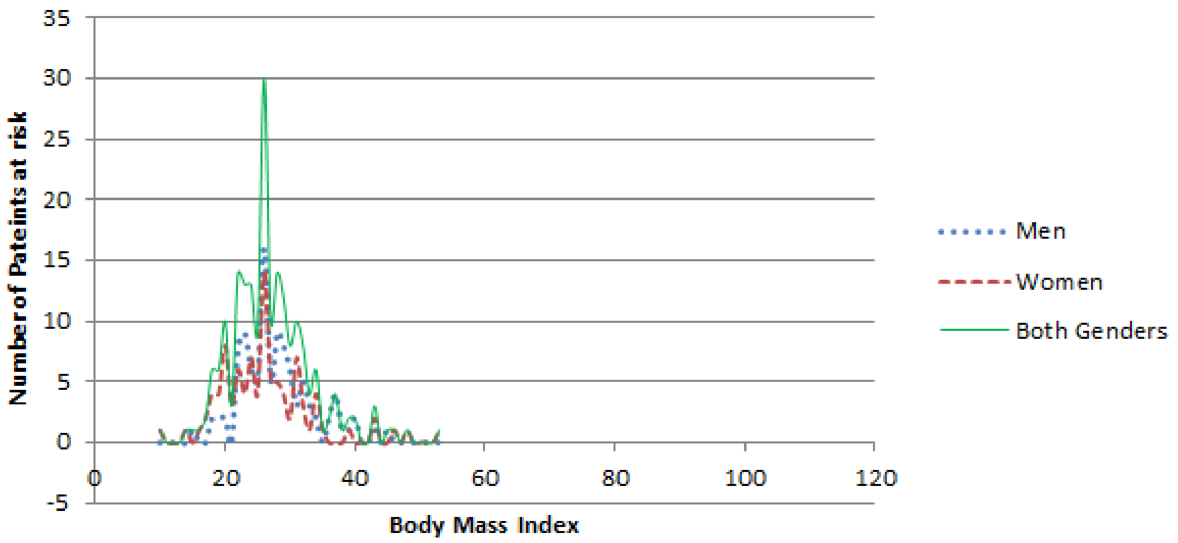


Figure 8. 16 Relation between patients' BMI and the risk of cerebrovascular diseases

In Figure 8.17 the variation of hypertension risk with the patients' age is illustrated. We notice that the age of men who risk suffering from hypertension varies from 18 to 90 years old, while the women's age varies 38 to 90 years old. We conclude that men begin suffering from hypertension from a younger age than women. We also notice that the risk of this disease generally increases in ages over 40 years for both genders. Additionally, for the age group of 45 – 75 we notice that men reach the highest risk of hypertension. On the contrary, the women's highest risk of hypertension occurs at the age group of 60 – 80. Furthermore, we notice that till the age of 59, men have higher risk of hypertension, than women.

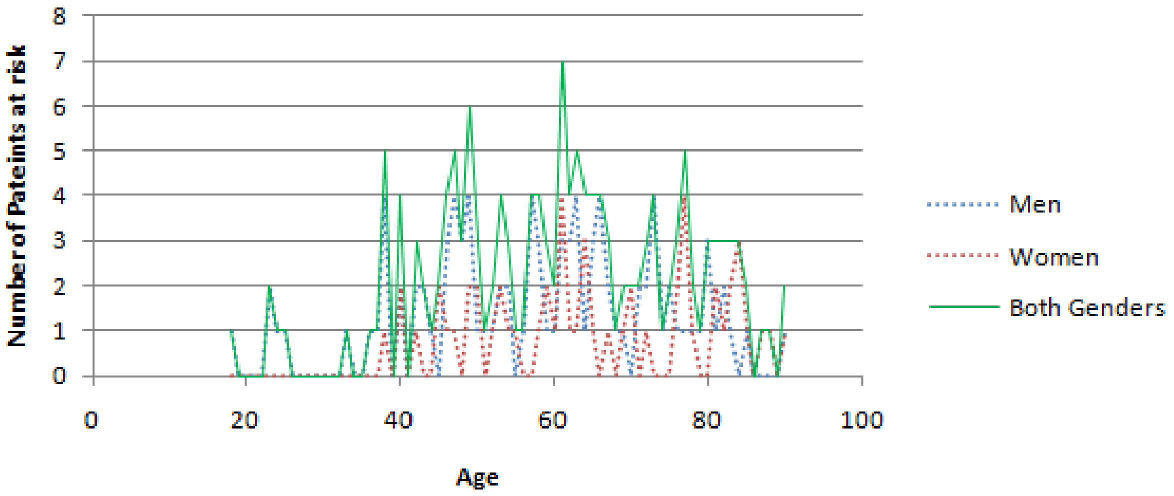


Figure 8. 17 Relation between patients' age and the risk of hypertension

In Figure 8.18 the variation of hypertension risk with the patients' BMI is illustrated. We notice that men's BMI who suffer from hypertension varies from 17 to 40.18, while the women's BMI varies from 14.38 to 34. We conclude that women begin suffering from hypertension from a lower BMI than men, by having as starting point the underweight category. We also notice that the majority of those, whose the risk for hypertension is high, are overweight or obese. Additionally, based on our prediction from the 151 patients who were considered positive to hypertension: i) 11 patients belonged to the underweight BMI category, ii) 66 patients were considered from the normal category, iii) 58 patients were classified into the overweight category, and iv) 16 patients were considered from the obese category. It should be mentioned that the above extracted results correspond to our descriptive analysis (c1) which states that as the BMI increases so does the risk of hypertension.

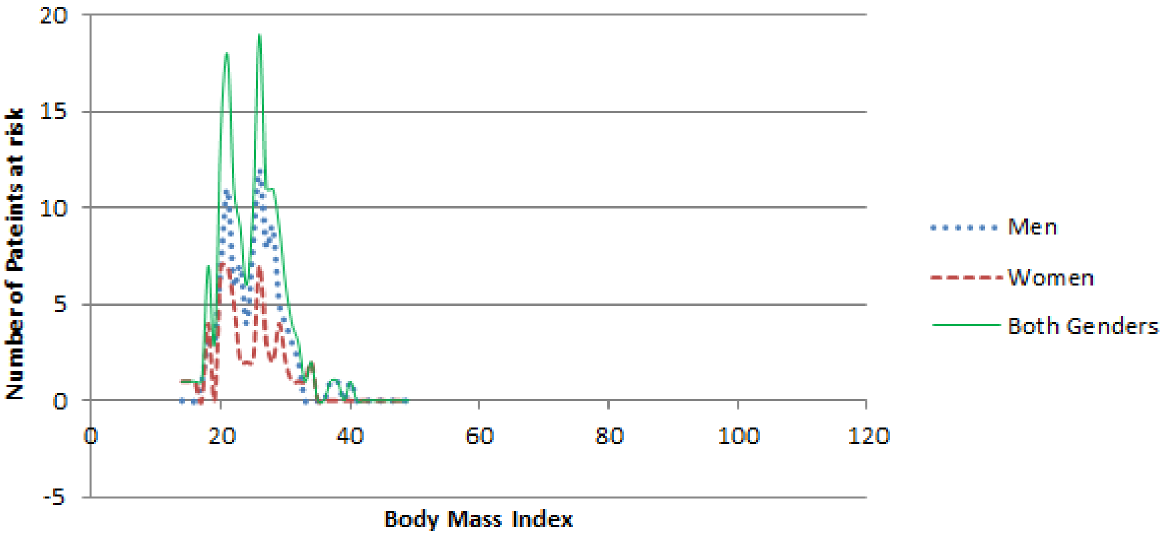


Figure 8. 18 Relation between patients' BMI and the risk of hypertension

3) Discussion

Applying dynamic and personalized context handlers for emergency access control has the following benefits. Firstly, access control is dependent on both subjective expert knowledge and objective patients' medical information. The expert knowledge extraction is achieved by utilizing the machine learning approach, in which our predictive mechanism connects the medical metrics with the patient's criticality, which states the level of patient's health risk. Additionally, except from the patients' medical information, personal metrics of patients' age, BMI, and gender are considered. Furthermore, access control evaluation is relied on context-based rules, which are responsible for the evaluation of the criticality based on the response of our predictive mechanism.

The limitations of our methodology comprise the fact that only the age, BMI, gender and the limited set of medical metrics of SBP, DBP, and HR are considered for the eval-uation of the critical conditions related to the risk of cerebral infarction, cerebrovascular diseases, and hypertension. Additionally, the access control rules which take under con-sideration the estimated risk of these three diseases for the criticality access result are deemed as acceptable by healthcare professionals, but the inclusion of additional critical conditions such as the risk of cardiovascular diseases, would ameliorate the completeness of the access control policies. Additional medical metrics include the oxygen level or the level of glucose in blood, or the existence of chronic diseases.

By comparing RBAC implementations with the emergency access control, in which the emergency healthcare professionals have predefined access in critical conditions based on their role, the proposed ABAC mechanism leverages personalized context which considers patients' personal information and current medical information. It is worth mentioning that in our scenario, part of the emergency access decision is made by emergency healthcare team. The result of the predictive mechanism which evaluates the risk of existence of hypertension is sent to the emergency team along with the patient's current health metrics and personal information of age, BMI, and gender. By having at their disposal both the system's prediction result for hypertension and the patient's contextual information, the emergency professionals can deduce if the patient risks suffering from a hypertensive crisis or not, based on patient's personalized information and the result of the risk of prediction. It should be noted that only the predictive mechanism of hypertension is sent to the emergency healthcare professional, while partial access control decisions which are derived from the corresponding predictive mechanisms of cerebral infarction and cerebrovascular diseases are sent directly to the final criticality assessment, without the emergency team's input.

Chapter 9

9. Conclusions and Future Work

In this Chapter, the conclusions and the contribution of the thesis are summarized. In addition, directions for future work and the limitations of our current work are outlined.

A. Conclusions

In a nutshell, the main contribution of the current thesis is the the

diagnosis and prognosis of the patient's health state in order to assist the final decision of the healthcare professional. This ABAC extension is possible by having as a basis, the developed Context-aware Security Model, Context-aware Security Model Editor and Policy Editor. In addition, stochastic approaches and machine learning techniques are implemented and used in these context handlers for better accuracy. Finally, all predictive mechanisms are embedded in a private and permissioned blockchain network by leveraging the Hyperledger Fabric Blockchain platform.

In particular the following contributions were realized:

The contribution of the current Ph.D. dissertation is summarized to the following sectors:

- **It proposes a Multi-continent Descriptive Analysis for correlation health metrics and diseases.** In health-based descriptive analysis, the patient's health-related contextual information should be taken into account along with the age, the gender and the nationality in order to detect their correlation with health problems such as obesity, hypertension or smoking habits. Such a descriptive analysis is necessary so that healthcare professionals have at their disposal such a statistical analysis so as to have an overall clinical profile concerning the patient's condition. In this dissertation, by using descriptive analytics we introduced a multi-continent overview based on patient's health indices and their correlation to contextual information such as gender and age, that serve as a basis for identifying health problems such as obesity, hypertension and smoking habits. In addition, by our analysis, a descriptive synthesis is produced, based on our literature review, which deduces continent-based investigation according to the patient's heath related information. Finally, in order to validate and compare the results which were extracted by this systematic literature review, we developed and implemented a web application capable of processing and analyzing real datasets in order to present each patient's current health information along with the mean value of the health metrics of SBP, DBP, BMI and the corresponding percentages of smoking and hypertension per continent so as to facilitate the doctor.

- **It proposes Personalized Context Handlers.** i) **It proposes a Non-complex Fuzzy Personalized Context Handlers.** In an emergency situation, the criticality of a patient's medical condition should be taken into account when granting access to her EHR. Such emergency access controls are necessary so that healthcare professionals make informed decisions in life threatening situations. In this work, we introduced contextual attributes that serve in the criticality assessment of situations where access to patients' data is requested. We extended ABAC with healthcare-related context handlers, capable of inferring access policies by dynamically evaluating contextual attributes when granting access to healthcare data. We also created personalized context handlers so as to take into account the specificities of each patient when inferring access policies. ABAC with personalized context handlers is more capable than baseline ABAC and ABAC with non-personalized context handlers in detecting critical situations, especially in the oldest age group that is the most important. ii) **It proposes Complex Fuzzy Personalized Context Handlers.** Implementing personalized complex context handlers in critical situations, for emergency access control, results in more adequate access control, which is dependent on objective patients' metrics and on subjective expert knowledge as well. By exploiting a fuzzy logic approach, in which conjunctive complex fuzzy rules associate the fuzzy variables per health metric with the criticality, we achieve to evaluate the patient's health risk level. Additional personal information is considered, e.g., the patient's age, and finally access control is deduced based on a new and complex fuzzy rule-based inference process, which calculates the patients' criticality risk. In an acute care situation, the criticality of a patient's health status should be considered when yielding access to healthcare professionals regarding her medical data so as to decide about emergency cases. In this work, we introduced complex context handlers, able of deducting access control policies by dynamically examining contextual attributes when permitting access to medical sensitive information. We conclude that ABAC with personalized complex context handlers is more efficient than baseline ABAC and ABAC with non-personalized complex context handlers in identifying emergency conditions, notably in the oldest age group which is the mostimportant.

- **It proposes Prognostic-based Context Handlers.** In emergency healthcare situations, the health criticality of patients should be considered when permitting access to their EHRs. That is, recognizing life threatening situations in automated healthcare access control systems is imperative. Our work introduces an innovative access control method by taking into consideration machine learning techniques by estimating the patient's future health metrics, based on her recent history. The access control method provides secure access for emergency healthcare professionals to sensitive healthcare information and simultaneously safeguarding the patient's health. Results show that personalization of fuzzy context handlers improves the accuracy of the access control results, in comparison with non-personalized context handlers. Our evaluation has shown that the Personalized ABAC Fuzzy Context Handler exhibits a low percentage error in predicting the overall health criticality of a patient. The integration of the predictive mechanism within the personalized context handler proved to be a robust tool to enhance the efficiency of the access control mechanism in EHRs System.
- **It proposes a Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records.** In critical medical conditions, the patients' health criticality should be taken under consideration when allowing access to their sensitive EHRs. Thus, identifying life threatening cases in automated healthcare access control systems is imperative. This dissertation introduces a permissioned blockchain network for access control management in emergency health situations, which incorporates machine learning techniques along with a

personalized fuzzy mechanism for estimating the patient's future health metrics, related to his recent history. The access control mechanism offers secure access for emergency health care professionals to sensitive medical data. The developed access control mechanism provides secure access for emergency clinicians to sensitive information and simultaneously safeguards the patient's private data. The proposed permissioned blockchain network is capable of securing patient's sensitive information based on the personalized policies in the blockchain network. Furthermore, our approach is proactive because it provides access control based on near-future predictions about the criticality of the patient's situation. Moreover, it has the ability to track the history of who and when gained access to the sensitive patient's data so that trust is achieved as well. Limitations of our approach include the incorporation of a small number of health metrics to characterize the criticality of a patient's situation.

- **It proposes Neural-Network based context handlers for Diagnostic Access Control.** This Ph.D idissertation developed machine learning techniques based on patients' health metrics and integrated them with an ABAC paradigm which can grant access to a sensitive EHRs system by applying personalized machine learning-based context handlers which can be used so as to identify medical diseases. In addition, based on patient's health metrics and personal information, we made a prediction if the patient is in peril for hypertension or cerebrovascular diseases, by leveraging NNs. In addition, this thesis developed a sufficient web application so as to evaluate this work.

B. <u>Future Work</u>

For future work we plan to:

i. Incorporate a fully parameterized system able to adjust dynamically in real-time the number of health metrics involved in the fuzzy inferencing process as fuzzy variables, along with the fuzzy variables ranges and number of categories, as well as the fuzzy rules. Furthermore, we plan to enhance our system by incorporating logging capabilities in order to track the system's results, the time, the subject who requests access, and the corresponding patient whose sensitive data are to be accessed as well. Finally, the healthcare professional’s final decision is to be registered by our system in order to alter the fuzzy rules in the ABAC with context handlers approach and the respective thresholds in the ABAC baseline method, or alternatively the corresponding thresholds and rules can be changed in real time by the visual web interface by the healthcare professional herself.

ii. Develop additional machine learning context handlers and compare them with our already existing NN based context handlers.

iii. Insert additional personalized parameters regarding our fuzzy inferencing process.

Chapter 10

10. List of Publications

Evgenia Psarra has 7 publications in scientific journals and proceedings of international scientific conferences, which have taken 26 citations. Additionally, 1 conference paper and 2 journal papers are under review. The h-index of Evgenia Psarra is 3 and has been calculated with the application Publish or Perish (03/05/2023).

A. PhD Publications

1) Journal Publications

[J1] Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., & Mentzas, G. (2021). Accessing electronic health records in critical incidents using context-aware attribute-based access control. Intelligent Decision Technologies, 15(4), 667-679.

[J2] Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2022). Context-Based, Predictive Access Control to Electronic Health Records. Electronics, 11(19), 3040.

2) Conference Publication – Proceedings

[C1] Psarra, E., Ntetsika, N., & Apostolou, D. (2022, July). Multi-continent descriptive analytics of hypertension, obesity, and smoking. In 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-8). IEEE.

B. Other scientific works

1) Journal Publication

[J3] de Oliveira, M. T., Verginadis, Y., Reis, L. H., Psarra, E., Patiniotakis, I., & Olabarriaga, S. D. (2023). AC-ABAC: Attribute-based access control for electronic medical records during acute care. Expert Systems with Applications, 213, 119271.

2) ***Conference Publication – Proceedings***

[C2] Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., & Mentzas, G. (2020, April). A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain. In Workshops of the International Conference on Advanced Information Networking and Applications (pp. 1133-1142). Springer, Cham.

[C3] Psarra, E., Patiniotakis, I., Verginadis, Y., Apostolou, D., & Mentzas, G. (2020, July). Securing access to healthcare data with context-aware policies. In 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-6). IEEE.

[C4] Psarra, E., & Apostolou, D. (2019, July). Timetable scheduling using a hybrid particle swarm optimization with local search approach. In 2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-8). IEEE.

3) ***Accepted Scientific Work***

[C5] Psarra, E., Apostolou, D. (2023). A Combination of Genetic Algorithms and Local Search to Solve a Real Data University Timetable Scheduling Problem (IISA2023)

4) ***Under Review Scientific Works***

[J4] Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2023). Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records. BMC.

[J5] Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2023). Neural Network-based Context Handlers for Diagnostic Access Control.

Chapter 11

11. References

A. *References (Chapter 1)*

1. Dey, Anind K.: Understanding and Using Context. Personal Ubiquitous Computing (2001) 4-7
2. Ferrari, E.: Access Control in Data Management Systems. Synthesis Lectures on Data Management, Vol. 2, No. 1. Morgan & Claypool Publishers (2010)
3. Khan, A., Access control in cloud computing environment.. ARPN Journal of Engineering and Applied Sciences (2012)
4. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller R., and Scarfone K.: Guide to Attribute Based Access Control (ABAC) definition and considerations. NIST special publication (2014)
5. Sahai A., and Waters, B.: Fuzzy identity-based encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg (2005) 457-473
6. Kronenfeld MR, Bay RC, Coombs W. Survey of user preferences from a comparative trial of UpToDate and ClinicalKey. J Med Libr Assoc. 2013;101(2):151–4.
7. Isaac T, Zheng J, Ashish J. Use of UpToDate and outcomes in US hospitals. J Hosp Med. 2012;7(2):85–90.
8. Tate KE, Gardner RM, Weaver LK. A computerized laboratory alerting system. MD comput. 1990;7(5):296–301.
9. Kuperman GJ, Teich JM, Tanasijevic MJ, Ma'Luf N, Rittenberg E, Jha A, et al. Improving response to critical laboratory results with automation: results of a randomized controlled trial. J Am Med Inform Assoc. 1999;6(6):512–22.
10. Nebeker JR, Hoffman JM, Weir CR, Bennett CL, Hurdle JF. High rates of adverse drug events in a highly computerized hospital. Arch Intern Med. 2005;165(10):1111–6.
11. Magrabi F, Ammenwerth E, Hypponen H, de Keizer N, Nykanen P, Rigby M, et al. Improving evaluation to address the unintended consequences of health information technology: a position paper from the Working Group on Technology Assessment & Quality Development. Yearb Med Inform. 2016;1:61–9.

12. Lehmann CU, Seroussi B, Jaulent MC. Troubled waters: navigating unintended consequences of health information technology. Yearb Med Inform. 2016;1:5–6.

13. Mamlin BW, Tierney WM. The promise of information and communication technology in healthcare: extracting value from the chaos. Am J Med Sci. 2016;351(1):59–68.

14. Frost & Sullivan White Paper, "Drowning in Big Data? Reducing Information Technology Complexities and Costs For Healthcare Organizations". 2012. Retrieved from http://www. emc.com/collateral/analystreports/frost-sullivan-reducing-information-technology-complexities-ar.pdf.

15. Bresnick J. The difference between big data and smart data in healthcare. Available from: https://healthitanalytics.com/features/the-difference-between-big-data-and-smart-data-in-healthcare

16. Musen MA, Shahar Y, Shortliffe EH. Clinical decision-support systems. In: Shortliffe EH, Cimino JJ, editors. Biomedical informatics: computer applications in health care and biomedicine. 4th ed. London/New York: Springer; 2014.

17. Zeiger RF. McGraw-Hill's Diagnosaurus. 4.0 2018. Available from: http://accessmedicine. mhmedical.com/diagnosaurus.aspx

18. Smith M, Nazario B, Bhargava H, Cassoobhoy A. WebMD: WebMD LLC. 2018. Available from: https://www.webmd.com/

19. Scheepers-Hoeks AM, Grouls RJ, Neef C, Korsten HH. Strategy for implementation and first results of advanced clinical decision support in hospital pharmacy practice. Stud Health Technol Inform. 2009;148:142–8.

20. Latoszek-Berendsen A, Tange H, van den Herik HJ, Hasman A. From clinical practice guidelines to computer-interpretable guidelines. A literature overview. Methods Inf Med. 2010;49(6):550–70.

21. Stojadinovic A, Bilchik A, Smith D, Eberhardt JS, Ward EB, Nissan A, et al. Clinical decision support and individualized prediction of survival in colon cancer: bayesian belief network model. Ann Surg Oncol. 2013;20(1):161–74.

22. Neapolitan R, Jiang X, Ladner DP, Kaplan B. A primer on bayesian decision analysis with an application to a kidney transplant decision. Transplantation. 2016;100(3):489–96.

23. Jalali A, Bender D, Rehman M, Nadkanri V, Nataraj C. Advanced analytics for outcome prediction in intensive care units. Conf Proc IEEE Eng Med Biol Soc. 2016;2016:2520–4.

24. Shamir RR, Dolber T, Noecker AM, Walter BL, McIntyre CC. Machine learning approach to optimizing combined stimulation and medication therapies for Parkinson's disease. Brain Stimul. 2015;8(6):1025–32.

25. Tenorio JM, Hummel AD, Cohrs FM, Sdepanian VL, Pisa IT, de Fatima Marin H. Artificial intelligence techniques applied to the development of a decision-support system for diagnosing celiac disease. Int J Med Inform. 2011;80(11):793–802.

26. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? potential health benefits, savings, and costs. Health affairs, 24 , 1103–1117.

27. Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, 18 , 1431–1441.

28. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. et al. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of medical systems, 44 , 1–9.

29. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Proceedings of EUROCRYPT'05 (pp. 1–17). Springer.

30. J. Bethencourt, A. S., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In in Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, (Washington, DC, USA) (pp. 321–334). IEEE Computer Society.

31. S. Hamsanandhini, M. E., & Varanambika, V. (2022). Health record maintenance using cloud computing and multi authority attribute based encryption. In International Conference on Computer Communication and Informatics (ICCCI) (pp. 1–8). doi:https://doi.org/10.1109/ICCCI54379. 2022.9740880.

32. Oberko, O. V. . X. H., P.S.K. (2022). A survey on multi-authority and decentralized attribute-based encryption. J Ambient Intell Human Comput, 13 , 515–533. doi:https://doi.org/10.1007/s12652-021-02915-5.

33. Amit Sahai, H. S., & Waters, B. (2012). Dynamic credentials and ciphertext delegation for attribute-based encryption. In 32nd Annual Cryptology Conference on Advances in Cryptology (CRYPTO 2012) (pp. 199–217). Springer-Verlag New York, Inc. volume 7417.
34. M. Green, S. H., & Waters, B. (2011). Outsourcing the decryption of abe ciphertexts. In 20th USENIX Conference on Security, SEC'11 (pp. 34–34). USENIX Association volume 7417.
35. Verginadis, Y., Patiniotakis, I., Gouvas, P., Mantzouratos, S., Veloudis, S., Schork, S. T., Seitzluwig, L., Paraskakis, I., & Mentzas, G. (2022). Contextaware policy enforcement for paas-enabled access control. IEEE Transactions on Cloud Computing, 10, 276–291. doi:10.1109/TCC.2019.2927341.
36. Tampere, U., for E-health Research, N. C., & UMC, A. (2019). D1.2 - ASCLEPIOS Reference Architecture, Security and E-health Use Cases, and Acceptance Criteria. URL: https://doi.org/10.5281/zenodo.4022298. doi:10.5281/zenodo.4022298.
37. de Oliveira, M. T., Bakas, A., Frimpong, E., Groot, A. E., Marquering, H. A., Michalas, A., & Olabarriaga, S. D. (2020). A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud. Annals of Telecommunications, (pp. 1–17).
38. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC Medical Informatics and Decision Making. 2022 Mar 28;22(1).
39. Natsiavas P, Rasmussen J, Voss-Knude M, Votis K, Coppolino L, Campegiani P, et al. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Medical Informatics and Decision Making. 2018 Oct 16;18(1).
40. Mackey TK, Kuo TT, Gummadi B, Clauson KA, Church G, Grishin D, et al. "Fit-for-purpose?" – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine. 2019 Mar 27;17(1).

B. References (Chapter 2)

1. Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-preserving attribute-based access control model for XML-based electronic health record system. IEEE Access. 2018;6:9114–28.
2. Oasis-open.org. [cited 2021 Sep 16]. Available from: http://docs.oasis-open.org/xacml
3. Quirolgico S, Hu V, Karygiannis T. Access control for sar systems. 2011.
4. Open Policy Agent [Internet]. Openpolicyagent.org. [cited 2021 Sep 27]. Available from: https://www.openpolicyagent.org/
5. Siebach JAJ. The Abacus: A New Approach to Authorization. Brigham Young University; 2021.
6. Verginadis Y, Patiniotakis I, Gouvas P, Mantzouratos S, Veloudis S, Schork ST, et al. Context-aware policy enforcement for PaaS-enabled access control. IEEE trans cloud comput. 2019;1–1.
7. Dennis JB, Van Horn EC. Programming semantics for multiprogrammed computations. Commun ACM. 1966;9(3):143–55.
8. Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of Things. Mathematical and Computer Modelling. 2013;58(5-6):1189-1205.
9. Gong L. A secure identity-based capability system. In: Proceedings 1989 IEEE Symposium on Security and Privacy. IEEE Comput. Soc. Press; 2003.
10. Dey, Anind K.: Understanding and Using Context. Personal Ubiquitous Computing (2001) 4-7
11. Sahai A., and Waters, B.: Fuzzy identity-based encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg (2005) 457-473
12. Bethencourt, J., Sahai, A., & Waters, B.: Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07). IEEE (2007, May) 321-334
13. Müller, S., Katzenbeisser, S., and Eckert C.: Distributed attribute-based encryption. International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg (2008) 20-36

14. Moffat, S., M. Hammoudeh, and R. Hegarty: A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. Proceedings of the International Conference on Future Networks and Distributed Systems. ACM (2017)

15. Wang, S., Gao, T., & Zhang, Y.. Searchable and revocable multi-data owner attribute-based encryption scheme with hidden policy in cloud storage. Vol. 13, PloS one (2018)

16. Lewko Allison and Brent Waters: Decentralizing attribute-based encryption. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, (2011) 568-588

17. Liu, Z., Jiang, Z. L., Wang, X., & Yiu, S. M.: Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating, Vol. 108. Journal of Network and Computer Applications (2018) 112-123

18. Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D.: Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications, Vol. 140 (2019) 38-60

19. Zhang Leyou, Yilei Cui, and Yi Mu: Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. IEEE Systems Journal (2019)

20. Attrapadung, N.: Unbounded Dynamic Predicate Compositions in Attribute-Based Encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham. (2019, May) 34-67

21. Xu, Q., Tan, C., Zhu, W., Xiao, Y., Fan, Z., & Cheng, F.: Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing. Future Generation Computer Systems. (2019)

22. Li, Q., Zhu, H., Xiong, J., Mo, R., Ying, Z., & Wang, H.: Fine-grained multi-authority access control in IoT-enabled mHealth. Annals of Telecommunications, (2019) 1-12

23. Liang, P., Zhang, L., Kang, L., & Ren, J. Privacy-preserving decentralized ABE for secure sharing of personal health records in cloud storage. Journal of Information Security and Applications, Vol. 47 (2019) 258-266

24. Covington MJ, Sastry MR. A contextual attribute-based access control model. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 1996–2006.
25. Yunda L, Pacheco D, Millan J. A Web-based fuzzy inference system based tool for cardiovascular disease risk assessment. Nova. 2015;13(24):7.
26. Kalaivani K, Sivakumar R. A novel fuzzy based bio-key management scheme for medical data security. J Electr Eng Technol. 2016;11(5):1509–18.
27. Guzman JC, Melin P, Prado-Arechiga G. Design of an optimized fuzzy classifier for the diagnosis of blood pressure with a new computational method for expert rule optimization. Algorithms. 2017;10(3):79.
28. Moameri S, Samadinai N. Diagnosis of coronary artery disease via a Novel Fuzzy expert system optimized by CUCKOO SEARCH. International Journal of Engineering. 2018;31(12):2028–2036,.
29. Leyla N, MacCaull W. A personalized access control framework for workflow-based health care information. In: Business Process Management Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 273–284.
30. Zerkouk M, Cavalcante P, Mhamed A, Boudy J, Messabih B. Behavior and capability based access control model for personalized TeleHealthCare assistance. Mob Netw Appl. 2014;19(3):392–403.
31. Common Attack Pattern Enumeration and Classification (CAPEC), MITRE. Available online at: https://capec.mitre.org/
32. National Drug Code (NDC), Food and Drug Administration (FDA), Available online at: https://www.fda.gov/drugs/drug-approvals-and-databases/national-drug-code-directory
33. Health Level Seven Version 3 Standard (HL7 V3): Patient Administration, Person Registry, Release 1. Available online at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=376
34. Current Procedural Terminology (CPT), American Medical Association. Available online at: https://www.ama-assn.org/practice-management/cpt/cpt-overview-and-code-approval

35. National Uniform Claim Committee(NUCC), Version 19.1, 7/1/19, Available online at: http://www.nucc.org/index.php/code-sets-mainmenu-41/provider-taxonomy-mainmenu-40/csv-mainmenu-57
36. Systematized Nomenclature of Medicine - Clinical Terms. Available online at: http://www.snomed.org
37. Logical Observation Identifiers Names and Codes (LOINC). Available online at: https://loinc.org/faq/structure-of-loinc-codes-and-names/
38. International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10), World Health Organization (WHO). Available online at: https://icd.who.int/browse10/2016/en
39. Anatomical Therapeutic Chemical Classification System / Defined Daily Dose (ATC/DDD), Available online at: https://www.whocc.no/ddd/list_of_ddds_for_3_years_revisio/
40. Clinical Document Architecture (CDA). Available online at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
41. European Guideline on the electronic exchange of health data under CrossBorder Directive 2011/24/EU Release 2 Patient Summary for unscheduled care. Available online at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf
42. European Guideline on the electronic exchange of health data under CrossBorder Directive 2011/24/EU Release 2 ePrescriptions and eDispensations. Available online at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co091_en.pdf

C. References (Chapter 4)

1. Global Health Risks Report - WHO. Retrieved January 2, 2022, from https://www.who.int/healthinfo/global_burden_disease/GlobalHealthRisks_report_full.pdf.
2. Google Scholar. Retrieved January 2, 2022, from https://scholar.google.com/

3. U.S. National Library of Medicine. (n.d.). PubMed. National Center for Biotechnology Information. Retrieved January 2, 2022, from https://pubmed.ncbi.nlm.nih.gov/
4. Kengne, A. P., Awah, P. K., Fezeu, L., & Mbanya, J. C. (2007). The burden of high blood pressure and related risk factors in urban sub-Saharan Africa: evidences from Douala in Cameroon. African health sciences, 7(1).
5. Bello, S. I., Ojieabu, W. A., & Bello, I. K. (2016). Prevalence of Hypertension Among Fulani Herdsmen in Rural Community of Nigeria. Bangladesh Journal of Medicine, 27(2), 48-54.
6. Bello, S. I., Ojieabu, W. A., & Bello, I. K. (2016). Prevalence and risk factors of hypertension among Fulani herdsmen in Rural Community of Nigeria.
7. Hussain, A. A., Elzubier, A. G., & Ahmed, M. E. K. (1999). Target organ involvement in hypertensive patients in Eastern Sudan. Journal of human hypertension, 13(1), 9-12.
8. Prakaschandra, R., & Naidoo, D. P. (2017). Increased waist circumference is the main driver for the development of the metabolic syndrome in South African Asian Indians. Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 11, S81-S85.
9. Duarte-Clíments, G., Mauricio, T. F., Gómez-Salgado, J., Moreira, R. P., Romero-Martín, M., & Sánchez-Gómez, M. B. (2021, January). Assessment of Cardiovascular Risk Factors in Young Adults through the Nursing Diagnosis: A Cross-Sectional Study among International University Students. In Healthcare (Vol. 9, No. 1, p. 91). Multidisciplinary Digital Publishing Institute.
10. MH, R., Halla, I., AI, A., & AMM, E. (2016). ENVIRONMENTAL INDICATORS LEADING TO CARDIAC MALFUNCTION AMONG TEXTILE WORKERS. Journal of Environmental Science, 36(2), 17-39.
11. Lo, K., Woo, B., Wong, M., & Tam, W. (2018). Subjective sleep quality, blood pressure, and hypertension: a meta-analysis. The Journal of Clinical Hypertension, 20(3), 592-605.
12. Tyrovolas, S., Koyanagi, A., Garin, N., Olaya, B., Ayuso-Mateos, J. L., Miret, M., ... & Haro, J. M. (2015). Determinants of the components of arterial pressure among older adults–The role of anthropometric and clinical factors: A multi-continent study. Atherosclerosis, 238(2), 240-249.

13. PubMed_ Angaw, K., Dadi, A. F., & Alene, K. A. (2015). Prevalence of hypertension among federal ministry civil servants in Addis Ababa, Ethiopia: a call for a workplace-screening program. BMC cardiovascular disorders, 15(1), 1-6.
14. Bhupatiraju, C., Saini, D., Patkar, S., Deepak, P., Das, B., & Padma, T. (2012). Association of shorter telomere length with essential hypertension in Indian population. American Journal of Human Biology, 24(4), 573-578.
15. Yosefy, C., Dicker, D., Viskoper, J. R., Tulchinsky, T. H., Ginsberg, G. M., Leibovitz, E., & Gavish, D. (2003). The Ashkelon Hypertension Detection and Control Program (AHDC Program): a community approach to reducing cardiovascular mortality☆. Preventive medicine, 37(6), 571-576.
16. Tomitani, N., Hoshide, S., Buranakitjaroen, P., Chia, Y. C., Park, S., Chen, C. H., ... & HOPE Asia Network. (2021). Regional differences in office and self-measured home heart rates in Asian hypertensive patients: AsiaBP@ Home study. The Journal of Clinical Hypertension, 23(3), 606-613.
17. Girisha, B. S., & Thomas, N. (2017). Metabolic syndrome in psoriasis among urban South Indians: a case control study using SAM-NCEP criteria. Journal of clinical and diagnostic research: JCDR, 11(2), WC01.
18. Bhowmik, B., Munir, S. B., Ahmed, K. R., Siddiquee, T., Diep, L. M., Wright, E., ... & Hussain, A. (2014). Anthropometric indices of obesity and type 2 diabetes in Bangladeshi population: Chandra Rural Diabetes Study (CRDS). Obesity research & clinical practice, 8(3), e220-e229.
19. Gandhi, G., Mehta, T., Contractor, P., & Tung, G. (2018). Genotoxic damage in end-stage renal disease. Mutation Research/Genetic Toxicology and Environmental Mutagenesis, 835, 1-10.
20. Terra, N., Moriguchi, Y., Bittencourt, L., Trois, R. S., Piccoli, J. E. C., & Cruz, I. B. M. (2011). Apolipoprotein E polymorphism in elderly Japanese-Brazilian immigrants does not explain the reduced cardiovascular risk factor incidence. Genetics and Molecular Research, 10(3), 1975-1985.
21. Hassan, N. S. M. Risk factors for Diabetic foot amputation in sample of Iraqi patients.
22. Helvaci, M. R., Aydin, Y., & Gundogdu, M. (2012). Smoking induced atherosclerosis in cancers. HealthMED, 6(11), 3744-3749.

23. Sankar, P., Subhramaniyan, T., Paulraj, M. S., Jayanthi, J., & Ragunathan, M. G. Diabetic Neuropathy Prediction by Logistic Model.
24. Mihir, G., Parul, P., Sunil, N., HK, M., Rakesh, S., Dharmesh, D., & Patel, R. K. (2010). Needle stick and sharp instruments injuries among health care providers at cardiology institute, Ahmedabad. National Journal, 1(2), 114.
25. Wang, Y., Xu, H., Qian, Y., Guan, J., Yi, H., & Yin, S. (2017). Patients with obstructive sleep apnea display decreased flow-mediated dilatation: evidence from a meta-analysis. Medical science monitor: international medical journal of experimental and clinical research, 23, 1069.
26. Heilbrunn, E. S., Ssentongo, P., Chinchilli, V. M., & Ssentongo, A. E. (2020). Sudden death in patients with sleep apnea: a systematic review and meta-analysis. medRxiv.
27. Amraoui, F., Van Der Hoeven, N. V., Van Valkengoed, I. G., Vogt, L., & Van Den Born, B. J. H. (2014). Mortality and cardiovascular risk in patients with a history of malignant hypertension: a case-control study. The Journal of Clinical Hypertension, 16(2), 122-126.
28. Hogg, R. E., Woodside, J. V., Gilchrist, S. E., Graydon, R., Fletcher, A. E., Chan, W., ... & Chakravarthy, U. (2008). Cardiovascular disease and hypertension are strong risk factors for choroidal neovascularization. Ophthalmology, 115(6), 1046-1052.
29. Cardaropoli, S., Giuffrida, D., Piazzese, A., & Todros, T. (2015). Helicobacter pylori seropositivity and pregnancy-related diseases: a prospective cohort study. Journal of reproductive immunology, 109, 41-47.
30. Brandl, C., Breinlich, V., Stark, K. J., Enzinger, S., Aßenmacher, M., Olden, M., ... & Heid, I. M. (2016). Features of age-related macular degeneration in the general adults and their dependency on age, sex, and smoking: results from the German KORA study. PloS one, 11(11), e0167181.
31. Portillo Baquedano, M. P., & PREDIMED-PLUS Investigators. (2019). Association of lifestyle factors and inflammation with sarcopenic obesity: data from the PREDIMED-Plus trial.
32. Adriana, G. (2013). PREVALENCE OF OBESITY IN ADULT PATIENTS WITH DIABETES MELLITUS TYPE 2 AND AUTOIMMUNE CHRONIC THYROIDITIS. European Scientific Journal, 9(36).

33. PubMed_ Society, B. C., Society, B. H., Diabetes, U. K., Society, P. C. C., & Stroke Association. (2005). JBS 2: Joint British Societies' guidelines on prevention of cardiovascular disease in clinical practice. Heart (British Cardiac Society), 91(Suppl 5), v1-v52.
34. Feio, C. M. A., Fonseca, F. A., Rego, S. S., Feio, M. N., Elias, M. C., Costa, E. A., ... & Carvalho, A. C. (2003). Lipid profile and cardiovascular risk in two Amazonian populations. Arquivos brasileiros de cardiologia, 81, 596-599.
35. Bermúdez, V., Rojas, J., Salazar, J., Calvo, M. J., Morillo, J., Torres, W., ... & Cano-Ponce, C. (2014). The Maracaibo city metabolic syndrome prevalence study: primary results and agreement level of 3 diagnostic criteria. Revista Latinoamericana de Hipertensión, 9(4), 20-32.
36. Valmore Bermúdez, M. D., Salazar, J., Bsc, M. J. C., Bsc, J. M., Bsc, W. T., Bsc, C. C., ... & Añez, R. (2014). The Maracaibo city metabolic syndrome prevalence study: primary results and agreement level of 3 diagnostic criteria/Estudio de Prevalencia de Síndrome Metabólico: resultados preliminares y nivel de concordancia de 3 criterios diagnósticos. Revista Latinoamericana de Hipertension, 9(4), 20.
37. Zioupos, M. E., Takai, J., Ahmad, M., & Zioupos, P. The diabetes epidemic in the South Pacific: a pilot study utilising hand grip strength in Tonga.
38. Neuhauser, H., Thamm, M., & Ellert, U. (2013). Blutdruck in Deutschland 2008–2011. Bundesgesundheitsblatt-Gesundheitsforschung-Gesundheitsschutz, 56(5-6), 795-801.
39. Pereira, M., Carreira, H., Vales, C., Rocha, V., Azevedo, A., & Lunet, N. (2012). Trends in hypertension prevalence (1990–2005) and mean blood pressure (1975–2005) in Portugal: a systematic review. Blood pressure, 21(4), 220-226.
40. Vera, G., Nataša, D., Svetlana, K., Sonja, Š., Jasmina, G., & Sonja, T. (2012). Epidemiology of hypertension in Serbia: results of a National Survey. Journal of epidemiology, 22(3), 261-266.
41. Zhou, Y., Jia, L., Lu, B., Gu, G., Hu, H., Zhang, Z., ... & Cui, W. (2019). Updated hypertension prevalence, awareness, and control rates based on the 2017ACC/AHA high blood pressure guideline. The Journal of Clinical Hypertension, 21(6), 758-765.

42. Ramakrishnan, S., Zachariah, G., Gupta, K., Rao, J. S., Mohanan, P. P., Venugopal, K., ... & Banerjee, S. C. A. (2019). Prevalence of hypertension among Indian adults: results from the great India blood pressure survey. Indian heart journal, 71(4), 309-313.

43. Artyukhov, I. P., Grinshtein, Y. I., Petrova, M. M., Shabalin, V. V., & Ruf, R. R. (2017). Prevalence of arterial hypertension in the Krasnoyarsk Krai (Siberia, Russia). BMC cardiovascular disorders, 17(1), 1-6.

44. Azizi, F., Ghanbarian, A., Madjid, M., & Rahmani, M. (2002). Distribution of blood pressure and prevalence of hypertension in Tehran adult population: Tehran Lipid and Glucose Study (TLGS), 1999–2000. Journal of human hypertension, 16(5), 305-312.

45. Gnatiuc, L., Alegre-Díaz, J., Halsey, J., Herrington, W. G., López-Cervantes, M., Lewington, S., ... & Kuri-Morales, P. (2017). Adiposity and blood pressure in 110 000 Mexican adults. Hypertension, 69(4), 608-614.

46. Kadiri, S., Walker, O., Salako, B. L., & Akinkugbe, O. (1999). Blood pressure, hypertension and correlates in urbanised workers in Ibadan, Nigeria: a revisit. Journal of human hypertension, 13(1), 23-27.

47. Poulter, N. E. I. L., Khaw, K. T., Hopwood, B. E., Mugambi, M. U. T. A. M. A., Peart, W. S., Rose, G. E. O. F. F. R. E. Y., & Sever, P. S. (1984). Blood pressure and associated factors in a rural Kenyan community. Hypertension, 6(6_pt_1), 810-813.

48. Leite, C. D. M. B. A., Di Renzo, L., Salimei, P. S., Gualtieri, P., Schieferdecker, M. M., Vilela, R. M., ... & De Lorenzo, A. (2018). Lean body mass: reference values for Italian population between 18 to 88 years old. European review for medical and pharmacological sciences, 22, 7891-7898.

49. Reas, D. L., Nygård, J. F., Svensson, E., Sørensen, T., & Sandanger, I. (2007). Changes in body mass index by age, gender, and socio-economic status among a cohort of Norwegian men and women (1990–2001). BMC public health, 7(1), 1-7.

50. Abaci, A., Oguz, A., Kozan, O., Toprak, N., Senocak, H., Deger, N., ... & Erol, C. (2006). Treatment and control of hypertension in Turkish population: a survey on high blood pressure in primary care (the TURKSAHA study). Journal of human hypertension, 20(5), 355-361.

51. Ahranjani, S. A., Kashani, H., Forouzanfar, M. H., Meybodi, H. A., Larijani, B., Aalaa, M., & Mohajeri-Tehrani, M. R. (2012). Waist circumference, weight, and body mass index of iranians based on national non-communicable disease risk factors surveillance. Iranian journal of public health, 41(4), 35.
52. Chhabra, P., & Chhabra, S. K. (2007). Distribution and determinants of body mass index of non-smoking adults in Delhi, India. Journal of health, population, and nutrition, 25(3), 294.
53. Hayes, A., Gearon, E., Backholer, K., Bauman, A., & Peeters, A. (2015). Age-specific changes in BMI and BMI distribution among Australian adults using cross-sectional surveys from 1980 to 2008. International Journal of Obesity, 39(8), 1209-1216.
54. DiBonaventura, M., Nicolucci, A., Meincke, H., Le Lay, A., & Fournier, J. (2018). Obesity in Germany and Italy: prevalence, comorbidities, and associations with patient outcomes. ClinicoEconomics and outcomes research: CEOR, 10, 457.
55. Papathanasiou, G., Zerva, E., Zacharis, I., Papandreou, M., Papageorgiou, E., Tzima, C., ... & Evangelou, A. (2015). Association of high blood pressure with body mass index, smoking and physical activity in healthy young adults. The open cardiovascular medicine journal, 9, 5.
56. Polonia, J., Martins, L., Pinto, F., & Nazare, J. (2014). Prevalence, awareness, treatment and control of hypertension and salt intake in Portugal: changes over a decade. The PHYSA study. Journal of hypertension, 32(6), 1211-1221.
57. Faizi, N., & Kazmi, S. (2017). Universal health coverage-There is more to it than meets the eye. Journal of family medicine and primary care, 6(1), 169.
58. Pengpid, S., & Peltzer, K. (2021). Overweight and obesity among adults in Iraq: prevalence and correlates from a National Survey in 2015. International Journal of Environmental Research and Public Health, 18(8), 4198.
59. Ahmed, H., & Thaver, I. H. (2020). Hypertension and obesity in community of Nain-Sukh. JPMA. The Journal of the Pakistan Medical Association, 70(4), 482-487.
60. Barquera, S., Campos-Nonato, I., Hernández-Barrera, L., Villalpando, S., Rodríguez-Gilabert, C., Durazo-Arvizú, R., & Aguilar-Salinas, C. A. (2010). Hypertension in Mexican adults: results from the National Health and Nutrition Survey 2006. salud pública de méxico, 52, S63-S71.

61. Almeida, J. B., Kian, K. O., Lima, R. C., & Souza, M. C. C. D. (2016). Total and abdominal adiposity and hypertension in indigenous women in Midwest Brazil. PloS one, 11(6), e0155528.

62. Gabal, M. S., Abd Elaziz, K. M., Mostafa, N. S., & Khallaf, M. K. (2018). Prevalence of hypertension and quality of life among hypertensive patients in an Egyptian village. Egypt J Communit Med, 36(2).

63. Gatimu, S. M., & John, T. W. (2020). Socioeconomic inequalities in hypertension in Kenya: a decomposition analysis of 2015 Kenya STEPwise survey on non-communicable diseases risk factors. International journal for equity in health, 19(1), 1-11.

64. Abdelbagi, O., Musa, I. R., Musa, S. M., ALtigani, S. A., & Adam, I. (2021). Prevalence and associated factors of hypertension among adults with diabetes mellitus in northern Sudan: a cross-sectional study. BMC cardiovascular disorders, 21(1), 1-7.

65. Gaio, V., Antunes, L., Namorado, S., Barreto, M., Gil, A., Kyslaya, I., ... & INSEF Research group. (2018). Prevalence of overweight and obesity in Portugal: results from the first Portuguese Health Examination Survey (INSEF 2015). Obesity research & clinical practice, 12(1), 40-50.

66. Dare, S., Mackay, D. F., & Pell, J. P. (2015). Relationship between smoking and obesity: a cross-sectional study of 499,504 middle-aged adults in the UK general population. PloS one, 10(4), e0123579.

67. Sun, M., Jiang, Y., Sun, C., Li, J., Guo, X., Lv, Y., ... & Jin, L. (2019). The associations between smoking and obesity in northeast China: a quantile regression analysis. Scientific reports, 9(1), 1-6.

68. Mohammadian, M., Sarrafzadegan, N., Roohafza, H. R., Sadeghi, M., Hasanzadeh, A., & Rejali, M. (2018). A Comparative Study on the Prevalence and Related Factors of Cigarette Smoking in Iran and Other Asian Countries: Results of Isfahan Cohort Study (ICS). World Cancer Research Journal, 5(4).

69. DiBonaventura, M. D., Meincke, H., Le Lay, A., Fournier, J., Bakker, E., & Ehrenreich, A. (2018). Obesity in Mexico: prevalence, comorbidities, associations with patient outcomes, and treatment experiences. Diabetes, metabolic syndrome and obesity: targets and therapy, 11, 1.

70. Kudel, I., Alves, J. S., de Menezes Goncalves, T., Kull, K., & Nørtoft, E. (2018). The association between body mass index and health and economic outcomes in Brazil. Diabetology & metabolic syndrome, 10(1), 1-11.

71. Omar, S. M., Taha, Z., Hassan, A. A., Al-Wutayd, O., & Adam, I. (2020). Prevalence and factors associated with overweight and central obesity among adults in the Eastern Sudan. PloS one, 15(4), e0232624.

72. Pallangyo, P., Mkojera, Z. S., Hemed, N. R., Swai, H. J., Misidai, N., Mgopa, L., ... & Janabi, M. (2020). Obesity epidemic in urban Tanzania: a public health calamity in an already overwhelmed and fragmented health system. BMC endocrine disorders, 20(1), 1-9.

73. Gatimu, S. M., & John, T. W. (2020). Socioeconomic inequalities in hypertension in Kenya: a decomposition analysis of 2015 Kenya STEPwise survey on non-communicable diseases risk factors. International journal for equity in health, 19(1), 1-11.

74. Liang Y, Liu G, Chen Z, Elgendi M. PPG-BP Database [Internet]. figshare. 2021 [cited 18 September 2021]. Available from: https://figshare.com/articles/dataset/PPG-BP_Database_zip/5459299

75. Quesada, P. J. (2019, January 14). Dataset of "A retrospective international study on factors associated with injury, discomfort and pain perception among cyclists." Mendeley Data. Retrieved February 19, 2022, from https://data.mendeley.com/datasets/dg9hf7kk46/1

76. Framingham CHD dataset. (2021, February 22). Kaggle. Retrieved February 19, 2022, from https://www.kaggle.com/captainozlem/ framingham-chd-preprocessed-data

77. pima-indians-diabetes.csv. (2018, February 27). Kaggle. Retrieved February 19, 2022, from https://www.kaggle.com/kumargh/ pimaindiansdiabetescsv

78. Cundiff, D. (2021, December 13). Global burden of disease analysis dataset of Noncommunicable Disease Outcomes, Risk Factors, and SAS codes. Mendeley Data. Retrieved February 20, 2022, from https://data.mendeley.com/datasets/g6b39zxck4/7

79. NCD-RisC - BP dataset. NCD-RisC. Retrieved February 20, 2022, from https://ncdrisc.org/data-downloads-blood-pressure.html

80. NCD-RisC - BMI dataset. NCD-RisC. Retrieved February 20, 2022, from https://ncdrisc.org/data-downloads-adiposity.html
81. NCD-RisC - Hypertension dataset. NCD-RisC. Retrieved February 20, 2022, from https://ncdrisc.org/data-downloads-hypertension.html
82. WHO - Smoking dataset. WHO. Retrieved February 20, 2022, from https://apps.who.int/gho/data/node.main.TOBAGESTDCURR?langen

D. <u>References (Chapter 5)</u>

1. Ferrari E. Access control in data management systems. Synth lect data manag. 2010;2(1):1–117.
2. Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to attribute based access control (abac) definition and considerations. 2014.
3. Dey AK. Understanding and using context. Pers Ubiquitous Comput. 2001;5(1):4–7.
4. Yanase J, Triantaphyllou E. A systematic survey of computer-aided diagnosis in medicine: Past and present developments. Expert Systems with Applications. 2019;138:112821.
5. Zadeh L. Fuzzy sets. Information and Control. 1965;8(3):338-353.
6. Zadeh L. The concept of a linguistic variable and its application to approximate reasoning—II. Information Sciences. 1975;8(4):301-357.
7. American Heart Association [Internet]. Heart.org. [cited 2021 Sep 17]. Available from: https://www.heart.org/
8. Mahmood U, Al-Jumaily A, Al-Jaafreh M. Type-2 fuzzy classification of blood pressure parameters. In: 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE; 2007. p. 595–600.
9. Lapum JL, Verkuyl M, Garcia W, St-Amant O, Tan A. Vital Sign Measurement Across the Lifespan-1st Canadian Edition. 2018.
10. Low blood pressure (hypotension) [Internet]. Nhs.uk. [cited 2021 Sep 17]. Available from: https://www.nhs.uk/conditions/low-blood-pressure-hypotension/
11. Abdullah AA, Fadil NS, Khairunizam W. Development of fuzzy expert system for diagnosis of diabetes. In: 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA). IEEE; 2018. p. 1–8.

12. Al-Dmour JA, Sagahyroon A, Al-Ali AR, Abusnana S. A fuzzy logic-based warning system for patients classification. Health Informatics J. 2019;25(3):1004–1024.
13. Target heart rate and estimated maximum heart rate [Internet]. Cdc.gov. 2020 [cited 2021 Sep 18]. Available from: https://www.cdc.gov/physicalactivity/basics/measuring/heartrate.htm
14. Gutierrez PP. CloudEHRServer by CaboLabs [Internet]. Cloudehrserver.com. [cited 2021 Sep 18]. Available from: https://cloudehrserver.com/
15. Sam Heard TB. openEHR Home [Internet]. Openehr.org. [cited 2021 Sep 18]. Available from: https://www.openehr.org/
16. Liang Y, Liu G, Chen Z, Elgendi M. PPG-BP Database [Internet]. figshare. 2021 [cited 18 September 2021]. Available from: https://figshare.com/articles/dataset/PPG-BP_Database_zip/5459299

E. References (Chapter 6)

1. Ferrari, E. Access Control in Data Management Systems. Synth. Lect. Data Manag. 2010, 2, 1–117. https://doi.org/10.2200/s00281ed1v01y201005dtm004.
2. Hu, V.C.; Ferraiolo, D.; Kuhn, R.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Spec. Publ. 2013, 800, 162. https://doi.org/10.6028/nist.sp.800-162.
3. Dey, A.K. Understanding and Using Context. Pers. Ubiquitous Comput. 2001, 5, 4–7. https://doi.org/10.1007/s007790170019.
4. Simpao, A. F., Ahumada, L. M., Gálvez, J. A., & Rehman, M. A. (2014). A review of analytics and clinical informatics in health care. Journal of medical systems, 38(4), 1-7.
5. Cortada, J. W., Gordon, D., & Lenihan, B. (2012). The value of analytics in healthcare: From insights to outcomes. IBM Global Business Services, Executive Report.
6. Tomar, D., & Agarwal, S. (2013). A survey on Data Mining approaches for Healthcare. International Journal of Bio-Science and Bio-Technology, 5(5), 241-266.
7. Lustig, I., Dietrich, B., Johnson, C., & Dziekan, C. (2010). The analytics journey. Analytics Magazine, 3(6), 11-13.

8. Khalifa, M. (2018). Health Analytics Types, Functions and Levels: A Review of Literature. ICIMTH, 137-140.

9. Basu, A. T. A. N. U. (2013). Five pillars of prescriptive analytics success. Analytics magazine, 8-12.

10. Bernstein, J. H. (2009). The data-information-knowledge-wisdom hierarchy and its antithesis.

11. Khalifa, M. (2015). Reducing emergency department crowding using health analytics methods: designing AnEvidence based decision algorithm. Procedia Computer Science, 63, 409-416.

12. Madsen, L. (2012). Healthcare Business Intelligence: A Guide to Empowering Successful Data Reporting and Analytics. John Wiley & Sons

13. Kohn, M. S., Sun, J., Knoop, S., Shabo, A., Carmeli, B., Sow, D., ... & Rapp, W. (2014). IBM's health analytics and clinical decision support. Yearbook of medical informatics, 23(01), 154-162.

14. Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS quarterly, 1165-1188.

15. Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. (2014). Big data in health care: using analytics to identify and manage high-risk and high-cost patients. Health affairs, 33(7), 1123-1131.

16. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735-1780.

17. Yin, J., Han, J., Xie, R., Wang, C., Duan, X., Rong, Y., ... & Tao, J. (2021). MC-LSTM: Real-Time 3D Human Action Detection System for Intelligent Healthcare Applications. IEEE Transactions on Biomedical Circuits and Systems, 15(2), 259-269.

18. Kadri, F., Baraoui, M., & Nouaouri, I. (2019, September). An LSTM-based deep learning approach with application to predicting hospital emergency department admissions. In 2019 International Conference on Industrial Engineering and Systems Management (IESM) (pp. 1-6). IEEE.

19. Tsai, F. S., Weng, Y. M., Ng, C. J., & Lee, C. C. (2017, October). Embedding stacked bottleneck vocal features in a LSTM architecture for automatic pain level

classification during emergency triage. In 2017 Seventh International Conference on Affective Computing and Intelligent Interaction (ACII) (pp. 313-318). IEEE.

20. Mantas, J. (2020). Using long short-term memory (LSTM) neural networks to predict emergency department wait time. The Importance of Health Informatics in Public Health during a Pandemic, 272, 199.
21. Nwakanma, C. I., Islam, F. B., Maharani, M. P., Kim, D. S., & Lee, J. M. (2021, April). Iot-based vibration sensor data collection and emergency detection classification using long short term memory (lstm). In 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 273-278). IEEE.
22. Reddy, B. K., & Delen, D. (2018). Predicting hospital readmission for lupus patients: An RNN-LSTM-based deep-learning methodology. Computers in biology and medicine, 101, 199-209.
23. Zhang, W., Li, L., Zhu, Y., Yu, P., & Wen, J. (2022). CNN-LSTM neural network model for fine-grained negative emotion computing in emergencies. Alexandria Engineering Journal, 61(9), 6755-6767.
24. Mou, H., & Yu, J. (2021). CNN-LSTM prediction method for blood pressure based on pulse wave. Electronics, 10(14), 1664.
25. Chae, M., Han, S., & Lee, H. (2020). Outdoor particulate matter correlation analysis and prediction based deep learning in the Korea. Electronics, 9(7), 1146.
26. Mumtaz, R., Zaidi, S. M. H., Shakir, M. Z., Shafi, U., Malik, M. M., Haque, A., ... & Zaidi, S. A. R. (2021). Internet of things (Iot) based indoor air quality sensing and predictive analytic—a covid-19 perspective. Electronics, 10(2), 184.
27. Oasis-open.org. Available online: http://docs.oasis-open.org/xacml (accessed on 16 September 2021).
28. Quirolgico, S.; Hu, V.; Karygiannis, T. Access Control for SAR Systems; Department of Commerce US: Washington, DC, USA, 2011. https://doi.org/10.6028/nist.ir.7815.
29. Rasjid, Z.E.; Setiawan, R.; Effendi, A. A Comparison: Prediction of Death and Infected COVID-19 Cases in Indonesia Using Time Series Smoothing and LSTM Neural Network. Procedia Comput. Sci. 2021, 179, 982–988. https://doi.org/10.1016/j.procs.2021.01.102.

30. Brownlee, J. Deep learning for time series forecasting: Predict the future with MLPs, CNNs and LSTMs in Python. In Machine Learning Mastery; Jason Brownlee: Cambridge, MA, USA, 2018.
31. Silva, I.; Moody, G.; Mark, R.; Celi, L.A. Predicting mortality of ICU patients: The PHYSIONET/computing in cardiology challenge 2012. Predicting Mortality of ICU Patients: The PhysioNet/Computing in Cardiology Challenge 2012 v1.0.0. Available online: https://physionet.org/content/challenge-2012/1.0.0/ (accessed on 24 March 2020).
32. Joshi, M.; Joshi, K.; Finin, T. Attribute Based Encryption for Secure Access to Cloud Based EHR Systems. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)), San Francisco, CA, USA, 2–7 July 2018.
33. Gutierrez, P.P. Cloud EHRServer by CaboLabs. Available online: https://cloudehrserver.com/ (accessed on 18 September 2021).
34. Sam Heard, T.B. OpenEhr Home. Available online: https://www.openehr.org/ (accessed on 18 September 2021).

F. <u>References (Chapter 7)</u>

1. Ferrari E. Access Control in Data Management Systems. Synthesis Lectures on Data Management. 2010 Jan;2(1):1–117.
2. Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Guide to Attribute Based Access Control (ABAC) Definition and Considerations [Internet]. 2014 Jan; Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf
3. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC Medical Informatics and Decision Making. 2022 Mar 28;22(1).
4. Natsiavas P, Rasmussen J, Voss-Knude M, Votis K, Coppolino L, Campegiani P, et al. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Medical Informatics and Decision Making. 2018 Oct 16;18(1).

5. Mackey TK, Kuo TT, Gummadi B, Clauson KA, Church G, Grishin D, et al. “Fit-for-purpose?” – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine. 2019 Mar 27;17(1).
6. Silva I;Moody G;Scott DJ;Celi LA;Mark RG; Predicting in-hospital mortality of ICU patients: The PHYSIONET/computing in cardiology challenge 2012 [Internet]. Computing in cardiology. U.S. National Library of Medicine; [cited 2023Apr13]. Available from: https://pubmed.ncbi.nlm.nih.gov/24678516/
7. Benet J. IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3) [Internet]. Arxiv.org. [cited 2023 Apr 13]. Available from: http://arxiv.org/abs/1407.3561v1
8. Sookhak M, Jabbarpour MR, Safa NS, Yu FR. Blockchain and smart contract for access control in Healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications. 2021;178:102950.
9. Ben-Assuli O, Ziv A, Sagi D, Ironi A, Leshno M. Cost-effectiveness evaluation of EHR: Simulation of an abdominal aortic aneurysm in the emergency department. Journal of Medical Systems. 2016;40(6).
10. Povey D. Optimistic security. Proceedings of the 1999 workshop on New security paradigms. 1999;
11. Saberi MA, Adda M, Mcheick H. Towards an abac break-glass to access emrs in case of emergency based on Blockchain. 2021 IEEE International Conference on Digital Health (ICDH). 2021;
12. Saberi M, Adda M, Mcheick H. Break-glass conceptual model for distributed EHR Management System based on Blockchain, ipfs and ABAC [Internet]. Semantic Scholar. 1970 [cited 2023Apr13]. Available from: https://www.semanticscholar.org/paper/Break-Glass-Conceptual-Model-for-Distributed-EHR-on-Saberi-Adda/855245dd019b04671bbab84765b116b77906a1a7
13. Manasa D, Khanna KR. Sharing of PHR’s in Cloud Computing. Int J Comput Sci Netw Secur (IJCSNS). 2015;15.
14. Tsegaye T, Flowerday S. A Clark-Wilson and ANSI role-based access control model. Inf Comput Secur [Internet]. 2020;28(3):373–95. Available from: http://dx.doi.org/10.1108/ics-08-2019-0100

15. Farinha P, Cruz-Correia R, Antunes L, Almeida F, Ferreira A. From Legislation to Practice-A Case Study of Break the Glass in Healthcare. In: International Conference on Health Informatics. Arlington, VI, USA; 2010. p. 114–20.
16. Georgakakis E, Nikolidakis SA, Vergados DD, Douligeris C. Spatio temporal emergency role based access control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism. In: 2011 IEEE Symposium on Computers and Communications (ISCC). IEEE; 2011.
17. Marinovic S, Craven R, Ma J, Dulay N. Rumpole: A flexible break-glass access control model. In: Proceedings of the 16th ACM Symposium on Access Control Models and Technologies. New York, NY, USA, 7-9; 2011. p. 73–82.
18. Maw HA, Xiao H, Christianson B, Malcolm JA. An evaluation of break-the-glass access control model for medical data in wireless sensor networks. In: 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE; 2014.
19. Guan S, Wang Y, Shen J. Fingerprint-based access to personally controlled health records in emergency situations. Science China Information Sciences. 2017;61(5).
20. Künzi J, Koster P, Petković M. Emergency access to Protected Health Records [Internet]. Home Page. IOS Press; 2009 [cited 2023Apr13]. Available from: https://doi.org/10.3233/978-1-60750-044-5-705
21. Covington MJ, Sastry MR. A contextual attribute-based access control model. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 1996–2006.
22. Dey AK. Understanding and using context. Pers Ubiquitous Comput [Internet]. 2001;5(1):4–7. Available from: http://dx.doi.org/10.1007/s007790170019
23. Nomikos GD, Dounias G, Tselentis G, Vemmos K. Conventional vs. fuzzy modeling of diagnostic attributes for classifying acute stroke cases. In: Proceedings of the ESIT-2000, European Symposium on Intelligent Techniques. Aachen, Germany, 9; 2000. p. 192–200.
24. Mahmood U, Al-Jumaily A, Al-Jaafreh M. Type-2 fuzzy classification of blood pressure parameters. In: 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE; 2007.

25. Djam XY, Kimbi YH. Fuzzy expert system for the management of hypertension. The Pacific Journal of Science and Technology. 2011;12(1):390–402.
26. Moameri S, Samadinai N. Diagnosis of coronary artery disease via a Novel Fuzzy expert system optimized by CUCKOO SEARCH. Int J Engineering. 2018;31:2028–2036.
27. Zerkouk M, Mhamed A, Messabih B. A user profile based access control model and architecture. Int J Comput Netw Commun [Internet]. 2013;5(1):171–81. Available from: http://dx.doi.org/10.5121/ijcnc.2013.5112
28. Røstad L, Nytrø Ø. Personalized access control for a personally controlled health record. In: Proceedings of the 2nd ACM workshop on Computer security architectures. New York, NY, USA: ACM; 2008.
29. Petković M, Conrado C, Hammoutène M. Cryptographically enforced personalized role-based access control. In: Security and Privacy in Dynamic Environments. Boston, MA: Springer US; 2006. p. 364–76.
30. Son J, Kim J-D, Na H-S, Baik D-K. Dynamic access control model for privacy preserving personalized healthcare in cloud environ-ment. Technol Health Care [Internet]. 2015;24(s1):S123–9. Available from: http://dx.doi.org/10.3233/thc-151059
31. Son HX, Le TH, Quynh NTT, Huy HND, Duong-Trung N, Luong HH. Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems. In: Mobile, Secure, and Programmable Networking. Cham: Springer International Publishing; 2021. p. 44–56.
32. Le HT, Thanh LNT, Vo HK, Luong HH, Tuan KNH, Anh TD, et al. Patient-Chain: Patient-centered Healthcare System a Blockchain-based Technology in Dealing with Emergencies. In: International Conference on Parallel and Distributed Computing: Applications and Technologies. Cham: Springer; 2022. p. 576–83.
33. Morelli U, Ranise S, Sartori D, Sciarretta G, Tomasi A. Audit-based access control with a distributed ledger: Applications to healthcare organizations. In: Security and Trust Management. Cham: Springer International Publishing; 2019. p. 19–35.
34. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using Blockchain Technology. PLOS ONE. 2020;15(12).

35. Zhan W, Chen CL, Weng W, Tsaur WJ, Lim ZY, Deng YY. Incentive EMR Sharing System Based on Consortium Blockchain and IPFS. In Healthcare. Vol. 10. MDPI; 2022.
36. Malamas, V., Palaiologos, G., Kotzanikolaou, P., Burmester, M., & Glynos, D. (2022). Janus: Hierarchical Multi-Blockchain-Based Access Control (HMBAC) for Multi-Authority and Multi-Domain Environments. Applied Sciences, 13(1), 566
37. Sultana M, Hossain A, Laila F, Taher KA, Islam MN. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med Inform Decis Mak [Internet]. 2020;20(1):256. Available from: http://dx.doi.org/10.1186/s12911-020-01275-y
38. Ma S, Cao Y, Xiong L. Efficient logging and querying for blockchain-based cross-site Genomic Dataset Access Audit. BMC Medical Genomics. 2020;13(S7).
39. Gürsoy G, Brannon CM, Gerstein M. Using ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Medical Genomics. 2020;13(1).
40. Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A hierarchical multi blockchain for fine grained access to medical data. Ieee Access, 8, 134393-134412.
41. A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
42. Amit Sahai, Hakan Seyalioglu, and Brent Waters. 2012. Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption. In Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology (CRYPTO 2012) - Volume 7417, Reihaneh SafaviNaini and Ran Canetti (Eds.), Vol. 7417. Springer-Verlag New York, Inc., New York, NY, USA, 199-217.
43. Yin J, Han J, Xie R, Wang C, Duan X, Rong Y, et al. MC-LSTM: Real-time 3D human action detection system for intelligent healthcare applications. IEEE Trans Biomed Circuits Syst [Internet]. 2021;15(2):259–69. Available from: http://dx.doi.org/10.1109/tbcas.2021.3064841
44. Kadri F, Baraoui M, Nouaouri I. LSTM-based deep learning approach with application to predicting hospital emergency department ad-missions. In: Proceedings of the 2019 International Conference on Industrial Engineering and Systems Management (IESM). Shanghai, China; 2019. p. 1–6.

45. Tsai FS, Weng YM, Ng CJ, Lee CC. Embedding stacked bottleneck vocal features in a LSTM architecture for automatic pain level classification during emergency triage. In: Proceedings of the 2017 Seventh International Conference on Affective Computing and Intelligent Interaction (ACII). San Antonio, TX, USA; 2017. p. 313–8.
46. Mantas J. Using long short-term memory (LSTM) neural networks to predict emergency department wait time. The Importance of Health Informatics in Public Health during a Pandemic. Stud Health Technol Inform. 2020.
47. Nwakanma CI, Islam FB, Maharani MP, Kim DS, Lee JM. Iot-based vibration sensor data collection and emergency detection classification using long short term memory (lstm). In: Proceedings of the 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Rome, Italy; 2021. p. 273–8.
48. Reddy BK, Delen D. Predicting hospital readmission for lupus patients: An RNN-LSTM-based deep-learning methodology. Comput Biol Med [Internet]. 2018;101:199–209. Available from: http://dx.doi.org/10.1016/j.compbiomed.2018.08.029
49. Guzman JC, Melin P, Prado-Arechiga G. Design of an optimized fuzzy classifier for the diagnosis of blood pressure with a new computational method for expert rule optimization. Algorithms. 2017;10(3):79.
50. De Oliveira MT, Reis LH, Verginadis Y, Mattos DM, Olabarriaga SD. SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts. IEEE Access. 2022 Oct 26;10:117836-54.

G. <u>References (Chapter 8)</u>

1. Ferrari, E. Access Control in Data Management Systems. Synth. Lect. Data Manag. 2010, 2, 1–117. https://doi.org/10.2200/s00281ed1v01y201005dtm004.
2. Hu, V.C.; Ferraiolo, D.; Kuhn, R.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. *NIST Spec. Publ.* **2013**, *800*, 162. https://doi.org/10.6028/nist.sp.800-162.
3. Dey, A.K. Understanding and Using Context. *Pers. Ubiquitous Comput.* **2001**, *5*, 4–7. https://doi.org/10.1007/s007790170019.

4. Ben-Assuli, O.; Ziv, A.; Sagi, D.; Ironi, A.; Leshno, M. Cost-effectiveness evaluation of EHR: Simulation of an abdominal aortic aneurysm in the emergency department. *J. Med. Syst.* **2016**, *40*, 1–13.
5. Povey, D. Optimistic security: A new access control paradigm. In Proceedings of the 1999 workshop on New security paradigms, Caledon Hills, ON, Canada, 22–25 September 1999; pp. 40–45.
6. Manasa, D.; Khanna, K.R. Sharing of PHR's in Cloud Computing. *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)* **2015**, *15*, 86.
7. Tsegaye, T.; Flowerday, S. A Clark-Wilson and ANSI role-based access control model. *Inf. Comput. Secur.* **2020**, *28*, 373–395. https://doi.org/10.1108/ics-08-2019-0100.
8. Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Washington, WA, USA, 21–23 October 2021; Springer: Berlin/Heidelberg, Germany, 2010; pp. 89–106. https://doi.org/10.1007/978-3-642-16161-2_6.
9. Jagdale, V.; Kekan, D.; Baride, I. Secure Sharing of Personal Health Records in Cloud using Attribute-based Encryption. *Int. J. Comput. Sci. Mob. Comput.* **2015**, *4*, 309–312.
10. Brucker, A.D.; Petritsch, H. Extending access control models with break-glass. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, Athens, Greece, 11–15 June 2014; pp. 197–206.
11. Georgakakis, E.; Nikolidakis, S.A.; Vergados, D.D.; Douligeris, C. Spatio temporal emergency role based access control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Washington, DC, USA, 28 June–1 July 2011; pp. 764–770. https://doi.org/10.1109/iscc.2011.5983932.
12. Kabbani, B.; Laborde, R.; Barrère, F.; Benzekri, A. Managing Break-The-Glass using Situation-oriented au-thorizations. In Proceedings of the 9ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information-SAR-SSI, Paris, France, 13–16 May 2014; p. 0.

13. Marinovic, S.; Craven, R.; Ma, J.; Dulay, N. Rumpole: A flexible break-glass access control model. In Proceedings of the 16th ACM Symposium on Access Control Models and Technologies, New York, NY, USA, 7–9 June 2011; pp. 73–82.
14. Maw, H.A.; Xiao, H.; Christianson, B.; Malcolm, J.A. An evaluation of break-the-glass access control model for medical data in wireless sensor networks. In Proceedings of the 2014 IEEE 16th International Conference on E-Health Networking, Applications and Services (Healthcom), Natal-RN, Brazil, 15–18 October 2014; pp. 130–135. https://doi.org/10.1109/healthcom.2014.7001829.
15. Guan, S.; Wang, Y.; Shen, J. Fingerprint-based access to personally controlled health records in emergency situations. *Sci. China Inf. Sci.* **2018**, *61*, 059103.
16. Covington, M.J.; Sastry, M.R. A contextual attribute-based access control model. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*; Springer :Berlin/Heidelberg, Germany, 2006; pp. 1996–2006.
17. Nomikos, G.D.; Dounias, G.; Tselentis, G.; Vemmos, K. Conventional vs. fuzzy modeling of diagnostic attributes for classifying acute stroke cases. In Proceedings of the ESIT-2000, European Symposium on Intelligent Techniques, Aachen, Germany, 9–13 September 2000; pp. 192–200.
18. Mahmood, U.; Al-Jumaily, A. Type-2 fuzzy classification of blood pressure parameters. In 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, Piscataway, NJ, USA, 3–6 December 2007; pp. 595–600.
19. Djam, X.Y.; Kimbi, Y.H. Fuzzy expert system for the management of hypertension. *Pac. J. Sci. Technol.* **2011**, *12*, 390–402.
20. Zerkouk, M.; Mhamed, A.; Messabih, B. A User Profile Based Access Control Model and Architecture. *Int. J. Comput. Networks Commun.* **2013**, *5*, 171–181. https://doi.org/10.5121/ijcnc.2013.5112.
21. Røstad, L.; Nytrø, Ø. Personalized access control for a personally controlled health record. In Proceedings of the 2nd ACM workshop on Computer security architectures—CSAW '08, Alexandria, VA, USA, 16 June 2008; pp. 9–16. https://doi.org/10.1145/1456508.1456511.

22. Petković, M.; Conrado, C.; Hammoutène, M. Cryptographically Enforced Personalized Role-Based Access Control. *Secur. Priv. Dyn. Environ.* **2006**, *8*, 364–376. https://doi.org/10.1007/0-387-33406-8_31.
23. Khatri, K. L., & Tamil, L. S. (2017). Early detection of peak demand days of chronic respiratory diseases emergency department visits using artificial neural networks. *IEEE journal of biomedical and health informatics*, *22*(1), 285-290.
24. An, Y., Huang, N., Chen, X., Wu, F., & Wang, J. (2019). High-risk prediction of cardiovascular diseases via attention-based deep neural networks. *IEEE/ACM transactions on computational biology and bioinformatics*, *18*(3), 1093-1105.
25. Singh, D., Kumar, V., Vaishali, & Kaur, M. (2020). Classification of COVID-19 patients from chest CT images using multi-objective differential evolution–based convolutional neural networks. *European Journal of Clinical Microbiology & Infectious Diseases*, *39*, 1379-1389.
26. Roquette, B. P., Nagano, H., Marujo, E. C., & Maiorano, A. C. (2020). Prediction of admission in pediatric emergency department with deep neural networks and triage textual data. *Neural Networks*, *126*, 170-177.
27. Irfan, M., Iftikhar, M. A., Yasin, S., Draz, U., Ali, T., Hussain, S., ... & Althobiani, F. (2021). Role of hybrid deep neural networks (HDNNs), computed tomography, and chest X-rays for the detection of COVID-19. *International Journal of Environmental Research and Public Health*, *18*(6), 3056.
28. Ganesan, N., Venkatesh, K., Rama, M. A., & Palani, A. M. (2010). Application of neural networks in diagnosing cancer disease using demographic data. *International Journal of Computer Applications*, *1*(26), 76-85.
29. Launay, C. P., Rivière, H., Kabeshova, A., & Beauchet, O. (2015). Predicting prolonged length of hospital stay in older emergency department users: use of a novel analysis method, the Artificial Neural Network. *European journal of internal medicine*, *26*(7), 478-482.
30. Kiliçarslan, S., Közkurt, C., Baş, S., & Elen, A. (2023). Detection and classification of pneumonia using novel Superior Exponential (SupEx) activation function in convolutional neural networks. *Expert Systems with Applications*, *217*, 119503.

31. Oasis-open.org. Available online: http://docs.oasis-open.org/xacml (accessed on 16 September 2021).
32. Quirolgico, S.; Hu, V.; Karygiannis, T. *Access Control for SAR Systems*; Department of Commerce US: Washington, DC, USA, 2011. https://doi.org/10.6028/nist.ir.7815.
33. Liang Y, Liu G, Chen Z, Elgendi M. PPG-BP Database [Internet]. figshare. 2021 [cited 26 May 2023]. Available from: https://figshare.com/articles/dataset/PPG-BP_Database_zip/5459299
34. Joshi, M.; Joshi, K.; Finin, T. Attribute Based Encryption for Secure Access to Cloud Based EHR Systems. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)), San Francisco, CA, USA, 2–7 July 2018.
35. Gutierrez, P.P. Cloud EHRServer by CaboLabs. Available online: https://cloudehrserver.com/ (accessed on 18 September 2021).
36. Sam Heard, T.B. OpenEhr Home. Available online: https://www.openehr.org/ (accessed on 18 September 2021).
37. Silva, I.; Moody, G.; Mark, R.; Celi, L.A. Predicting mortality of ICU patients: The PHYSIONET/computing in cardiology challenge 2012. Predicting Mortality of ICU Patients: The PhysioNet/Computing in Cardiology Challenge 2012 v1.0.0. Available online: https://physionet.org/content/challenge-2012/1.0.0/ (accessed on 26 May 2023).
38. Son HX, Le TH, Quynh NTT, Huy HND, Duong-Trung N, Luong HH. Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems. In: Mobile, Secure, and Programmable Networking. Cham: Springer International Publishing; 2021. p. 44–56.
39. Le HT, Thanh LNT, Vo HK, Luong HH, Tuan KNH, Anh TD, et al. Patient-Chain: Patient-centered Healthcare System a Blockchain-based Technology in Dealing with Emergencies. In: International Conference on Parallel and Distributed Computing: Applications and Technologies. Cham: Springer; 2022. p. 576–83.
40. Zhan W, Chen CL, Weng W, Tsaur WJ, Lim ZY, Deng YY. Incentive EMR Sharing System Based on Consortium Blockchain and IPFS. In Healthcare. Vol. 10. MDPI; 2022.

41. de Oliveira MT, Reis LH, Verginadis Y, Mattos DM, Olabarriaga SD. SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts. IEEE Access. 2022 Oct 26;10:117836-54.

H. References (Chapter 12)

1. Dey, Anind K.: Understanding and Using Context. Personal Ubiquitous Computing (2001) 4-7
2. Ferrari, E.: Access Control in Data Management Systems. Synthesis Lectures on Data Management, Vol. 2, No. 1. Morgan & Claypool Publishers (2010)
3. Khan, A., Access control in cloud computing environment.. ARPN Journal of Engineering and Applied Sciences (2012)
4. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller R., and Scarfone K.: Guide to Attribute Based Access Control (ABAC) definition and considerations. NIST special publication (2014)
5. Sahai A., and Waters, B.: Fuzzy identity-based encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg (2005) 457-473
6. Veloudis, S., Y. Verginadis, I. Patiniotakis, I. Paraskakis and G. Mentzas. Context-aware Security Models for PaaS-enabled Access Control. 6th International Conference on Cloud Computing and Services Science (CLOSER 2016), Rome, Italy, April 23-25, 2016
7. Veloudis, S., Paraskakis, I., Verginadis, Y., Patiniotakis, I., & Mentzas, G.: Ontological Templates for Regulating Access to Sensitive Medical Data in the Cloud. In 2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS) IEEE (2017, June) 805-810
8. ASCLEPIOS Security Context Element overview diagram. Available online at: https://www.asclepios-project.eu/wp-content/uploads/2019/11/ASCLEPIOS_Security_Context_Element_overview_diagram.png
9. ASCLEPIOS Security Context Element Object overview diagram. Available online at: https://www.asclepios-project.eu/wp-content/uploads/2019/11/ASCLEPIOS_Security_Context_Element_Object_overview_diagram.png

10. Weber, G. M., Mandl, K. D., & Kohane, I. S. (2014). Finding the missing link for big biomedical data. Jama, 311(24), 2479-2480.
11. Extension of Security Context Element Subject overview diagram. Available online at: https://www.asclepios-project.eu/wp-content/uploads/2019/11/ASCLEPIOS_Security_Context_Element_Subject_overview_diagram.png
12. Common Attack Pattern Enumeration and Classification (CAPEC), MITRE. Available online at: https://capec.mitre.org/
13. Security awareness component. Available online at: https://www.asclepios-project.eu/wpcontent/uploads/2019/11/CAPEC_ASCLEPIOS_Security_Awareness_Component.png
14. de Oliveira, M. T., Verginadis, Y., Reis, L. H. A., Evgenia Psarra, I. P., & Olabarriaga, S. D. (2021b). AC-ABAC templates. https://github.com/ AMCeScience/AC-ABAC-modelling-public/tree/main/templates. Accessed: 01/04/2021.
15. Django (2021). Django Framework. https://www.djangoproject.com/. Accessed: 11/03/2021.
16. de Oliveira, M. T., Verginadis, Y., Reis, L. H. A., Evgenia Psarra, I. P., & Olabarriaga, S. D. (2021a). AC-ABAC Github repository. https://github. com/AMCeScience/AC-ABAC-modelling-public. Accessed: 01/04/2021.
17. Turkmen, F., den Hartog, J., Ranise, S., & Zannone, N. (2015). Analysis of xacml policies with smt. In R. Focardi, & A. Myers (Eds.), Principles of Security and Trust (pp. 115–134). Berlin, Heidelberg: Springer Berlin Heidelberg.
18. DesLauriers, J., Kiss, T., Ariyattu, R. C., Dang, H.-V., Ullah, A., Bowden, J., Krefting, D., Pierantoni, G., & Terstyanszky, G. (2021). Cloud apps to-go: Cloud portability with tosca and micado. Concurrency and Computation: Practice and Experience, 33 , e6093.
19. Bakas, A., Dang, H.-V., Michalas, A., & Zalitko, A. (2020). The cloud we share: Access control on symmetrically encrypted data in untrusted clouds. IEEE 725 Access, 8 , 210462–210477.

20. Verginadis, Y., Patiniotakis, I., Gouvas, P., Mantzouratos, S., Veloudis, S., Schork, S. T., Seitz, L., Paraskakis, I., & Mentzas, G. (2019). Context-aware policy enforcement for paas-enabled access control. IEEE Transactions on Cloud Computing.
21. Brumley, B. B., & Tuveri, N. (2011). Remote timing attacks are still practical. In V. Atluri, & C. Diaz (Eds.), Computer Security – ESORICS 2011 (pp. 355–371). Berlin, Heidelberg: Springer Berlin Heidelberg.

Chapter 12

12. APPENDIX

A. EHRServer

1) EHRServer Definition

EHRServer is an open source, service-oriented, openEHR clinical data repository. It provides a secure REST API to store and query clinical data in many ways, supporting standard formats like JSON and XML, that are easy to integrate with any front-end application. Data queries can be created via the Administrative User Interface, with the powerful and easy to use EHRServer Query Builder. EHRServer complies with the openEHR specifications (http://openehr.org/releases/1.0.2/), leveraging the openEHR Information Model and the Dual Modeling methodology, using standard Archetypes and Templates (http://www.openehr.org/downloads/ADLworkbench/working_with_templates) And it is open source, so you can customize it to your needs or you can collaborate helping with the development. It's license is Apache 2. EHRServer was designed and developed after years of research and development of openEHR-based Clinical Information Systems, when we detected a niche for openEHR-compliant open source clinical data repositories. EHRServer was created by Pablo Pazos Gutiérrez at CaboLabs Healthcare Informatics (http://cabolabs.com/en).

2) Competitive Advantage of EHRServer

EHRServer has the following competitive advantages over other clinical decision support systems:

- **Unique**: Currently there is no other system for openEHR clinical data storage, that has a secure REST API and is open source.
- **Fast**: Data commit and queries are executed in a few milliseconds.
- **Secure**: The Administrative User Interface and the REST API can be easily secured by SSL Certificates, both requires authentication, and the REST API can only accept requests with self-signed tokens obtained after user authentication.

- **Generic**: The EHRServer doesn't contain specific knowledge about the clinical records that will be stored.
- **Knowledge-driven**: All the clinical records that will be stored in the EHRServer will be defined by standard openEHR Operational Templates, created from Archetypes.
- **Adaptable**: The EHRServer can be adapted to different clinical contexts by configuring different sets of clinical document definitions (openEHR Operational Templates), and queries can be created from the Administrative User Interface.
- **Flexible**: The EHRServer can be used on a wide range of contexts, from small clinics, to networks of hospitals, from hundreds of EHRs to tens of thousands.
- **Modifiable**: To support new clinical documents and queries, no source code needs to be changed, nor the database schema needs to be changed. The EHRServer can be adapted to very different contexts, without changing the software.
- **Based on Standards**: The main design concern of the EHRServer was to be compliant with the openEHR specifications, and use standard communication protocols and standard formats to move data in and out the EHRServer.
- **Interoperable**: The use of standards, and a very well documented REST API, allows to integrate any application or system with the EHRServer in hours instead of weeks. OpenEHR Archetypes and Operational Templates guarantee Semantic Interoperability between the EHRServer and any system that makes use of it's data.
- **Accessible**: Users and systems with permissions can access the clinical information contained in the EHRServer anytime, from anywhere. All the data that comes in can be queried, avoiding the "information silos", a very common problem in healthcare information systems. Also, if users don't have the information they need, how they need it, a specific query can be created and tested in seconds, using the EHRServer Query Builder, and new queries can be available in seconds for users.
- **Versionable**: Because clinical documentation is inalterable, a versioning mechanism is needed to provide corrections or amendments to clinical

documents. The EHRServer supports versioning of clinical documents and maintains all the versions of each document in a traceable structure.

- **Multitenancy**: EHRServer supports different organizations, each EHR will be associated with one organization. This allows to support EHRs from many hospitals and clinics, on the same instance of the EHRServer. This is secure and very well delimited: one organization can't access the EHRs owned by other organization.
- **Intuitive Administrative**: User Interface (AUI) The EHRServer AUI allows to manage, audit and track any aspect of the clinical records, EHRs, patients and queries. Allows to create patients and their EHRs and to create and test data queries. It also looks great on mobile devices.
- **Easy to setup and use**: The EHRServer can be installed, configured and be running by reading the EHRServer guide.
- **Made for the cloud**: EHRServer can be easily deployed on the cloud on any PaaS provider that supports Java Web Applications, like OpenShift or AWS.
- **Well documented**: The EHRServer Guide contains all the information you need to setup, run and use the AUI. It also contains the full REST API documentation.
- **Supported**: The EHRServer is supported by CaboLabs Healthcare Informatics (http://www.cabolabs.com/en), experts on Healthcare Informatics, Interoperability and Standards, with many years of experience in R+D, consultancy and training.

3) Main use cases of EHRServer

EHRServer is designed to simplify the implementation of the following use cases, but is not limited in any way by them.

a) Shared Healthcare Record

It is very common that in a healthcare environment, like a clinic or hospital, multiple systems for clinical information recording are in use. It is also very frequent to have systems that are not designed to share information with other systems or clinical users, generating information accessibility problems because of the lack of interoperability, and fragmenting EHRs. EHRServer can be used as an integration backend to share clinical information between those systems in a standard way, enabling data accessibility to clinical users and removing the EHR fragmentation

Typical scenario

A clinic or hospital has many systems to record clinical information in different ways, for different medical specialties or allied healthcare professionals, and different units or departments. Those systems can be based on different technologies, platforms and devices, for example:

- a Web-based EMR for general consultation,
- a desktop EMR for the emergency department, and,
- a mobile application for the nurses to monitor patients at the ICU.

Clinical users will record information on those systems, but later they want a complete view over their patients, including the information from the three systems mentioned above, and other systems that might also be in place. For sake of simplicity let's keep just those three systems.

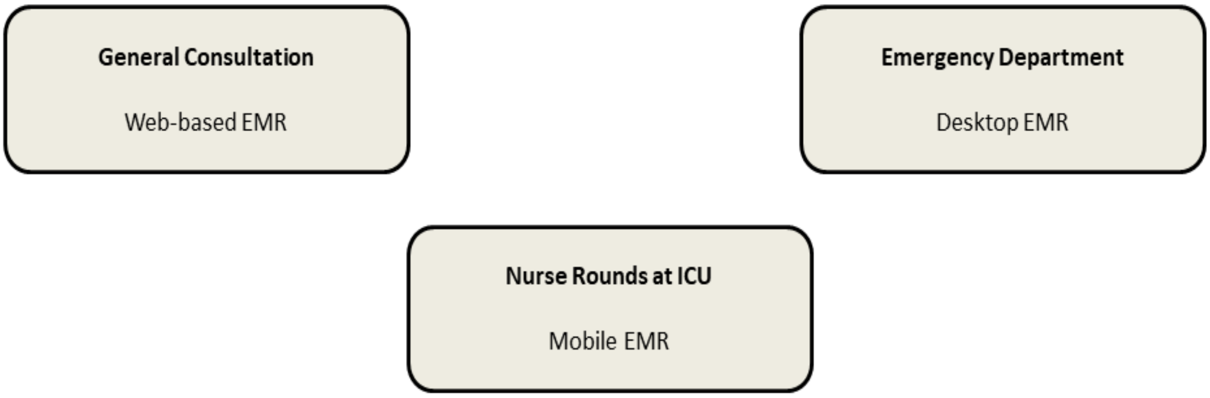


Figure 12. 1 Level1: No Information Sharing

First, let's share clinical information between those systems by integrating them with the EHRServer, using standard interfaces and data formats compliant with openEHR, instead of creating custom interfaces between each two of them (needs 2 interfaces to be implemented on each system).

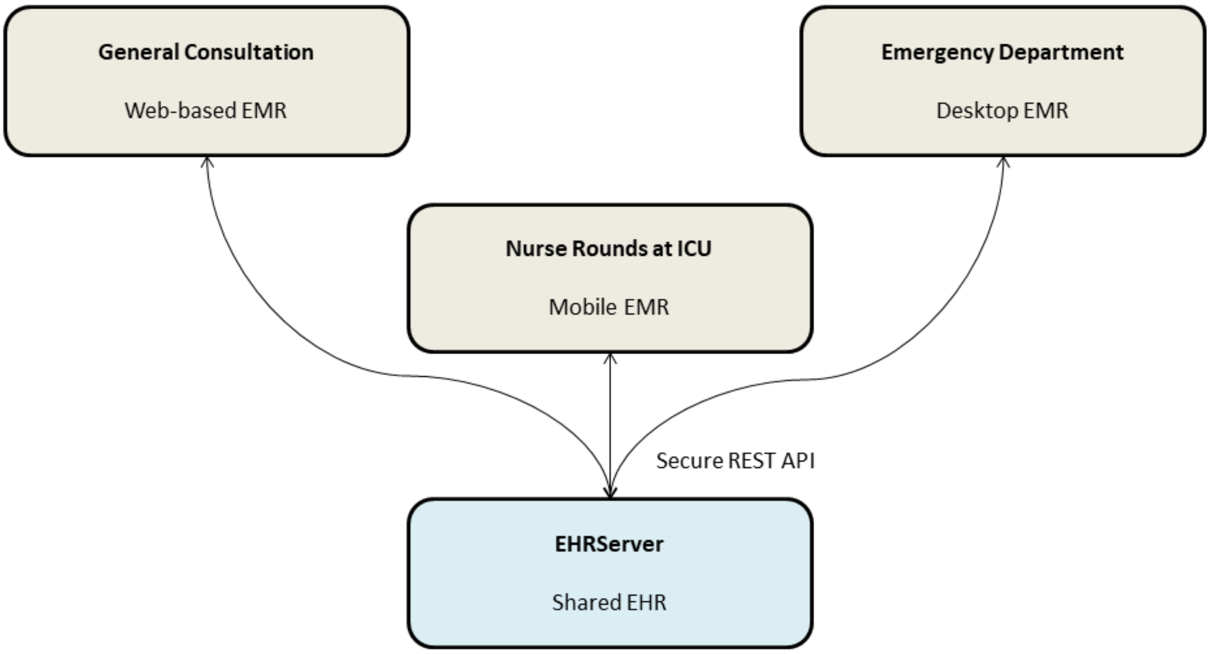


Figure 12. 2 Level 2: information sharing through EHRServer

Because there are no limits on what you can integrate, let's integrate more systems and apps that record clinical information, that display information, or for doing data analysis and research.

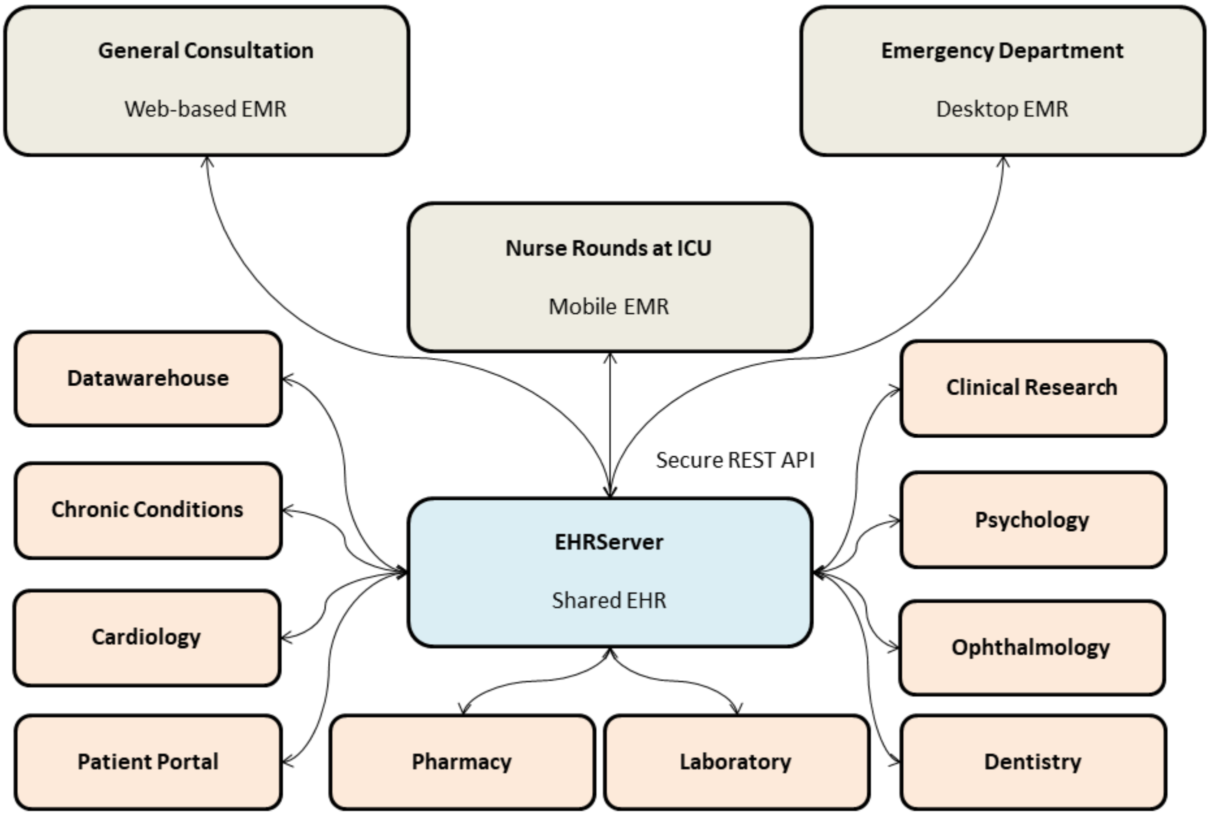


Figure 12. 3 Level 3: Sharing Information with more applications, EHRServer as a Platform

You will end up with an integrated and shared unique EHR per patient, accessible and interoperable.

b) Backend for Clinical Mobile Applications

Many software factories that develop mobile applications don't have specific health IT knowledge in-house, so implementing a standard like openEHR is very difficult. Also implementing flexible clinical data storage is a hard task for non-Health IT companies. EHRServer can alleviate the burden, all you need to know is how to use a REST API, XML and JSON, stuff that any software factory knows how to use. With EHRServer as the backend of your healthcare mobile apps, you can focus on features and have you app running in no time, EHRServer takes care of the clinical data storage and the queries to access that data.

Multiple mobile apps can use the same backend, even if those apps are used by different hospitals and clinics, because EHRServer supports multi-tenancy:

- all clinical data is associated with an organization (clinic, hospital, etc.)
- users under each organization can access only data under their organization

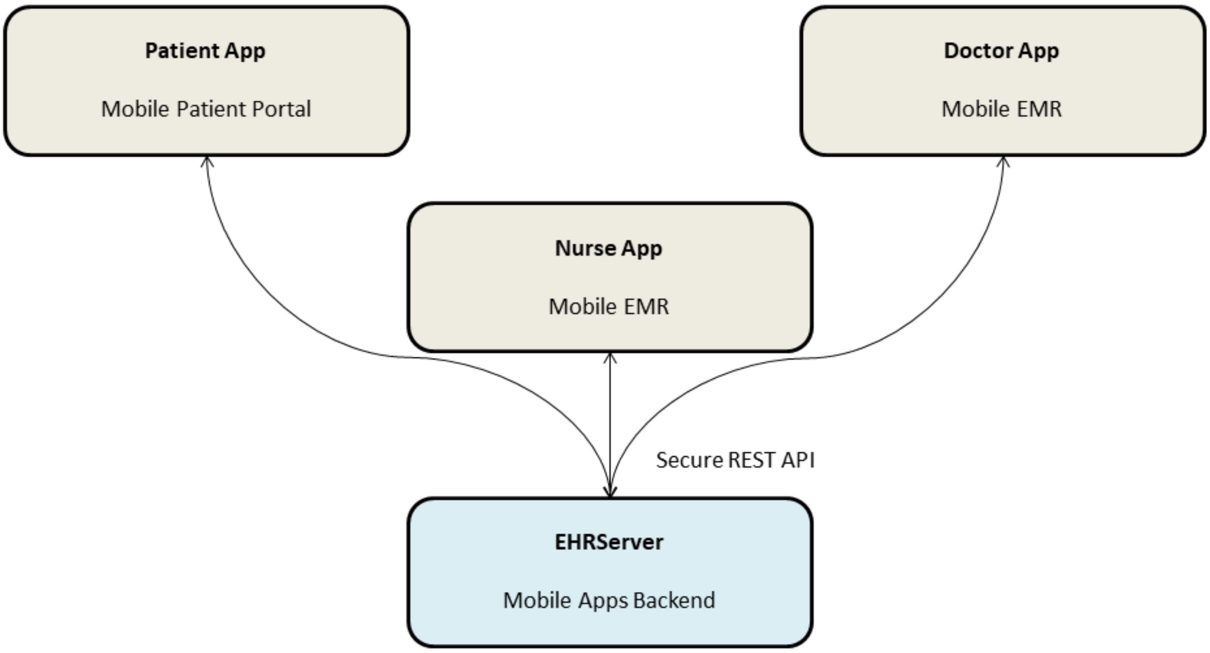


Figure 12. 4 EHRServer as backend of mobile apps

c) *Clinical Research Data source*

Researchers usually have big sets of heterogeneous data to analyze, compare, chart, evaluate, etc. But there is no easy way to query the data sets in the many forms needed by researchers, and researchers end up using productivity tools like Excel to store and analyse the data sets, and do manual queries. With EHRServer, the clinical data sets can be stored using a standard information model, that is easy to process and analyze, and the EHRServer Query Builder enable clinical researchers to create their own data queries to get the data they need, how they need it, allowing to finish the analysis in tools like Excel, where statistical analysis can be performed, but over a more specific data set. Also, as shown on the previous use cases, EHRServer can be used to integrate many data sources to obtain more abundant data sets, without the burden of doing the data source integration manually (a complex process that requires a lot of time to get the desired results).

d) *Distributed Clinical Data Store*

In the near future, many instances of EHRServer will be able to be deployed forming a cluster. An EHRServer cluster will work as one logical EHRServer, composed by many physical EHRServers. This solution will enable these features:

- **High Availability**: 100% uptime of the EHRServer services, even if a server goes down.
- **Backup**: clinical data will be duplicated or triplicated between different servers, one can go down without any loss of data.
- **Disaster Recovery**: A current outage, fire, tornado, tsunami, etc. can affect the physical servers, but because of the redundancy of the cluster, no data is lost and the service is not interrupted. Later, new EHRServers can be added to the cluster and data loaded again to reach the same service level to users.
- **Scaling**: If more apps are added as clients of the EHRServer cluster, if those apps have more and more users every day, new EHRServer instances can be added to a cluster with ease to support scaling.

Main scenario for an EHRServer cluster

Two or more EHRServer instances can be added to a cluster. Each instance can receive data commits from client applications, and that data will be replicated to the whole cluster, so all the EHRServer instances will have the same data. That data will be available through queries over each EHRServer. So any client app can send and query information to / from each EHRServer in the cluster.

Also, other information like queries, users, organizations, ehrs, etc. will be synchronized inside each cluster.

4) Exploiting OpenEHR capabilities in EHRServer

EHRServer is an open source, openEHR based, clinical data repository. EHRServer provides a secure REST API to store and query clinical data, supporting standard formats like JSON and XML, that could be implemented in front end applications. Data queries can be created via the Administrative User Interface, with the EHRServer Query Builder. Complies with the openEHR specifications, using standard Archetypes and Templates. Supports to have different organizations, each EHR will be associated with one organization. This allows to support EHRs from many hospitals and clinics, on the same instance of the EHRServer.

a) Administrative User Interface (AUI)

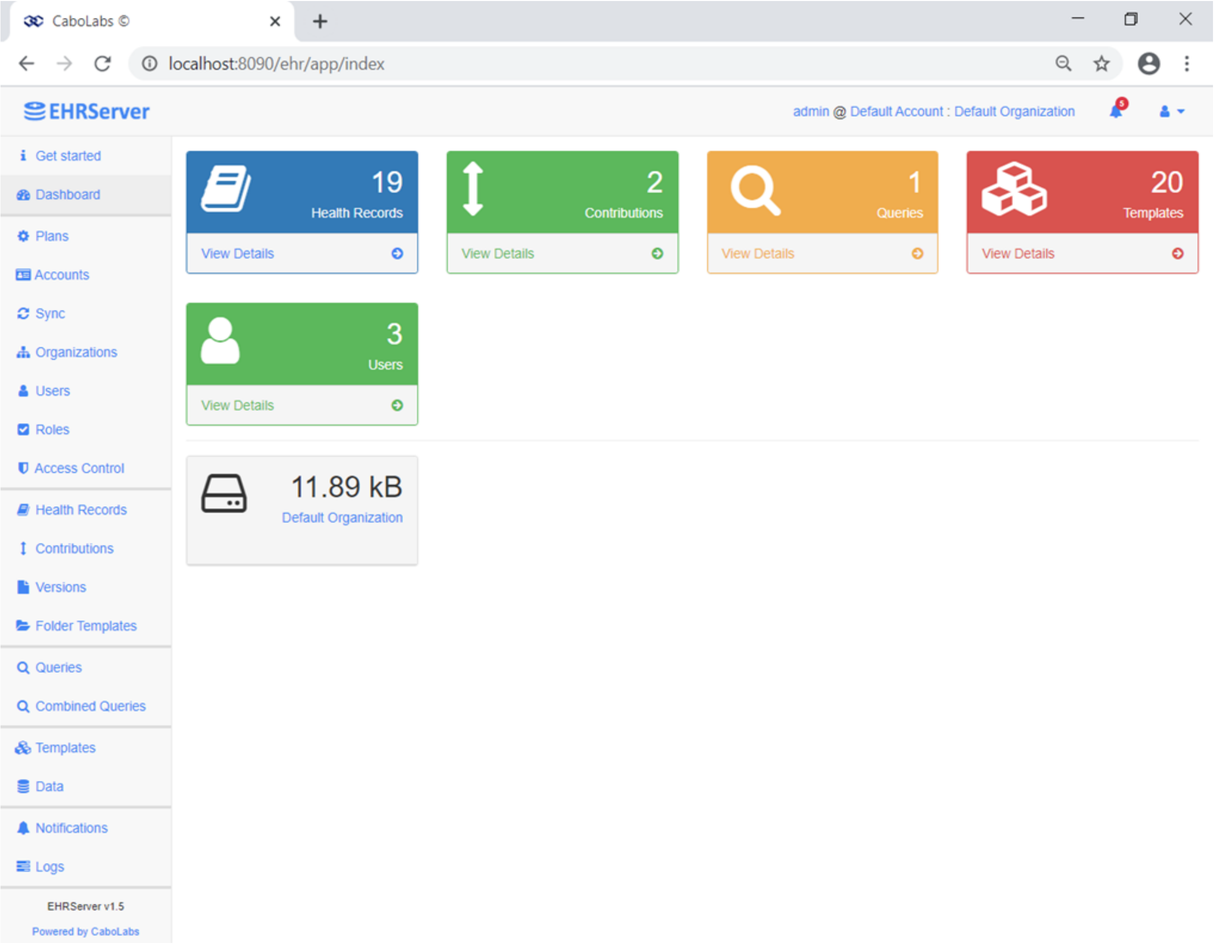
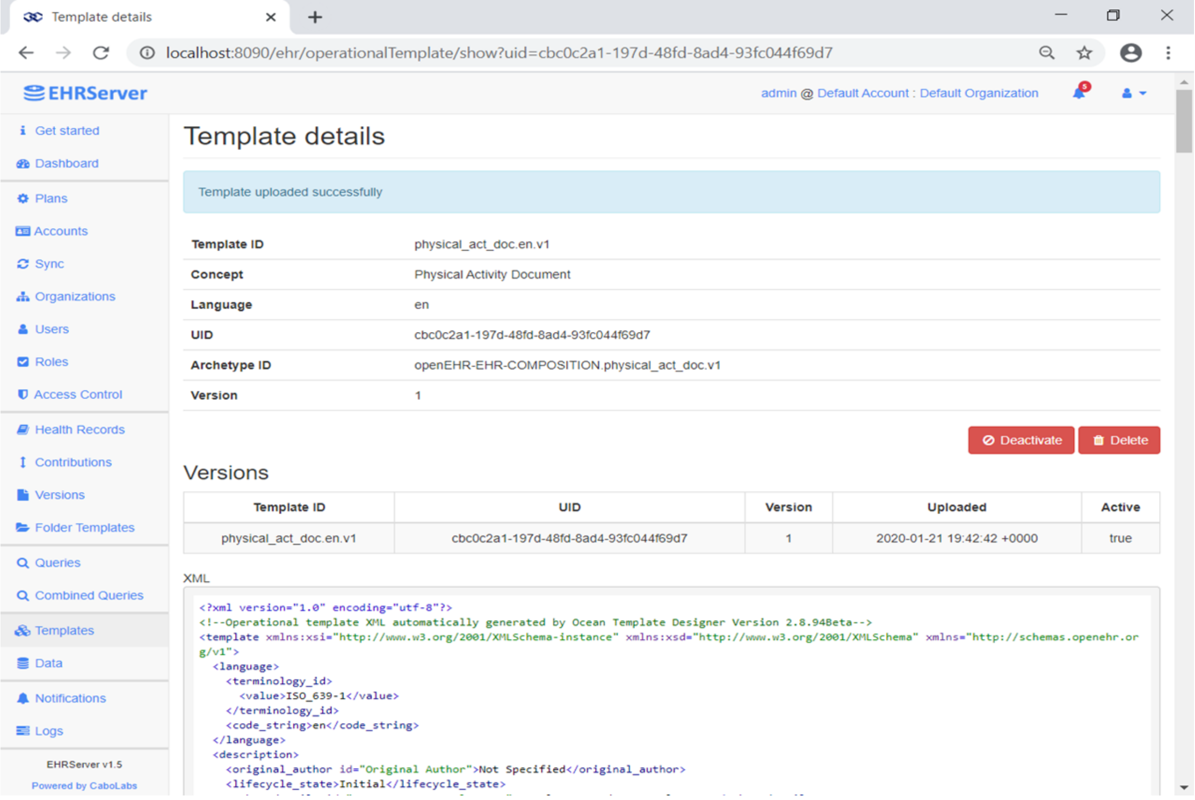


Figure 12. 5 EHRServer - Administrative User Interface

b) Upload an opt file to EHRServer



Template details

Template uploaded successfully

Template ID	physical_act_doc.en.v1
Concept	Physical Activity Document
Language	en
UID	cbc0c2a1-197d-48fd-8ad4-93fc044f69d7
Archetype ID	openEHR-EHR-COMPOSITION.physical_act_doc.v1
Version	1

Versions

Template ID	UID	Version	Uploaded	Active
physical_act_doc.en.v1	cbc0c2a1-197d-48fd-8ad4-93fc044f69d7	1	2020-01-21 19:42:42 +0000	true

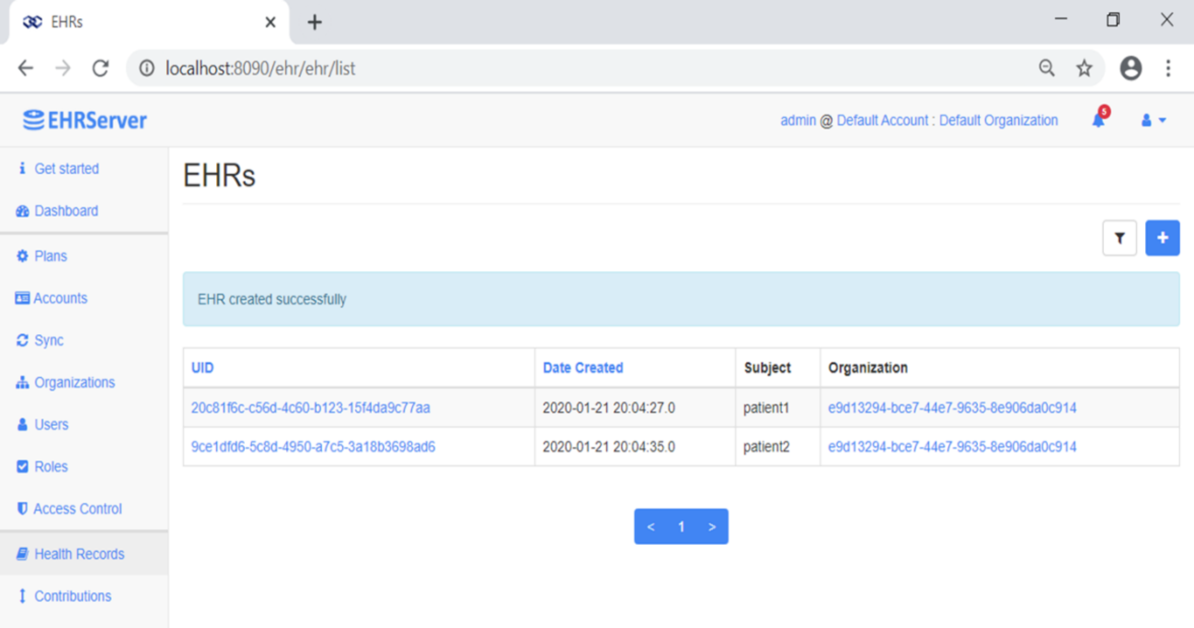
XML

```
<?xml version="1.0" encoding="utf-8"?>
<!--Operational template XML automatically generated by Ocean Template Designer Version 2.8.94Beta-->
<template xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.openehr.or
g/v1">
  <language>
    <terminology_id>
      <value>ISO_639-1</value>
    </terminology_id>
    <code_string>en</code_string>
  </language>
  <description>
    <original_author id="Original Author">Not Specified</original_author>
    <lifecycle_state>Initial</lifecycle_state>
```

Figure 12. 6 Upload an opt file to EHRServer

c) Creation of EHRs

We create two EHRs (patient1, patient2)



EHRs

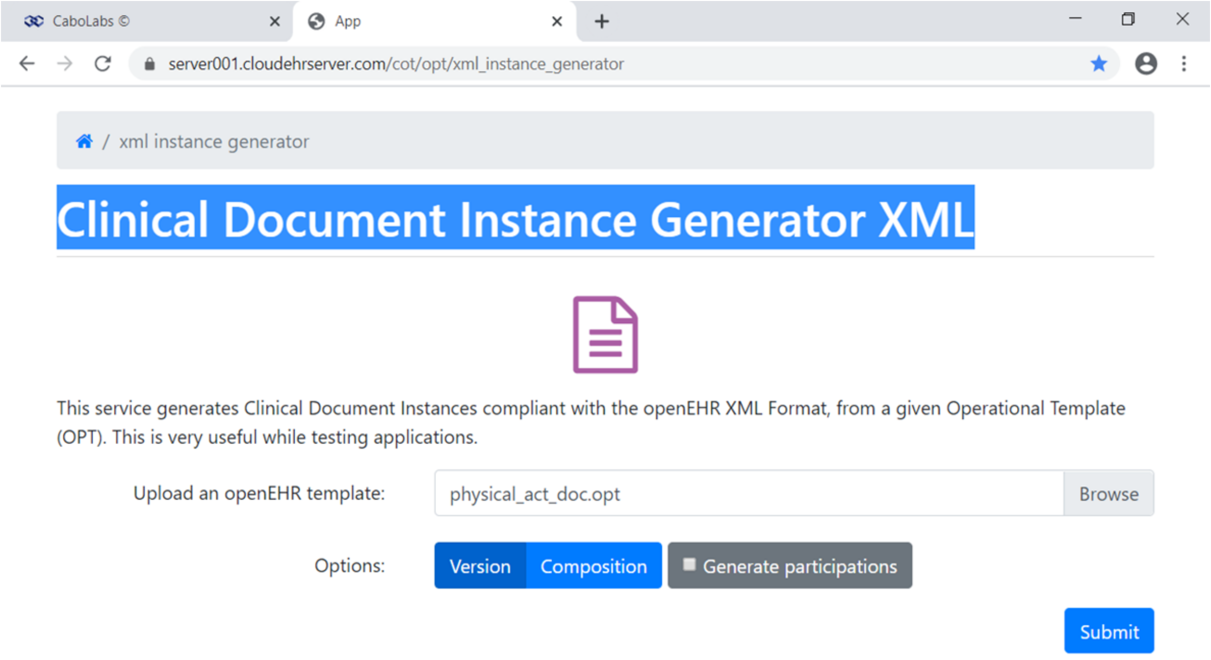
EHR created successfully

UID	Date Created	Subject	Organization
20c81f6c-c56d-4c60-b123-15f4da9c77aa	2020-01-21 20:04:27.0	patient1	e9d13294-bce7-44e7-9635-8e906da0c914
9ce1dfd6-5c8d-4950-a7c5-3a18b3698ad6	2020-01-21 20:04:35.0	patient2	e9d13294-bce7-44e7-9635-8e906da0c914

Figure 12. 7 Creation of EHRs

d) Clinical Document Instance Generator XML

It takes an operational template (*.opt) and generates a valid OpenEHR clinical document that complies with that opt.



Clinical Document Instance Generator XML

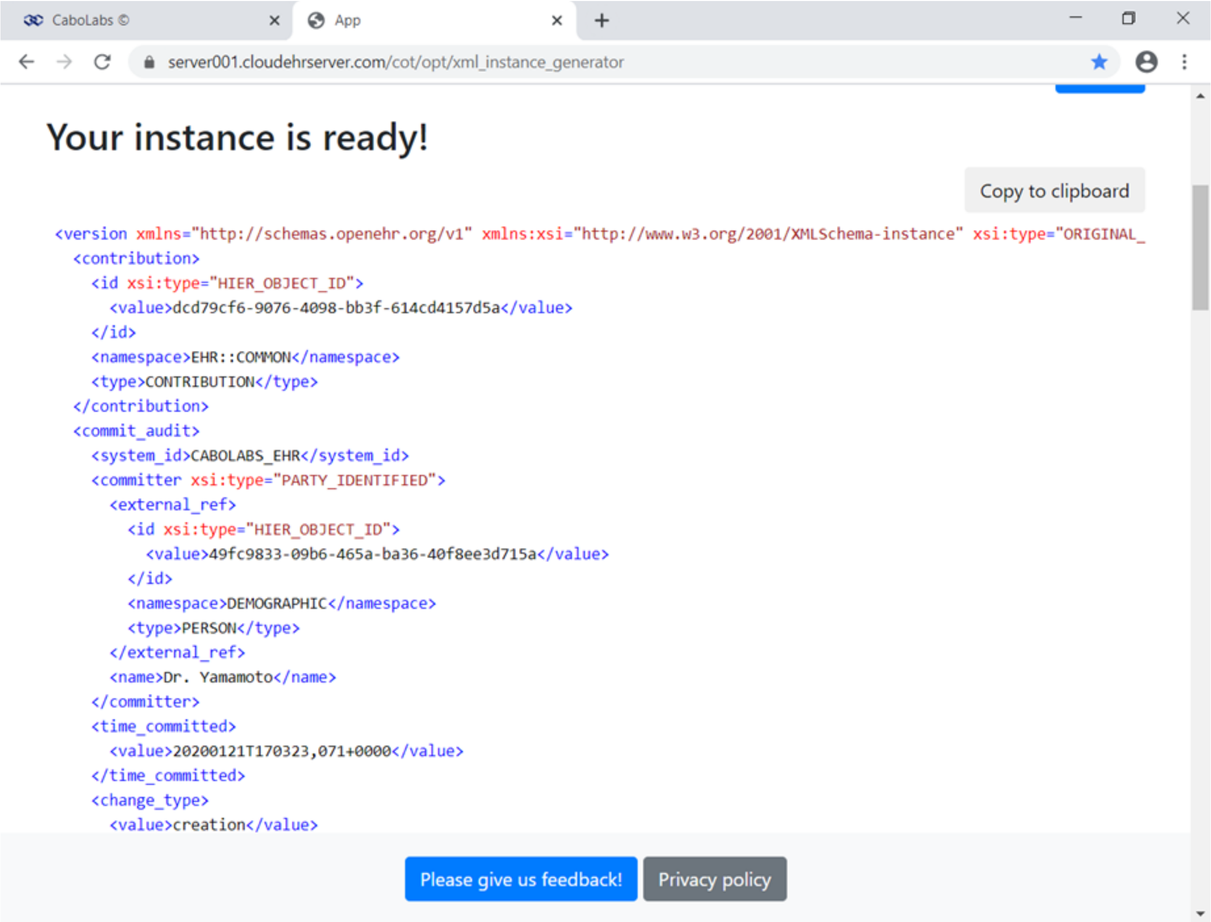
This service generates Clinical Document Instances compliant with the openEHR XML Format, from a given Operational Template (OPT). This is very useful while testing applications.

Upload an openEHR template: physical_act_doc.opt

Options: Version Composition ■ Generate participations

Figure 12. 8 Clinical Document Instance Generator XML

We get a full clinical document that complies with OpenEHR and complies with the operational template (opt file).



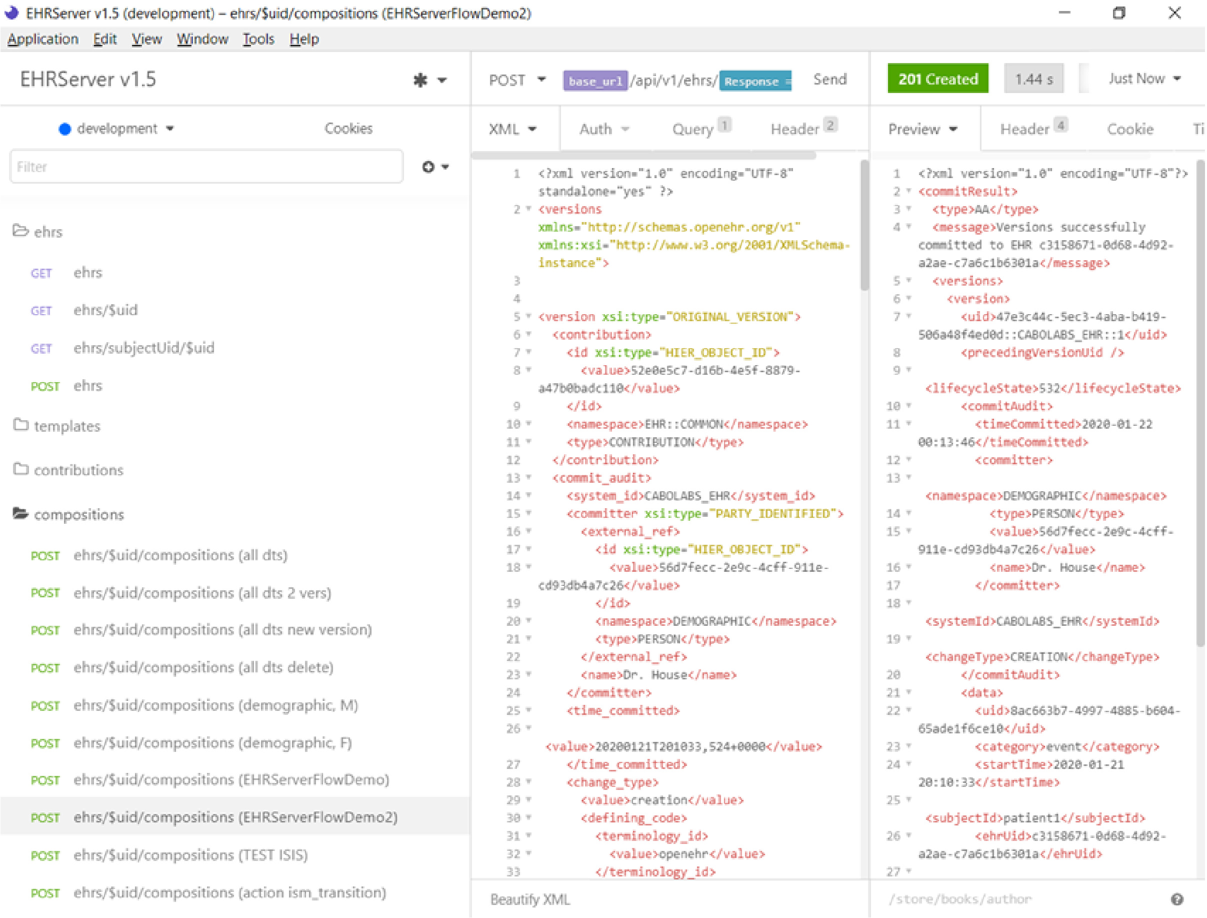
Your instance is ready!

```
<version xmlns="http://schemas.openehr.org/v1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ORIGINAL_
  <contribution>
    <id xsi:type="HIER_OBJECT_ID">
      <value>dcd79cf6-9076-4098-bb3f-614cd4157d5a</value>
    </id>
    <namespace>EHR::COMMON</namespace>
    <type>CONTRIBUTION</type>
  </contribution>
  <commit_audit>
    <system_id>CABOLABS_EHR</system_id>
    <committer xsi:type="PARTY_IDENTIFIED">
      <external_ref>
        <id xsi:type="HIER_OBJECT_ID">
          <value>49fc9833-09b6-465a-ba36-40f8ee3d715a</value>
        </id>
        <namespace>DEMOGRAPHIC</namespace>
        <type>PERSON</type>
      </external_ref>
      <name>Dr. Yamamoto</name>
    </committer>
    <time_committed>
      <value>20200121T170323,071+0000</value>
    </time_committed>
    <change_type>
      <value>creation</value>
```

Figure 12. 9 XML Instance of Clinical Instance Generator

e) XML Clinical Document Instance uploading to EHRServer via insomnia

We upload the XML Clinical Document Instance to EHRServer after updating the values of our fields.


EHRServer v1.5 (development) – ehrs/$uid/compositions (EHRServerFlowDemo2)
Application Edit View Window Tools Help
EHRServer v1.5
development
Cookies
Filter
ehrs
GET ehrs
GET ehrs/$uid
GET ehrs/subjectUid/$uid
POST ehrs
templates
contributions
compositions
POST ehrs/$uid/compositions (all dts)
POST ehrs/$uid/compositions (all dts 2 vers)
POST ehrs/$uid/compositions (all dts new version)
POST ehrs/$uid/compositions (all dts delete)
POST ehrs/$uid/compositions (demographic, M)
POST ehrs/$uid/compositions (demographic, F)
POST ehrs/$uid/compositions (EHRServerFlowDemo)
POST ehrs/$uid/compositions (EHRServerFlowDemo2)
POST ehrs/$uid/compositions (TEST ISIS)
POST ehrs/$uid/compositions (action ism_transition)
POST
base_url /api/v1/ehrs/ Response
Send
XML
Auth
Query 1
Header 2
201 Created
1.44 s
Just Now
Preview
Header 4
Cookie
Ti
Beautify XML
/store/books/author

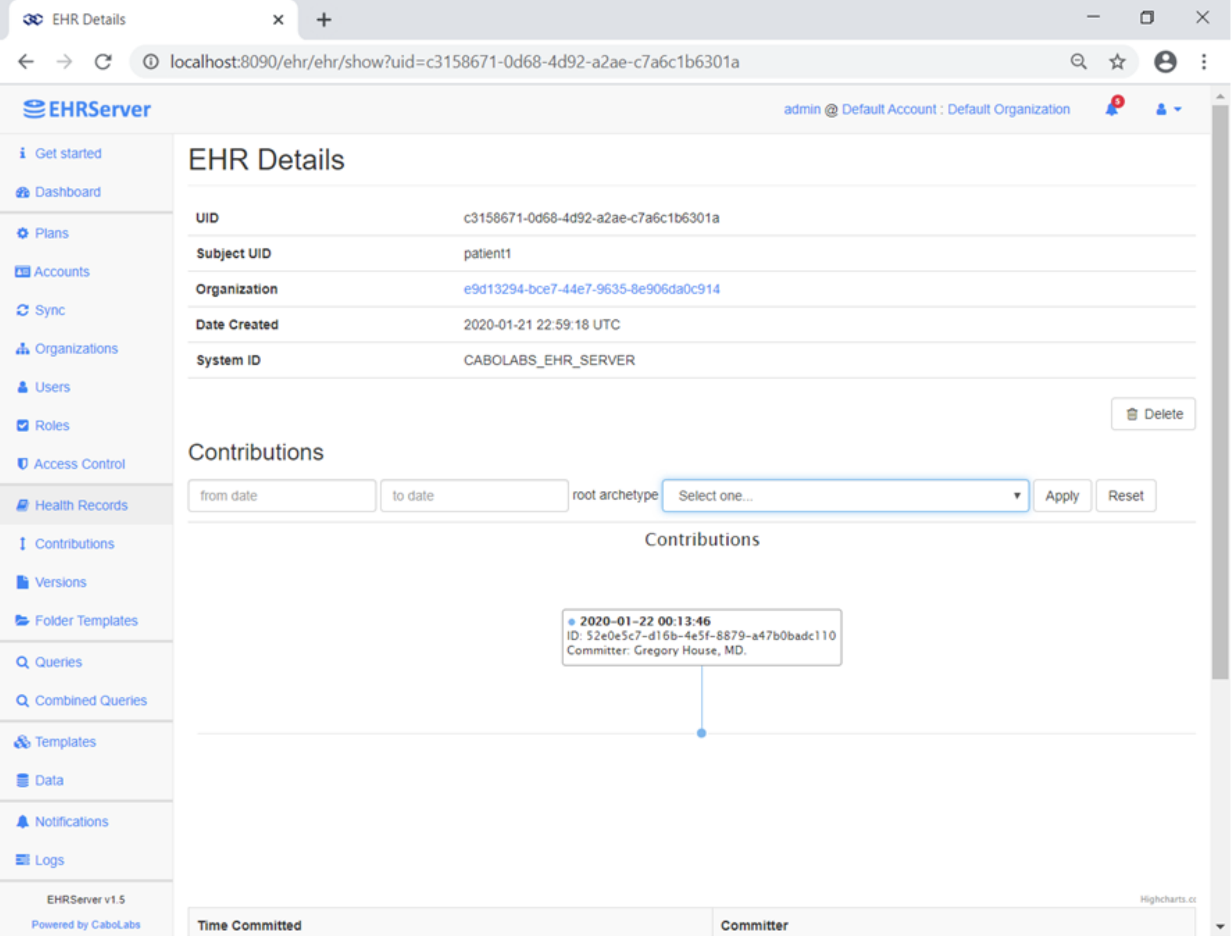
```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<versions xmlns="http://schemas.openehr.org/v1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">


<version xsi:type="ORIGINAL_VERSION">
  <contribution>
    <id xsi:type="HIER_OBJECT_ID">
      <value>52e0e5c7-d16b-4e5f-8879-a47b0badc110</value>
    </id>
    <namespace>EHR::COMMON</namespace>
    <type>CONTRIBUTION</type>
  </contribution>
  <commit_audit>
    <system_id>CABOLABS_EHR</system_id>
    <committer xsi:type="PARTY_IDENTIFIED">
      <external_ref>
        <id xsi:type="HIER_OBJECT_ID">
          <value>56d7fecc-2e9c-4cff-911e-cd93db4a7c26</value>
        </id>
        <namespace>DEMOGRAPHIC</namespace>
        <type>PERSON</type>
      </external_ref>
      <name>Dr. House</name>
    </committer>
    <time_committed>
      <value>20200121T201033,524+0000</value>
    </time_committed>
    <change_type>
      <value>creation</value>
      <defining_code>
        <terminology_id>
          <value>openehr</value>
        </terminology_id>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<commitResult>
  <type>AA</type>
  <message>Versions successfully committed to EHR c3158671-0d68-4d92-a2ae-c7a6c1b6301a</message>
  <versions>
    <version>
      <uid>47e3c44c-5ec3-4aba-b419-506a48f4ed0d::CABOLABS_EHR::1</uid>
      <precedingVersionUid />
      <lifecycleState>532</lifecycleState>
      <commitAudit>
        <timeCommitted>2020-01-22 00:13:46</timeCommitted>
        <committer>
          <namespace>DEMOGRAPHIC</namespace>
          <type>PERSON</type>
          <value>56d7fecc-2e9c-4cff-911e-cd93db4a7c26</value>
          <name>Dr. House</name>
        </committer>
        <systemId>CABOLABS_EHR</systemId>
        <changeType>CREATION</changeType>
      </commitAudit>
      <data>
        <uid>8ac663b7-4997-4885-b604-65ade1f6ce10</uid>
        <category>event</category>
        <startTime>2020-01-21 20:10:33</startTime>
        <subjectId>patient1</subjectId>
        <ehrUid>c3158671-0d68-4d92-a2ae-c7a6c1b6301a</ehrUid>
```

Figure 12. 10 XML Clinical Document Instance uploading to EHRServer via insomnia

f) ***XML Clinical Document Instance in the EHRServer (contribution)***

The previous XML Clinical Document Instance in EHRServer (contribution).



EHR Details

UID	c3158671-0d68-4d92-a2ae-c7a6c1b6301a
Subject UID	patient1
Organization	e9d13294-bce7-44e7-9635-8e906da0c914
Date Created	2020-01-21 22:59:18 UTC
System ID	CABOLABS_EHR_SERVER

Contributions

Contributions

2020-01-22 00:13:46
ID: 52e0e5c7-d16b-4e5f-8879-a47b0badc110
Committer: Gregory House, MD.

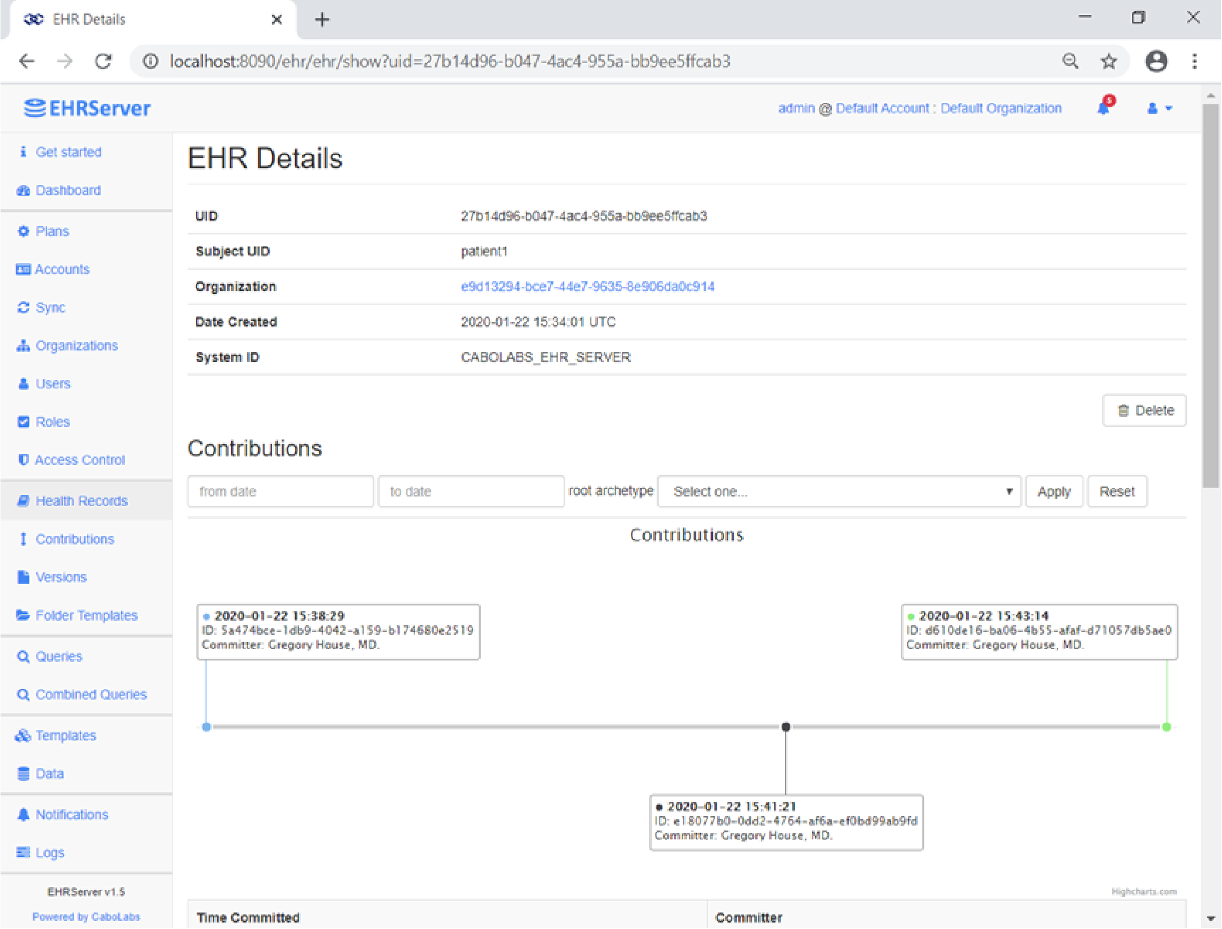
Time Committed	Committer

Figure 12. 11 XML Clinical Document Instance in the EHRServer (contribution)

g) ***Creation of three contributions***

Likewise, we create three contributions:

- Calories: 200, 260, 350
- Duration: 34, 46, 57



EHR Details

UID	27b14d96-b047-4ac4-955a-bb9ee5ffcab3
Subject UID	patient1
Organization	e9d13294-bce7-44e7-9635-8e906da0c914
Date Created	2020-01-22 15:34:01 UTC
System ID	CABOLABS_EHR_SERVER

Contributions

Contributions

2020-01-22 15:38:29
ID: 5a474bce-1db9-4042-a159-b174680e2519
Committer: Gregory House, MD.

2020-01-22 15:43:14
ID: d610de16-ba06-4b55-afaf-d71057db5ae0
Committer: Gregory House, MD.

2020-01-22 15:41:21
ID: e18077b0-0dd2-4764-af6a-ef0bd99ab9fd
Committer: Gregory House, MD.

Time Committed	Committer

Figure 12. 12 Creation of three contributions

h) <u>Queries</u>

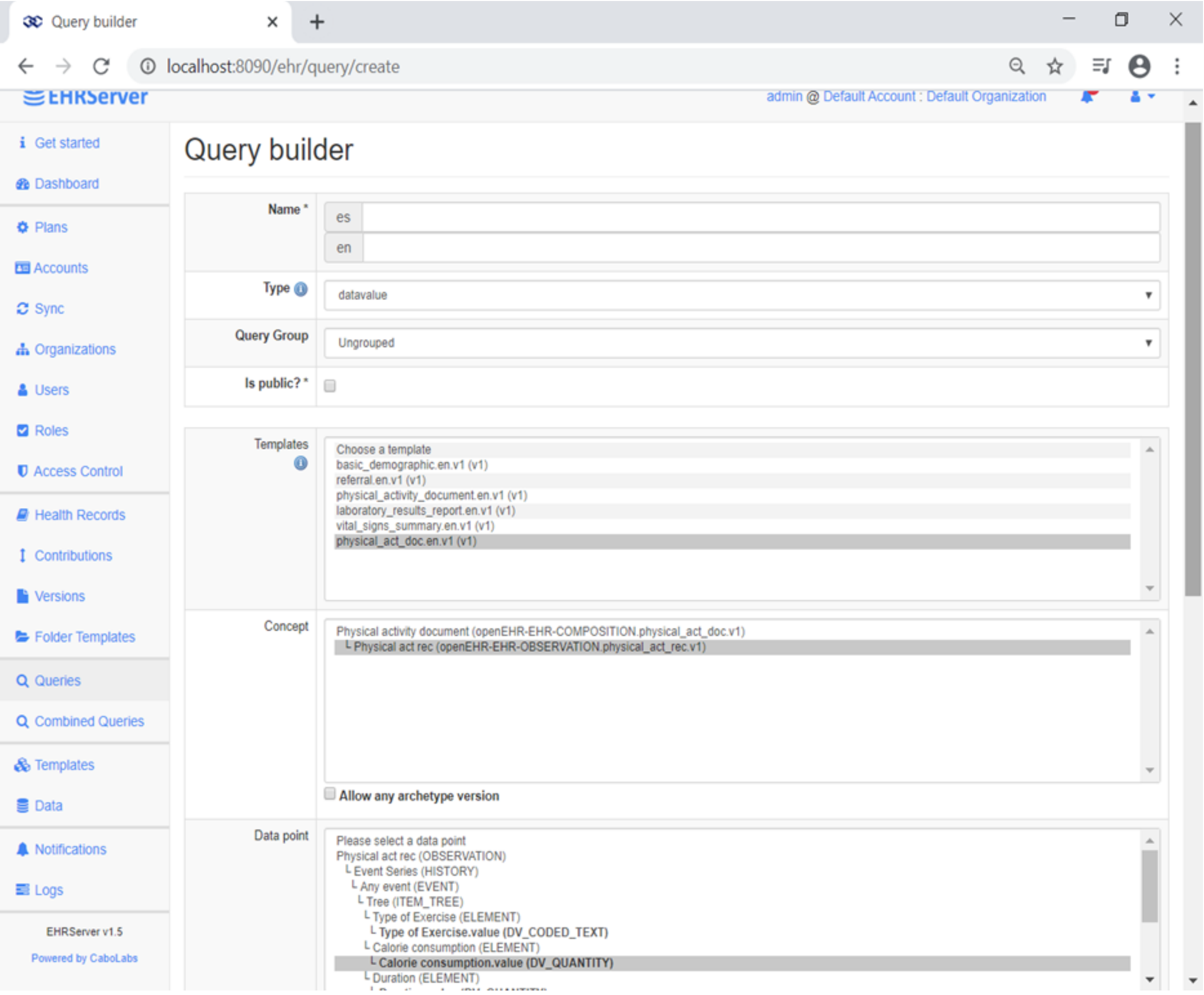
We have two options:

1) get data from database

2) get full documents

Queries 1st option – Get data

- In Templates: We choose our template.
- In Concept: We choose the observation file.



Query builder

Name * es
en

Type datavalue

Query Group Ungrouped

Is public? * □

Templates
Choose a template
basic_demographic.en.v1 (v1)
referral.en.v1 (v1)
physical_activity_document.en.v1 (v1)
laboratory_results_report.en.v1 (v1)
vital_signs_summary.en.v1 (v1)
physical_act_doc.en.v1 (v1)

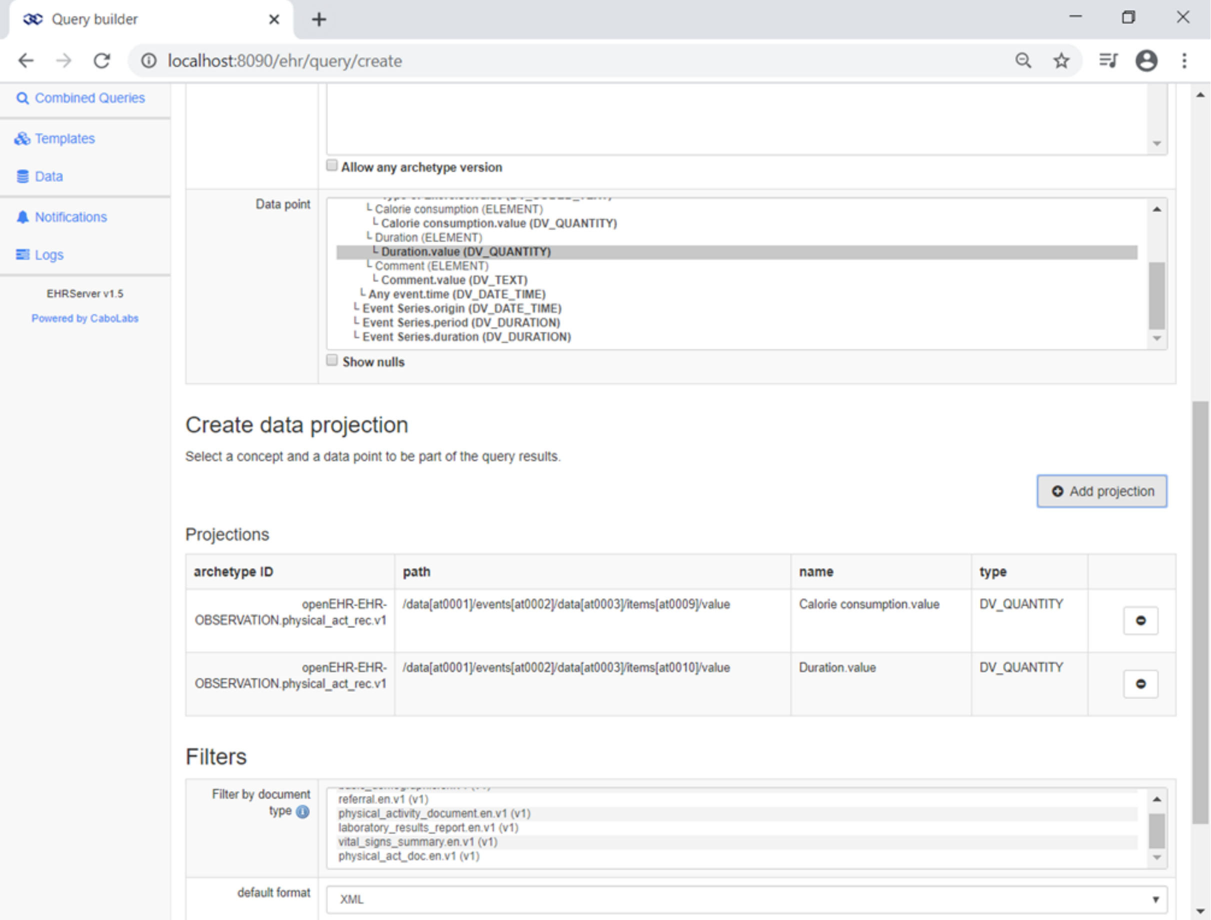
Concept
Physical activity document (openEHR-EHR-COMPOSITION.physical_act_doc.v1)
└ Physical act rec (openEHR-EHR-OBSERVATION.physical_act_rec.v1)

□ Allow any archetype version

Data point
Please select a data point
Physical act rec (OBSERVATION)
└ Event Series (HISTORY)
└ Any event (EVENT)
└ Tree (ITEM_TREE)
└ Type of Exercise (ELEMENT)
└ **Type of Exercise.value (DV_CODED_TEXT)**
└ Calorie consumption (ELEMENT)
└ **Calorie consumption.value (DV_QUANTITY)**
└ Duration (ELEMENT)

Figure 12. 13 Queries 1st option – Get data

- In Data point: We choose data point of our choice (e.g. calorie, duration) in order to create data projection.



☐ Allow any archetype version

Data point

```
    └ Calorie consumption (ELEMENT)
      └ Calorie consumption.value (DV_QUANTITY)
    └ Duration (ELEMENT)
      └ Duration.value (DV_QUANTITY)
    └ Comment (ELEMENT)
      └ Comment.value (DV_TEXT)
  └ Any event.time (DV_DATE_TIME)
 └ Event Series.origin (DV_DATE_TIME)
 └ Event Series.period (DV_DURATION)
 └ Event Series.duration (DV_DURATION)
```

☐ Show nulls

Create data projection

Select a concept and a data point to be part of the query results.

Projections

archetype ID	path	name	type	
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0009]/value	Calorie consumption.value	DV_QUANTITY	⊖
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0010]/value	Duration.value	DV_QUANTITY	⊖

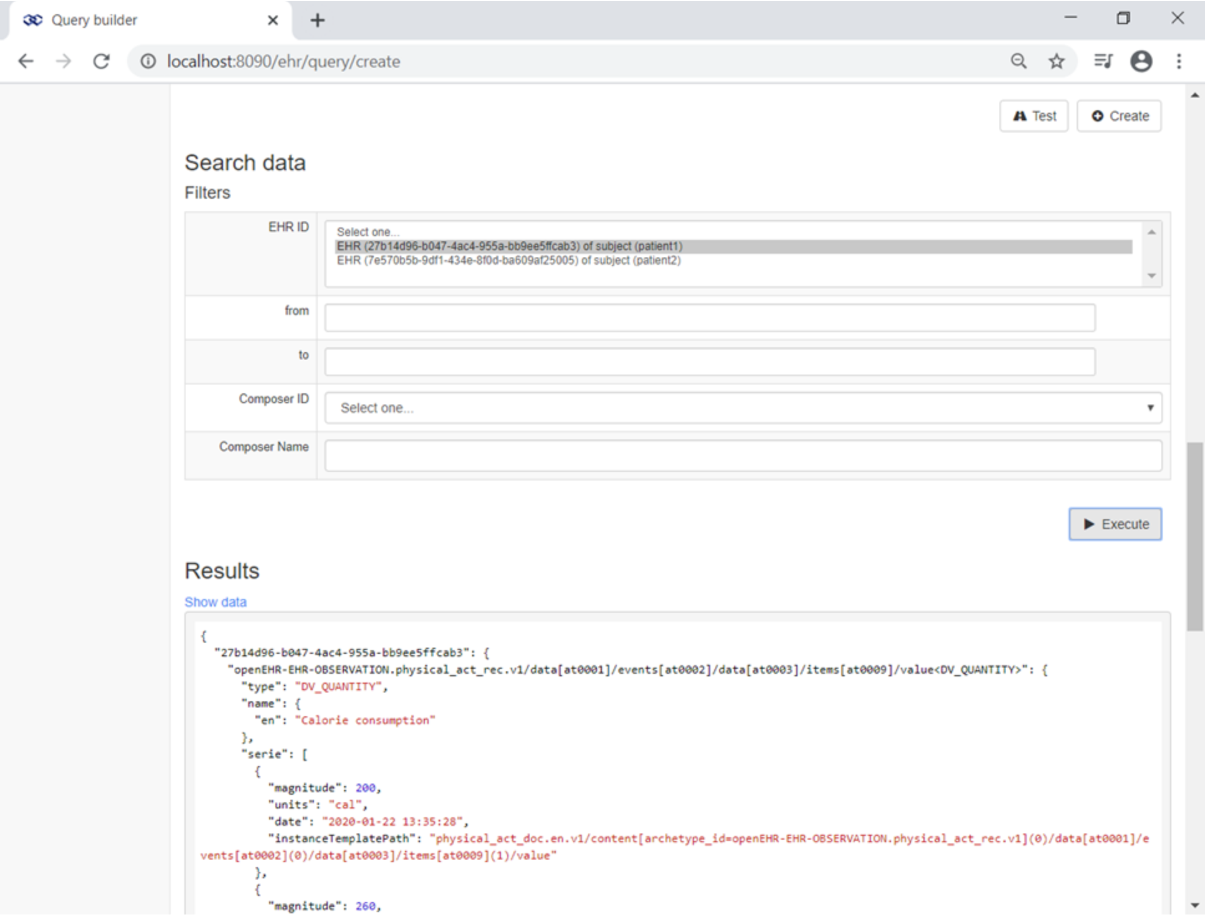
Filters

Filter by document type:
referral.en.v1 (v1)
physical_activity_document.en.v1 (v1)
laboratory_results_report.en.v1 (v1)
vital_signs_summary.en.v1 (v1)
physical_act_doc.en.v1 (v1)

default format: XML

Figure 12. 14 Queries 1st option – Get data – In Data point

- In EHRs: We choose the first patient



Search data

Filters

EHR ID
Select one...
EHR (27b14d96-b047-4ac4-955a-bb9ee5ffcab3) of subject (patient1)
EHR (7e570b5b-9df1-434e-8f0d-ba609af25005) of subject (patient2)

from

to

Composer ID: Select one...

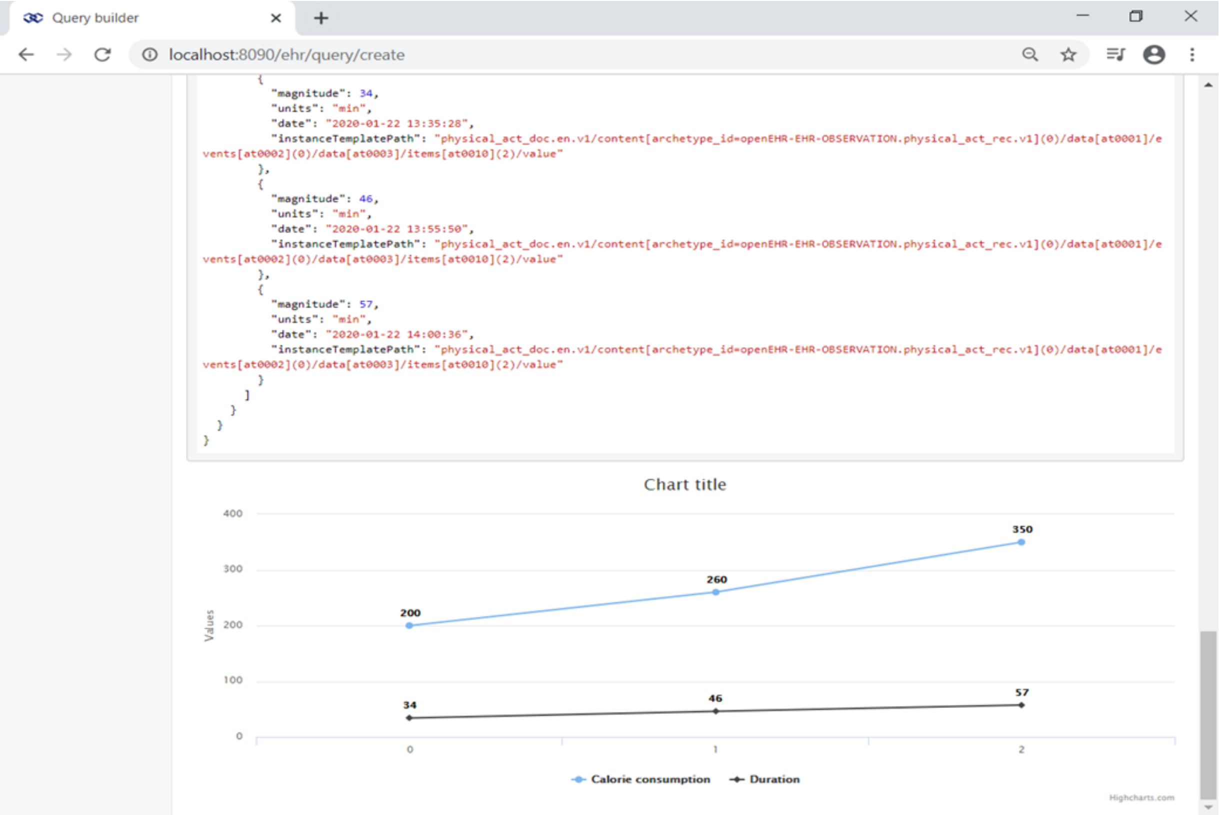
Composer Name

Results

```
{
  "27b14d96-b047-4ac4-955a-bb9ee5ffcab3": {
    "openEHR-EHR-OBSERVATION.physical_act_rec.v1/data[at0001]/events[at0002]/data[at0003]/items[at0009]/value<DV_QUANTITY>": {
      "type": "DV_QUANTITY",
      "name": {
        "en": "Calorie consumption"
      },
      "serie": [
        {
          "magnitude": 200,
          "units": "cal",
          "date": "2020-01-22 13:35:28",
          "instanceTemplatePath": "physical_act_doc.en.v1/content[archetype_id=openEHR-EHR-OBSERVATION.physical_act_rec.v1](0)/data[at0001]/e
vents[at0002](0)/data[at0003]/items[at0009](1)/value"
        },
        {
          "magnitude": 260,
```

Figure 12. 15 Queries 1st option – Get data – In EHRs

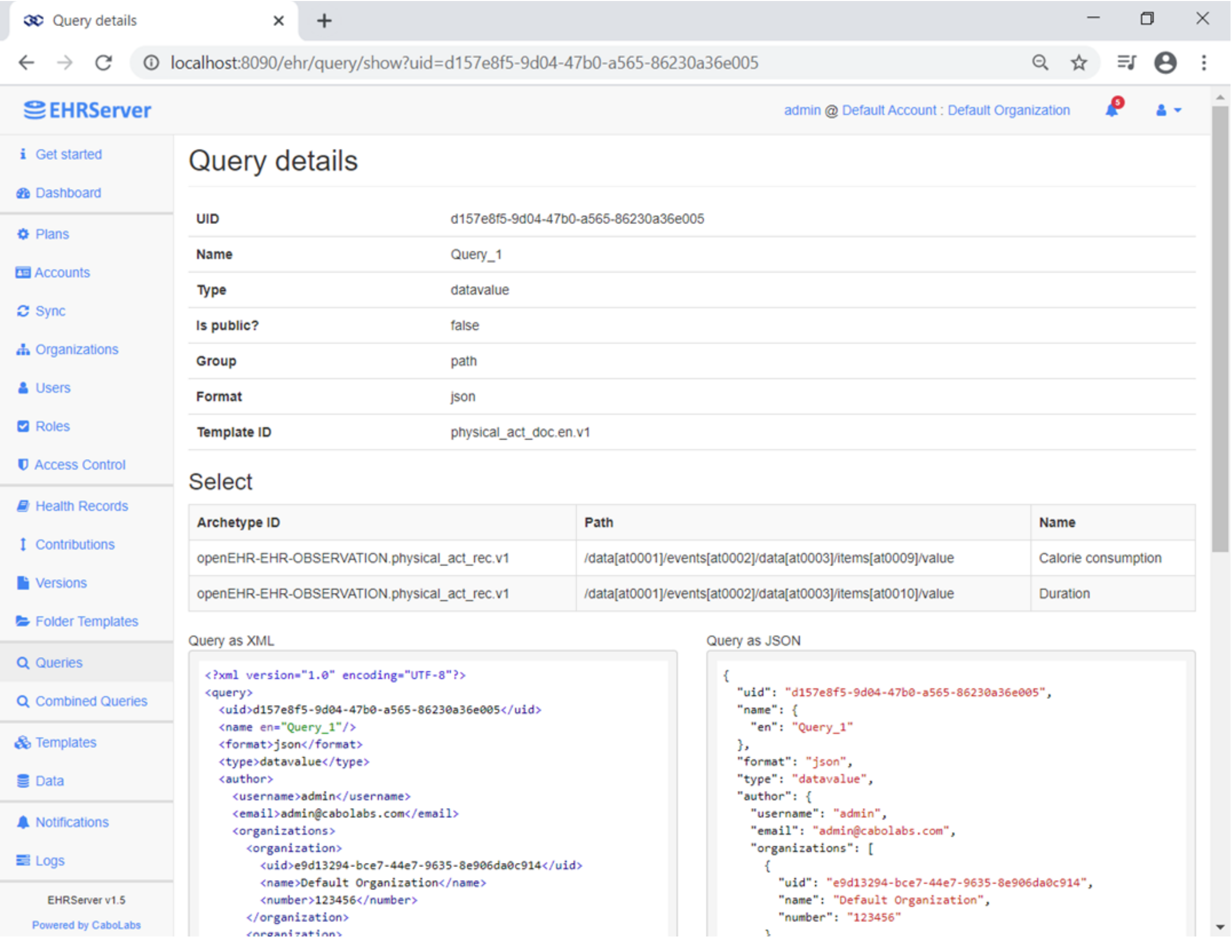
- We get the results of our data query (the calorie consumption and duration of exercise for patient 1)



```
        {
          "magnitude": 34,
          "units": "min",
          "date": "2020-01-22 13:35:28",
          "instanceTemplatePath": "physical_act_doc.en.v1/content[archetype_id=openEHR-EHR-OBSERVATION.physical_act_rec.v1](0)/data[at0001]/e
vents[at0002](0)/data[at0003]/items[at0010](2)/value"
        },
        {
          "magnitude": 46,
          "units": "min",
          "date": "2020-01-22 13:55:50",
          "instanceTemplatePath": "physical_act_doc.en.v1/content[archetype_id=openEHR-EHR-OBSERVATION.physical_act_rec.v1](0)/data[at0001]/e
vents[at0002](0)/data[at0003]/items[at0010](2)/value"
        },
        {
          "magnitude": 57,
          "units": "min",
          "date": "2020-01-22 14:00:36",
          "instanceTemplatePath": "physical_act_doc.en.v1/content[archetype_id=openEHR-EHR-OBSERVATION.physical_act_rec.v1](0)/data[at0001]/e
vents[at0002](0)/data[at0003]/items[at0010](2)/value"
        }
      ]
    }
  }
}
```

Figure 12. 16 The results of our data query

- We save the query as query_1



Query details

UID	d157e8f5-9d04-47b0-a565-86230a36e005
Name	Query_1
Type	datavalue
Is public?	false
Group	path
Format	json
Template ID	physical_act_doc.en.v1

Select

Archetype ID	Path	Name
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0009]/value	Calorie consumption
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0010]/value	Duration

Query as XML

```
<?xml version="1.0" encoding="UTF-8"?>
<query>
  <uid>d157e8f5-9d04-47b0-a565-86230a36e005</uid>
  <name en="Query_1"/>
  <format>json</format>
  <type>datavalue</type>
  <author>
    <username>admin</username>
    <email>admin@cabolabs.com</email>
    <organizations>
      <organization>
        <uid>e9d13294-bce7-44e7-9635-8e906da0c914</uid>
        <name>Default Organization</name>
        <number>123456</number>
      </organization>
      <organization>
```

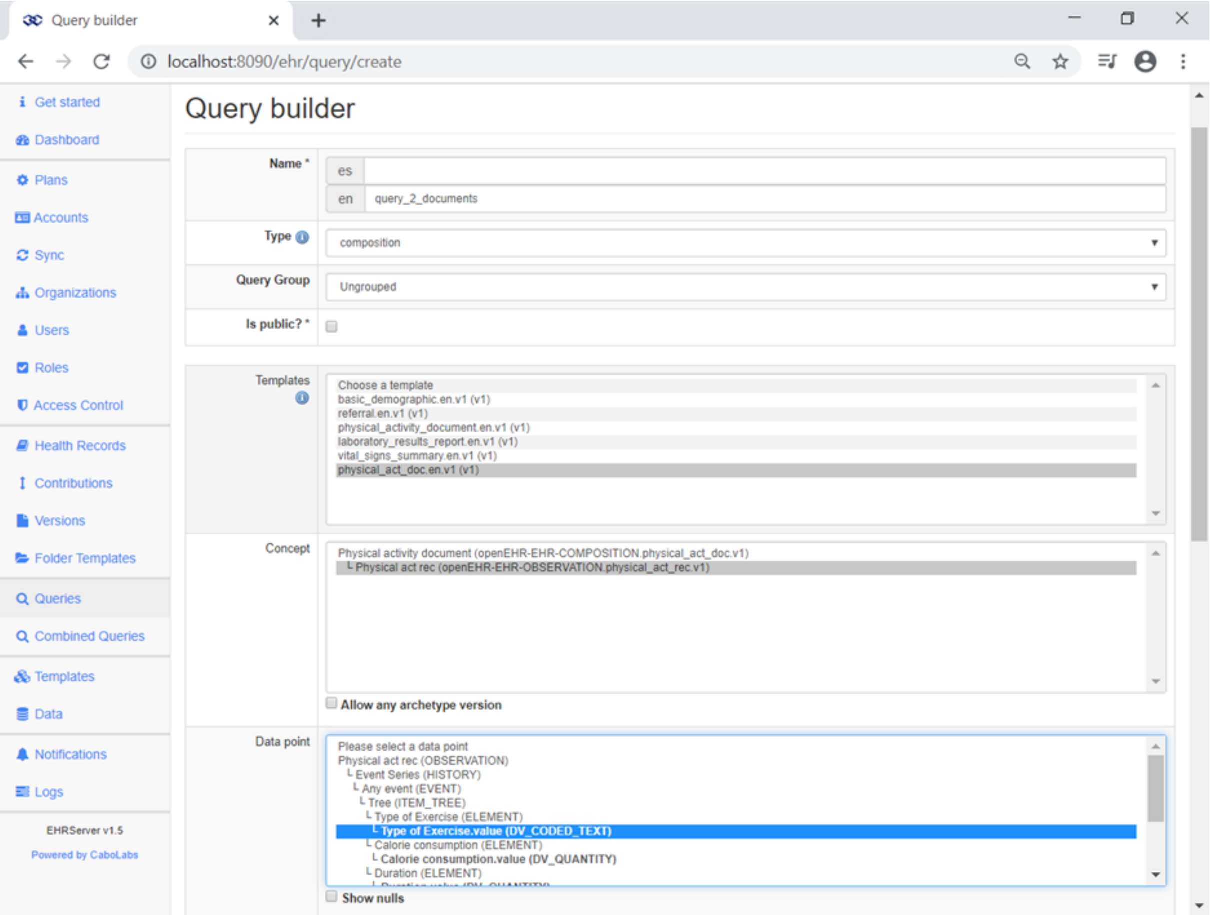
Query as JSON

```
{
  "uid": "d157e8f5-9d04-47b0-a565-86230a36e005",
  "name": {
    "en": "Query_1"
  },
  "format": "json",
  "type": "datavalue",
  "author": {
    "username": "admin",
    "email": "admin@cabolabs.com",
    "organizations": [
      {
        "uid": "e9d13294-bce7-44e7-9635-8e906da0c914",
        "name": "Default Organization",
        "number": "123456"
      }
```

Figure 12. 17 We save the query as query_1

Queries 2nd option – Get full document

- In Templates: We choose our template.
- In Concept: We choose the observation file.
- In Data point: We choose data point of our choice (e.g. calorie, duration).



Query builder

Name *
es
en query_2_documents

Type: composition

Query Group: Ungrouped

Is public? * □

Templates
Choose a template
basic_demographic.en.v1 (v1)
referral.en.v1 (v1)
physical_activity_document.en.v1 (v1)
laboratory_results_report.en.v1 (v1)
vital_signs_summary.en.v1 (v1)
physical_act_doc.en.v1 (v1)

Concept
Physical activity document (openEHR-EHR-COMPOSITION.physical_act_doc.v1)
└ Physical act rec (openEHR-EHR-OBSERVATION.physical_act_rec.v1)

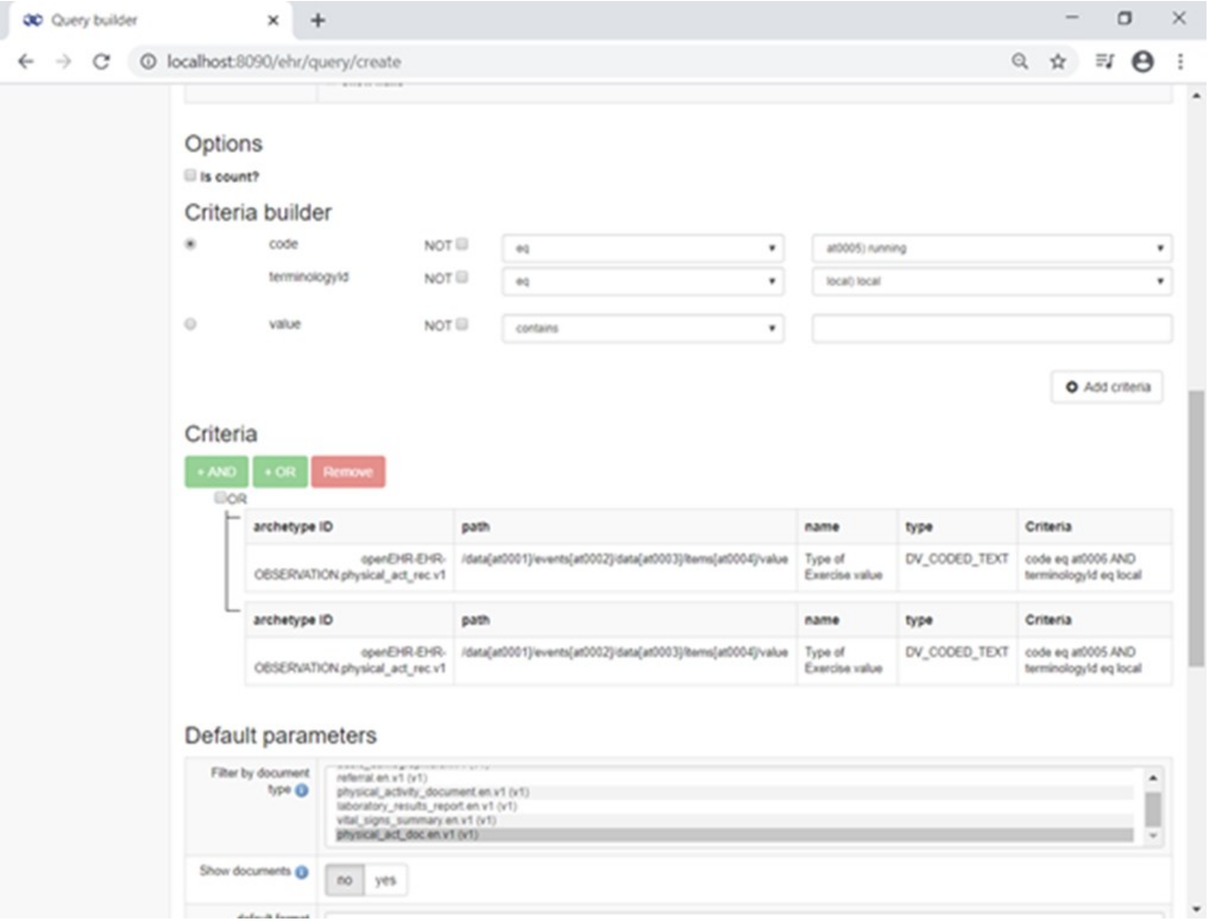
□ Allow any archetype version

Data point
Please select a data point
Physical act rec (OBSERVATION)
└ Event Series (HISTORY)
└ Any event (EVENT)
└ Tree (ITEM_TREE)
└ Type of Exercise (ELEMENT)
└ Type of Exercise.value (DV_CODED_TEXT)
└ Calorie consumption (ELEMENT)
└ Calorie consumption.value (DV_QUANTITY)
└ Duration (ELEMENT)

□ Show nulls

Figure 12. 18 Queries 2nd option – Get full document

- We choose the criteria of our query.
- In document type : We choose observation document of our choice.



Options

□ Is count?

Criteria builder

●	code	NOT □	eq	at0005) running
	terminologyId	NOT □	eq	local) local
○	value	NOT □	contains	

Criteria

□OR

archetype ID	path	name	type	Criteria
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0004]/value	Type of Exercise value	DV_CODED_TEXT	code eq at0006 AND terminologyId eq local

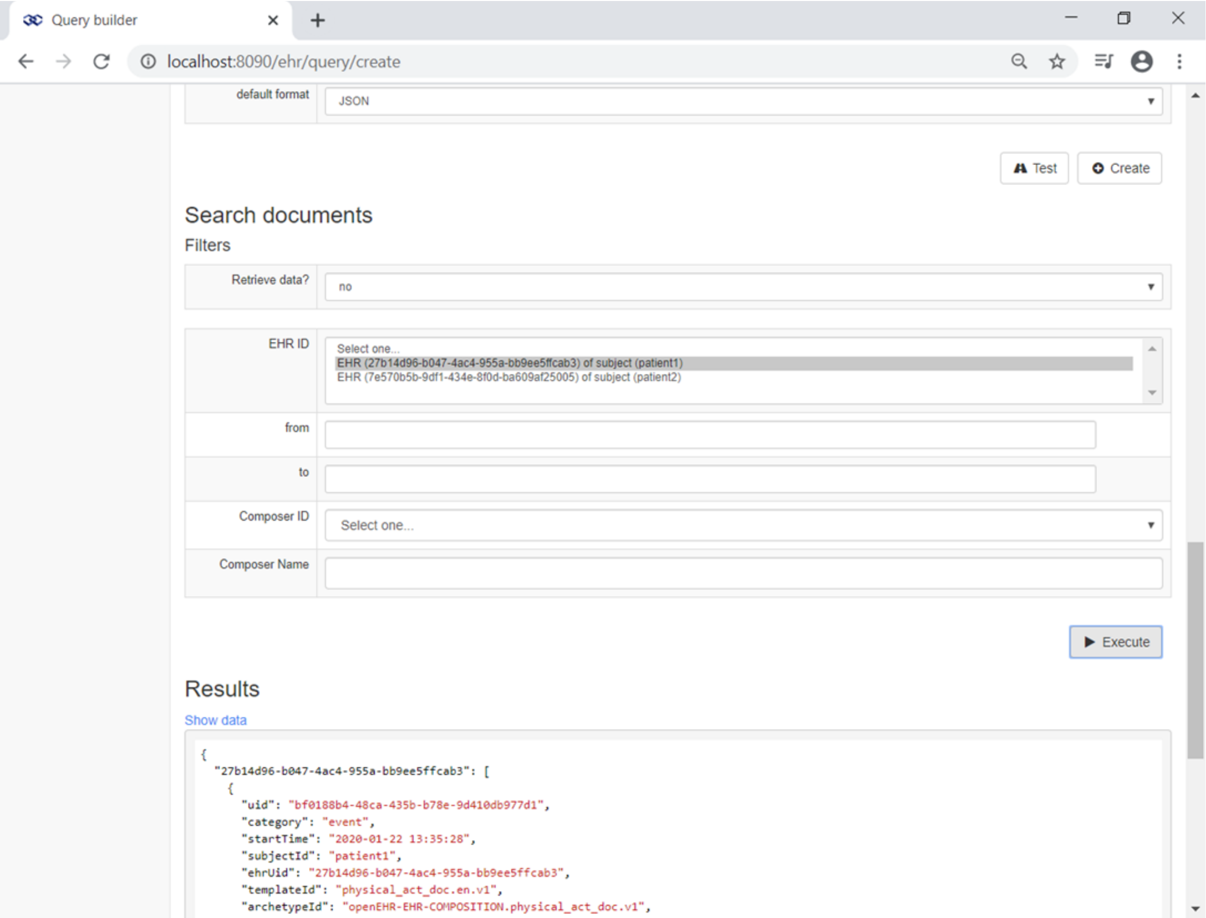
archetype ID	path	name	type	Criteria
openEHR-EHR-OBSERVATION.physical_act_rec.v1	/data[at0001]/events[at0002]/data[at0003]/items[at0004]/value	Type of Exercise value	DV_CODED_TEXT	code eq at0005 AND terminologyId eq local

Default parameters

Filter by document type	referral.en.v1 (v1) physical_activity_document.en.v1 (v1) laboratory_results_report.en.v1 (v1) vital_signs_summary.en.v1 (v1) physical_act_doc.en.v1 (v1)
Show documents	no yes

Figure 12. 19 Queries 2nd option – Get full document - In document type

- In EHRs: We choose the first patient.



default format: JSON

Search documents

Filters

Retrieve data?: no

EHR ID: Select one...
EHR (27b14d96-b047-4ac4-955a-bb9ee5ffcab3) of subject (patient1)
EHR (7e570b5b-9df1-434e-8f0d-ba609af25005) of subject (patient2)

from:

to:

Composer ID: Select one...

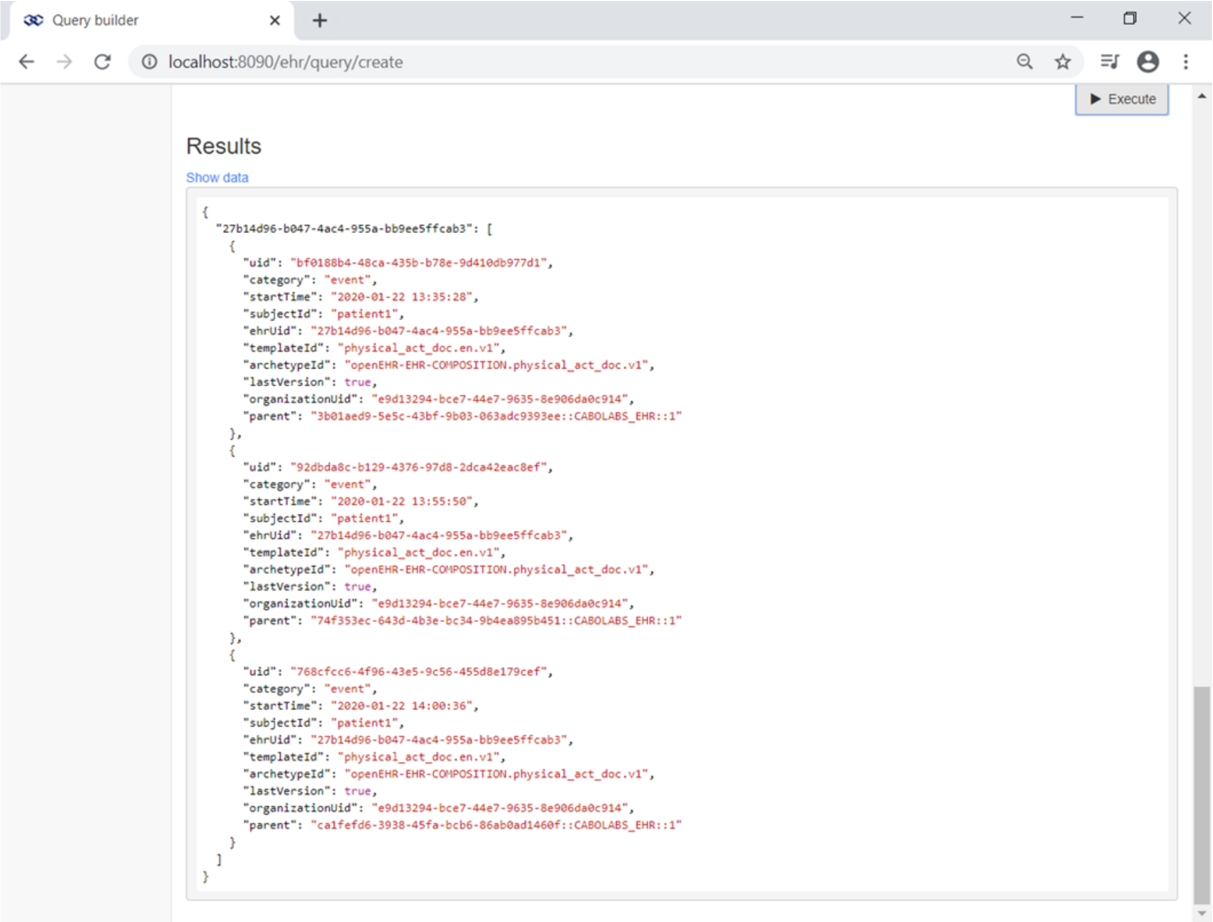
Composer Name:

Results

```
{
  "27b14d96-b047-4ac4-955a-bb9ee5ffcab3": [
    {
      "uid": "bf0188b4-48ca-435b-b78e-9d410db977d1",
      "category": "event",
      "startTime": "2020-01-22 13:35:28",
      "subjectId": "patient1",
      "ehrUid": "27b14d96-b047-4ac4-955a-bb9ee5ffcab3",
      "templateId": "physical_act_doc.en.v1",
      "archetypeId": "openEHR-EHR-COMPOSITION.physical_act_doc.v1",
```

Figure 12. 20 Queries 2nd option – Get full document - In EHRs

- We get the three documents that comply with the conditions (walking or running).



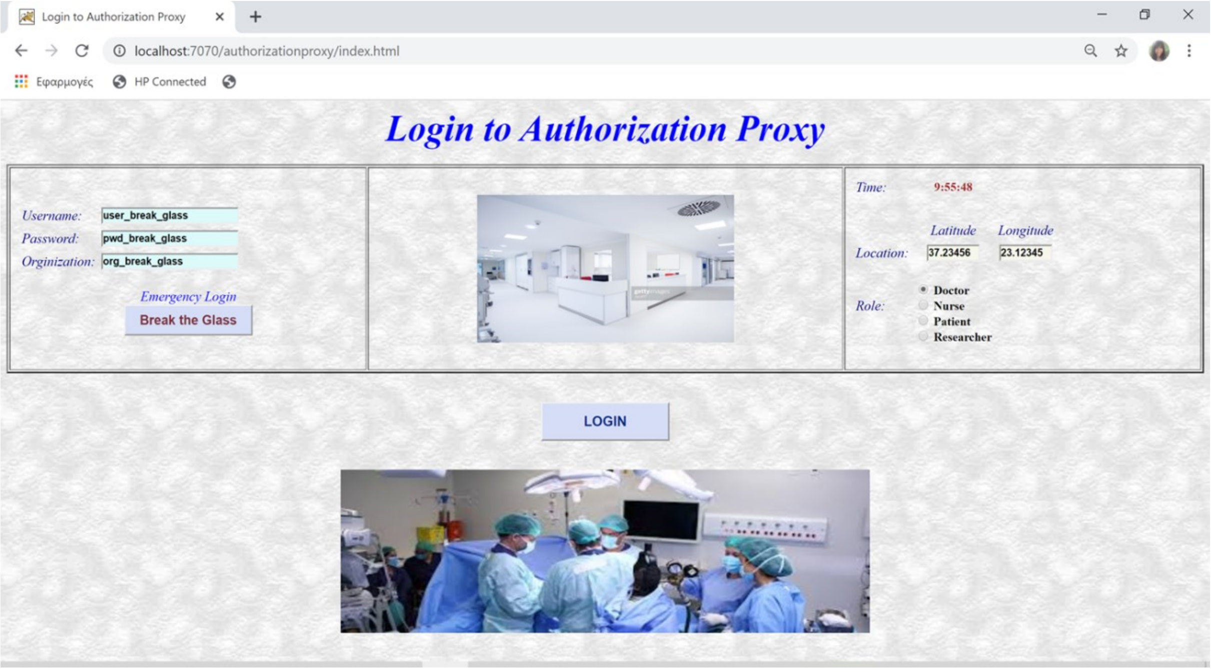
Results

```
{
  "27b14d96-b047-4ac4-955a-bb9ee5ffcab3": [
    {
      "uid": "bf0188b4-48ca-435b-b78e-9d410db977d1",
      "category": "event",
      "startTime": "2020-01-22 13:35:28",
      "subjectId": "patient1",
      "ehrUid": "27b14d96-b047-4ac4-955a-bb9ee5ffcab3",
      "templateId": "physical_act_doc.en.v1",
      "archetypeId": "openEHR-EHR-COMPOSITION.physical_act_doc.v1",
      "lastVersion": true,
      "organizationUid": "e9d13294-bce7-44e7-9635-8e906da0c914",
      "parent": "3b01aed9-5e5c-43bf-9b03-063adc9393ee::CABOLABS_EHR::1"
    },
    {
      "uid": "92dbda8c-b129-4376-97d8-2dca42eac8ef",
      "category": "event",
      "startTime": "2020-01-22 13:55:50",
      "subjectId": "patient1",
      "ehrUid": "27b14d96-b047-4ac4-955a-bb9ee5ffcab3",
      "templateId": "physical_act_doc.en.v1",
      "archetypeId": "openEHR-EHR-COMPOSITION.physical_act_doc.v1",
      "lastVersion": true,
      "organizationUid": "e9d13294-bce7-44e7-9635-8e906da0c914",
      "parent": "74f353ec-643d-4b3e-bc34-9b4ea895b451::CABOLABS_EHR::1"
    },
    {
      "uid": "768cfcc6-4f96-43e5-9c56-455d8e179cef",
      "category": "event",
      "startTime": "2020-01-22 14:00:36",
      "subjectId": "patient1",
      "ehrUid": "27b14d96-b047-4ac4-955a-bb9ee5ffcab3",
      "templateId": "physical_act_doc.en.v1",
      "archetypeId": "openEHR-EHR-COMPOSITION.physical_act_doc.v1",
      "lastVersion": true,
      "organizationUid": "e9d13294-bce7-44e7-9635-8e906da0c914",
      "parent": "ca1fefd6-3938-45fa-bcb6-86ab0ad1460f::CABOLABS_EHR::1"
    }
  ]
}
```

Figure 12. 21 Queries 2nd option – Get full document - In EHRs – 3 Results

i) Authorization proxy server

As of part of this thesis includes the creation of authorization proxy server in order to communicate with EHRServer's medical records.


Login to Authorization Proxy
localhost:7070/authorizationproxy/index.html
Εφαρμογές
HP Connected

Login to Authorization Proxy

Username: user_break_glass
Password: pwd_break_glass
Orginization: org_break_glass

Emergency Login

Break the Glass

Time: 9:55:48

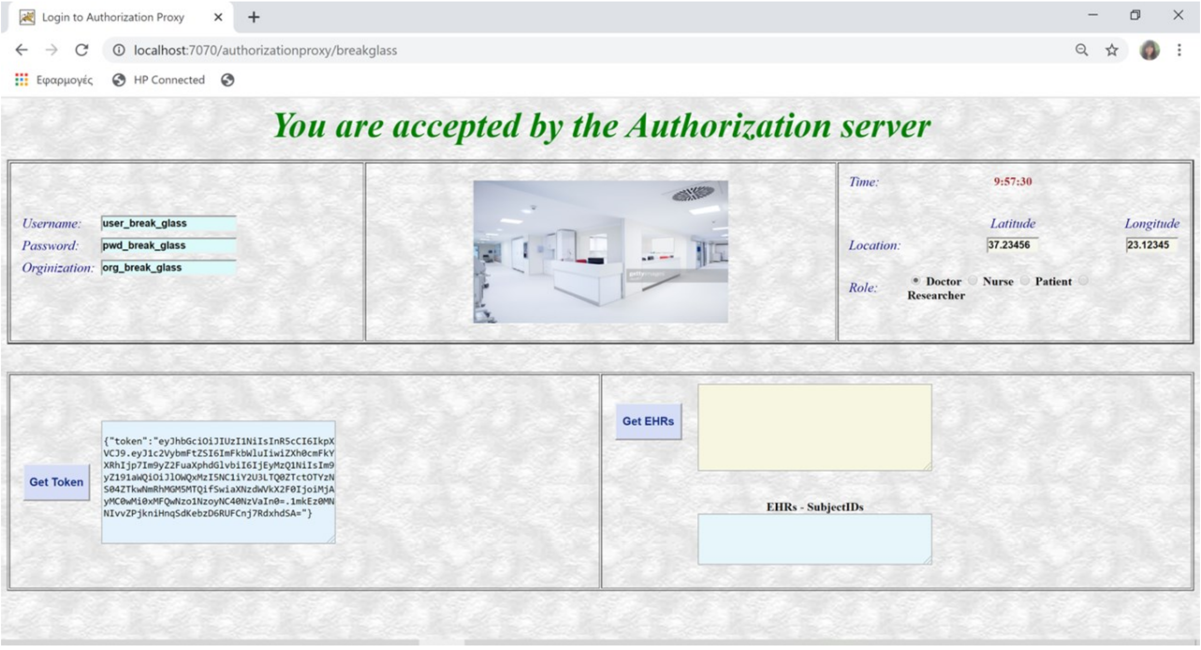
Location: Latitude 37.23456 Longitude 23.12345

Role:
● Doctor
○ Nurse
○ Patient
○ Researcher

LOGIN

Figure 12. 22 Authorization proxy server

First of all, we achieve the break the glass access from Authorization proxy server and we get token from EHRServer


Login to Authorization Proxy
localhost:7070/authorizationproxy/breakglass
Εφαρμογές
HP Connected

You are accepted by the Authorization server

Username: user_break_glass
Password: pwd_break_glass
Orginization: org_break_glass

Time: 9:57:30

Location: Latitude 37.23456 Longitude 23.12345

Role: ● Doctor ○ Nurse ○ Patient ○ Researcher

Get Token

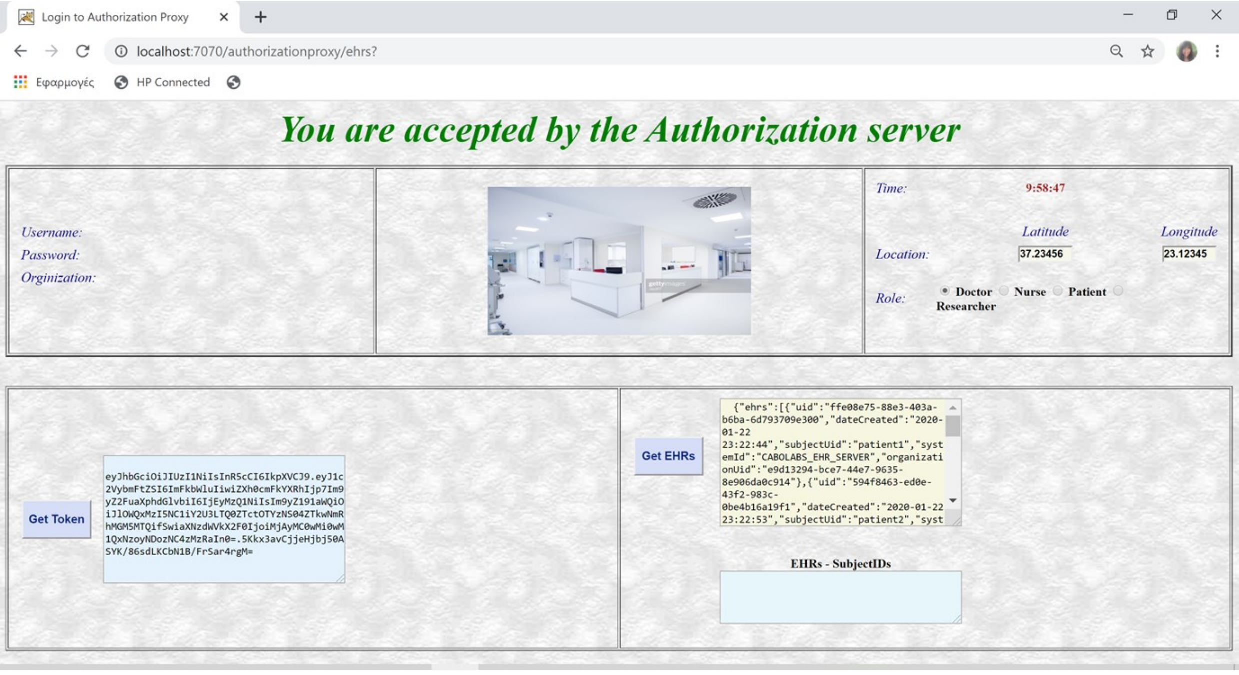
```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX
VCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXh0cmFkY
XRhIjp7Im9yZ2FuaXphdGlvbiI6IjEyMzQ1NiIsIm9
yZ191aWQiOiJlOWQxMzI5NC1iY2U3LTQ0ZTctOTYzN
S04ZTkwNmRhMGM5MTQifSwiaXNzdWVkX2F0IjoiMjA
yMC0wMi0xMFQwNzo1NzoyNC40NzVaIn0=.1mkEz0MN
NIvvZPjkniHnqSdKebzD6RUFCnj7RdxhdSA="}
```

Get EHRs

EHRs - SubjectIDs

Figure 12. 23 Authorization proxy server - Get the token from EHRServer

In addition, we get EHRs from EHRServer.


Login to Authorization Proxy
localhost:7070/authorizationproxy/ehrs?
Εφαρμογές
HP Connected
Get Token
Get EHRs

You are accepted by the Authorization server

Username:
Password:
Orginization:

Time: 9:58:47

Location: Latitude 37.23456 Longitude 23.12345

Role: ● Doctor ○ Nurse ○ Patient ○ Researcher

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c
2VybmFtZSI6ImFkbWluIiwiZXh0cmFkYXRhIjp7Im9
yZ2FuaXphdGlvbiI6IjEyMzQ1NiIsIm9yZ191aWQiO
iJlOWQxMzI5NC1iY2U3LTQ0ZTctOTYzNS04ZTkwNmR
hMGM5MTQifSwiaXNzdWVkX2F0IjoiMjAyMC0wMi0wM
1QxNzoyNDozNC4zMzRaIn0=.5Kkx3avCjjeHjbj50A
SYK/86sdLKCbN1B/FrSar4rgM=
```

```
 {"ehrs":[{"uid":"ffe08e75-88e3-403a-
b6ba-6d793709e300","dateCreated":"2020-
01-22
23:22:44","subjectUid":"patient1","syst
emId":"CABOLABS_EHR_SERVER","organizati
onUid":"e9d13294-bce7-44e7-9635-
8e906da0c914"},{"uid":"594f8463-ed0e-
43f2-983c-
0be4b16a19f1","dateCreated":"2020-01-22
23:22:53","subjectUid":"patient2","syst
```

EHRs - SubjectIDs

Figure 12. 24 Authorization proxy server - Get the EHRs from EHRServer

B. Context-aware Security Model, Context-aware Security Model Editor and Policy Editor

1) Motivation

The need of a trusted environment in which only authorized users are permitted to access a system was of imperative importance since the early days of cloud computing. Even nowadays, a lot of users seem to be reluctant to store their personal data in the cloud and specifically the data related to bank accounts and the health care domain. Our goal is to enhance the access control mechanisms that can be used in the healthcare domain for enhancing the security and privacy of EHR systems.

A promising approach for alleviating the security risks associated with cloud computing is to define effective context-aware security controls for the sensitive data of cloud applications. Our work hinges upon an access control scheme that takes into account the inherently dynamic nature of cloud environments and that will capture the knowledge that lurks behind such a scheme (e.g., actions, subjects, locations, environmental attributes, etc.) This access control scheme calls for the incorporation of the notion of context in access control policies, i.e., the consideration of dynamically-changing contextual attributes that may characterize data accesses. Context can be perceived as any information that can be used to characterize the situation of an entity (person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves [1]. In fact, the use of contextual information makes it possible to apply access control policies by mainly considering the circumstances under which access requests to sensitive data, should be granted. This characteristic, which involves the development of a re-usable and generic context-aware security model, is further elaborated in terms of this work.

Access control protocols are responsible for deciding if a user has the right to execute a certain operation on a specific object. Objects can be a server, a service, an application, an entire relational database, a single row in table or even an entire wide column in a NoSQL datastore. Common operations are read, write, delete, update etc. The user is considered as the active element and is called subject. A permission associates an object with an operation. Static access control models, usually, provide a list of permissions that each subject has on certain objects. Commonly used access control models are the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) and the Role-Based Access Control (RBAC) [2]. All these models are known as identity-based access control models where user (subjects) and resources (objects) are identified by unique names [3]. In the literature, a fourth type has been identified, the Attribute Based Access Control (ABAC) [4] which is by nature dynamic. In ABAC, there are no static lists of permissions that associate subjects with objects, but instead there are “snapshots” of such associations that can be generated and dynamically change, based on the current context. In our work, the process of granting/denying access on data artefacts is based on dynamically changing parameters, thus we rely on an ABAC model, which goes beyond the traditional security models that are usually context insensitive. The context parameters are individual for every single user or access request, so for granting access it is necessary to regard the single user, the object that s/he is requesting to access and any external information that should be considered for enhancing the security.

Contrary to the aforementioned models, the Attribute Based Access Control (ABAC) [4] is dynamic because there are no static lists of permissions that associate subjects with objects, but instead there are “snapshots” of such associations that can be generated and dynamically change, based on the current context. A recent model for encrypted access control is Attribute-Based Encryption (ABE) [5], in which ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography, but both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes instead.

This chapter focuses on defining and evaluating contextual information (e.g., the identity of a user, its role, patterns of access, connection type etc.) and attributes that characterise sensitivity levels of data. This information is considered in ASCLEPIOS before granting any data access request. Based on such information the contextual model was presented in (c2) and building on it a number of enforcement rules can be created as the most elementary structural elements of policies. Indicatively, attributes that are organized in a hierarchical structure may include concepts related to: i) the device from which there is an access attempt, ii) the actor that tries to access the data (e.g. location, IP, role in the healthcare use case, etc.) and iii) historic data that reveal patterns of access (e.g. frequency, usual dates or hours of access, usual duration of access, previously accessed data, etc.). Such concepts along with a number of properties that interrelate them, serve as background knowledge for the ASCLEPIOS access control policies. These access control policies are then enforced as part of two different authorisations paradigms that are employed in ASCLEPIOS in sequence for achieving even higher levels of security controls. These paradigms are the Attribute-based Access Control (ABAC) and the Attribute-based Encryption (ABE).

This part of the dissertation reports on the development of all the appropriate mechanisms for updating the contextual model and devising the context-aware access policies, i.e., editing functionalities for creating context-aware access policies (ABAC and ABE) and the interpretation mechanism that will export these policies in the appropriate format for enabling the access enforcement mechanisms, as presented in (c3) . The purpose of this work is two-fold. First it describes in a fine-grained way each related mechanism's purpose, value and overall contribution to the ASCLEPIOS framework, and second it reveals and comments on the details of the mechanisms' implementation.

The primary objectives of this deliverable are to:

1. Provide the necessary editor for improving and extending the ASCLEPIOS context-aware security model;
2. Develop the appropriate editing functionalities for allowing DevOps of cloud-based eHealth systems to declaratively create the minimum amount of rule-set that needs to be enforced for security purposes and organise it across ABAC policies;
3. Dynamically interpret these annotations into formats that enable the ABAC authorisation mechanisms.

*2) **Methods and Tools***

a) ASCLEPIOS Context Aware Security Model

The approach of (c2) proposes a context-aware security model based on a combination of the ABAC and ABE models. ABE considers supplemental important aspects of access control. More precisely, ABE is not used for directly encrypting or decrypting the health records but instead for the actual secret key that was used for encrypting them before being uploaded and persisted to "untrusted" cloud resources. In case a user (e.g., a general practitioner) would like to access a patient's Electronic Health Records (EHRs), s/he should be able to transmit a request along with certain attributes (expressing the current context of the requestor). In order to be successfully authorized, these attributes should satisfy ABAC and ABE policies, defined by the data owner beforehand. The ABE policy is used by the data owner for encrypting the symmetric key with which the sensitive medical data have been encrypted. Thus, a successful ABE authorization implies the decryption of a key, which then can be used for acquiring the plaintext of the encrypted medical records. The ABAC and ABE layers, which are both based on policies, are combined in an innovative way and enforced following the process described in Figure 12.25, in order to satisfy the need for advanced access control for cloud persisted health data. The ABAC layer provides a fine-grained access control by evaluating rules of any complexity that upon successful assessment, they provide access to any object persisted in cloud resources (i.e., encrypted EHR). The engagement of the ABE layer follows the ABAC permit decision, in order to authorize the deduction of the decryption key (i.e., symmetric searchable encryption private key) that can decrypt the requested EHR. The ABE paradigm enforcement comprises the result of a cryptographic function that evaluates any policy embedded on the ciphertext according to the attribute values embedded on the requestor's private key. We note that this cryptographic function restricts the potential complexity of the policies used as it allows only for conjunction and disjunction operators in the rules expressions. The final result is the decrypted healthcare-related data.

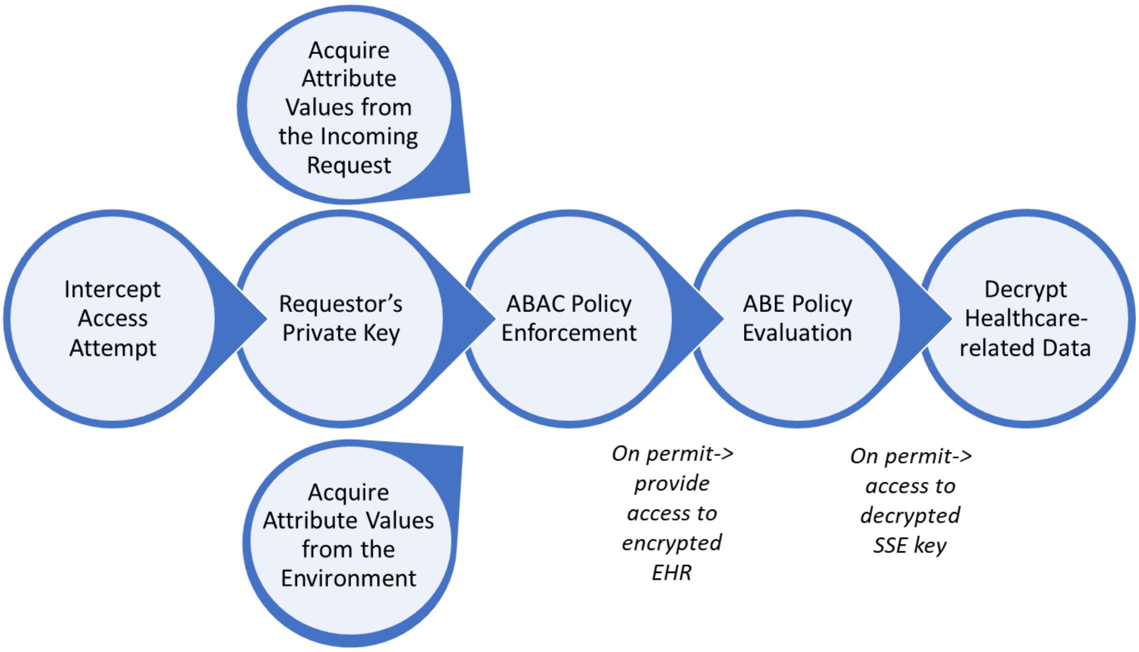

Acquire Attribute Values from the Incoming Request
Intercept Access Attempt
Requestor's Private Key
ABAC Policy Enforcement
ABE Policy Evaluation
Decrypt Healthcare-related Data
Acquire Attribute Values from the Environment
On permit-> provide access to encrypted EHR
On permit-> access to decrypted SSE key

Figure 12. 25 Data Authorization Process Combining ABAC and ABE Paradigms.

In this work, we focus on the formal description of the attributes that can be used both in ABAC and in ABE policy expressions. This refers to the definition and evaluation of contextual information, such as, the identity of a user, his/her role, patterns of access and connection type that should be considered before granting any data access request. Therefore, primarily, this context-aware security model conceptualizes, through an appropriate vocabulary, all the facets, that must be taken under consideration during the development and enforcement of a data access control policy. The existence of a common vocabulary in a context model is of paramount importance for its functionality. This vocabulary is also extended with medical taxonomies that amplify its cohesiveness and reusability. Based on this vocabulary, enforcement rules can be modeled as the most fundamental structural elements of policies. Indicatively, attributes that are organized in a hierarchical structure may include concepts related to: i) the device from which there is an access attempt, ii) the actor that tries to access the data (e.g., location, IP, role in the healthcare use case) and iii) historic data that reveal patterns of access (e.g., frequency, usual dates or hours of access, usual duration of access and previously accessed data). Such concepts along with a number of properties that interrelate them, serve as background knowledge for the access control policies.

Our model is an extension of the original PaaSword context aware security model [6] for supporting the combination of ABAC and ABE access models in the healthcare domain. The model is composed by five main classes. These classes described below, are subclasses of the class SecurityContextElement that refers to several contextual attributes that may be associated with the subject and/or the objects of a request as well as with the request itself [6], [7].

- ***Object***: contains types of sensitive data;
- ***Subject***: represents a requestor who intends to access the object content. More precisely, the requestor could be a person, an organization, a group or a software;
- ***Location***: models and registers the exact location of a subject who requests access to data;
- ***DateTime***: models the exact date and time of a subject requesting data access;
- ***Connectivity***: represents the device type, the connection type, the connection security and the connection metrics.

Security Context Element Overview

The ASCLEPIOS context model formally describes classes and properties with respect to: i) associations between types of access to sensitive data and situations under which this access should be permitted; ii) cryptographically matching policies between ABE private keys and ciphertexts for permitting decryption of sensitive data; iii) concepts that capture and highlight possible cyber security threats for enhancing the security awareness of actors in hospitals and care centres. This model constitutes the necessary background knowledge layer for enabling the ABAC and ABE paradigms. Specifically, such situations and policies are determined through a number of attributes that specify valuable security-related details of the entity that is requesting access to sensitive data, the data itself and its ambient environment. Such attributes are organized in a hierarchical structure that may include concepts related to: i) the device from which there is an access attempt, ii) the actor that tries to access the data (e.g. location, IP, role in the healthcare use case, etc.) and iii) historic data that reveal patterns of access (e.g. frequency, usual dates or hours of access, usual duration of access, previously accessed data, etc.). We reuse similar context models from the cloud security domain (e.g. PaaS Security Context model) and extend them in order to cope with concepts, challenges and standards from the healthcare domain.

This context-aware security model is based on the vocabulary of PaaSword context model which is the base for a generic and structured context model. We managed to extend it such as to serve the quite demanding, structured and specialized field of healthcare. Our context model has enriched the classes of Subject, Object and Connectivity to consider important concepts from the medical sector. In the class Subject, its subclasses Person, Organization and Authentication Method were enriched. The class Person was enriched with classes: Technical Staff, Contact Person / Legal Guardian, Administrative Staff, Medical Force, Researcher, Employer and Patient. The class Organization was enriched with classes: Insurance Company, GP (General Practitioner's) Office, Hospital, Diagnostic Centre and Research Institution. In class Authentication Method a subclass Biometric Information was added. In class Object, a subclass Medical Artefact was created. The class Medical Artefact has the following subclasses: EHR, Medical Process and Medical Report. In the subclass Security Protocol of the class Connectivity, the subclass Security Protocol Certificate was added. The class Connectivity was enriched so as to enhance the model's security and safety. Figure 12.26 demonstrates the enhancements of our model (dark blue colour denotes new classes), enriched with external medical ontologies (green colour), to the PaaSword context model (light blue colour). Figure 12.27 depicts precisely the enhancements of class Object. Finally, Figure 12.28 demonstrates analytically the enhancements of class Subject.

We provide an elaboration of ASCLEPIOS model in the form of facets. For each of these context model facets, we present an overview (i.e. class/sub-class) diagram, a list of its core concepts and properties (in tabular format), and a UML class diagram that formalises it.

Security Context Element Details

The security context element [8] (Figure 12.26) refers to the following five top-level concepts:

- ***Location***
- ***DateTime***
- ***Connectivity***
- ***Object***
- ***Subject***

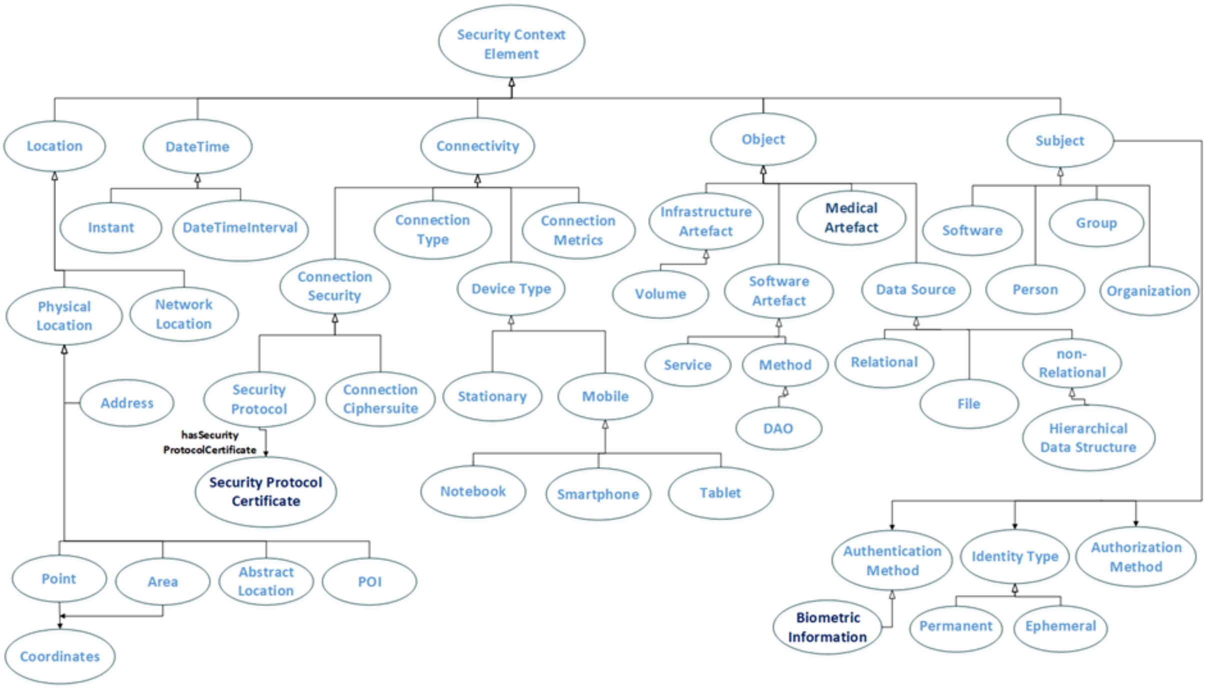


Figure 12. 26 ASCLEPIOS Security Context Element overview diagram

In Figure 12.27 [9], the details of the Object context element are presented. The class Object is extended by our context model by the main class Medical Artefact which is analysed to the three main classes EHR, Medical Process and Medical Report. We note that the following classes: Environment, Genetics, History, Treatment, Encounters, Diagnostics, Diagnoses, Socioeconomic and Symptoms, Lifestyle, Social Network existed in the proposed types of data of an EHR by Weber et al [10].

These three main classes are defined as follows:

- Medical Artefact: This class refers to any medical sensitive data entities stored in schema-based or schema-less databases that should be protected from unauthorized access.
- Medical Process: This class represents the administrative medical process of the medical condition of each patient during his or her treatment (e.g., it attempts to improve the medical condition of a patient based on some kind of treatment).
- Medical Report: This class represents the dispatch of the results of a medical examination of a patient.
- EHR: This class represents the patient’s Electronic Health Records (EHRs). EHR represents a digital collection of medical information about a person. It includes information about a patient’s health history, such as diagnoses, medicines received, tests, allergies, immunizations, and treatment plans.

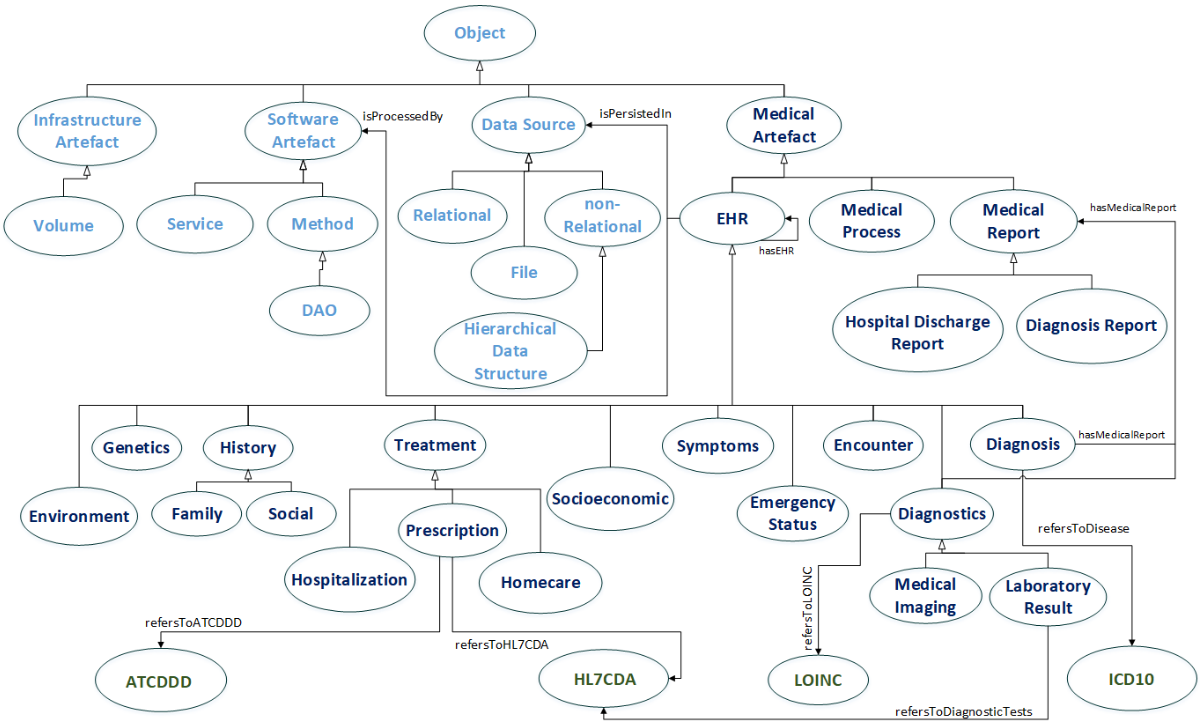


Figure 12. 27 Extension of Security Context Element Object overview diagram

In Figure 12.28 [11], the details of the Subject context element are presented. We note that although both Object and Subject may participate as individual concepts in access rules or policy expressions, we consider them as part of our model, in order to cover some of the valuable contextual information that usually accompany them. Such contextual information can enhance the access control where it might be not enough to identify who is the entity that is requesting access and what is the target object. Additional information about both of them can lead to the enforcement of even more dynamic and context-aware access controls (e.g. how has the entity been authenticated? What type of data does the access request target?).

In our context model, we focus, first of all, on the subclasses Person and Organization which derive from the parent class Subject. We also focus on the class Authentication Method which is related to class Subject. All these classes are categorized as follows:

- Person: This class represents people that are either treated as data owners or as data requestors by an EHR system.
- Technical Staff: This is subclass of Person which represents any entity with technical capabilities and responsibilities.
- Administrative Staff: This is a subclass of Person which represents any entity in charge of administrative responsibilities in healthcare provider organization.
- Medical Force: This is a subclass of Person which represents the medical staff who conducts research; improves or develops concepts, theories and operational methods; and applies scientific knowledge relating to medicine.
- Researcher: This is a subclass of Person with instances that correspond to a person who conducts scientific research involving background research, constructing a hypothesis, testing it, analyzing data and concluding the results.
- Employer: This is a subclass of Person with instances that correspond to those workers who, working on their own account or with one or a few partners, hold the type of job defined as a self-employed job, and in this capacity, on a continuous basis have engaged one or more persons to work for them in their business as employees.
- LegalGuardian: This is a subclass of Person that represents a person who legally assists and supports minor children, mentally disabled persons or incapacitated

older adults in their personal life. They can manage their property, help with daily financial administration and assist with the ward's medical or social needs.

- ContactPerson: This is a subclass of Person that represents someone who undertakes the responsibility of communication among healthcare providers or emergency call team in cases of an unconscious patient.
- Patient: This is a subclass of Person with instances that correspond to a person who is a recipient of healthcare, that is services received by individuals or communities to promote, maintain, monitor or restore health.
- Organization: This class represents a kind of agent corresponding to social institutions such as companies, societies etc.
- Insurance Company: This is a subclass of Organization which represents a financial institution which underwrites the risk of and compensates for the loss of, or damage to, personal and business assets (general insurance) and life or limb (life and accident insurance).
- GP Office: This is a subclass of Organization which represents the business entity of a general practitioner.
- Hospital: This is a subclass of Organization which represents an institution dedicated to medical and surgical treatment and nursing care for sick or injured people.
- Diagnostic Centre: This is a subclass of Organization which represents a freestanding facility, program, or provider, including but not limited to, physicians' offices, clinical laboratories, radiology centers, and mobile diagnostic programs.
- Authentication Method: This class reveals the technological means used for validating the identity of a Subject during an access request (e.g., OS, LDAP, OpenID, Anonymous access).
- Biometric Information: This class represents the measurement and statistical analysis of people's unique physical and behavioral characteristics (e.g., fingerprint, iris).

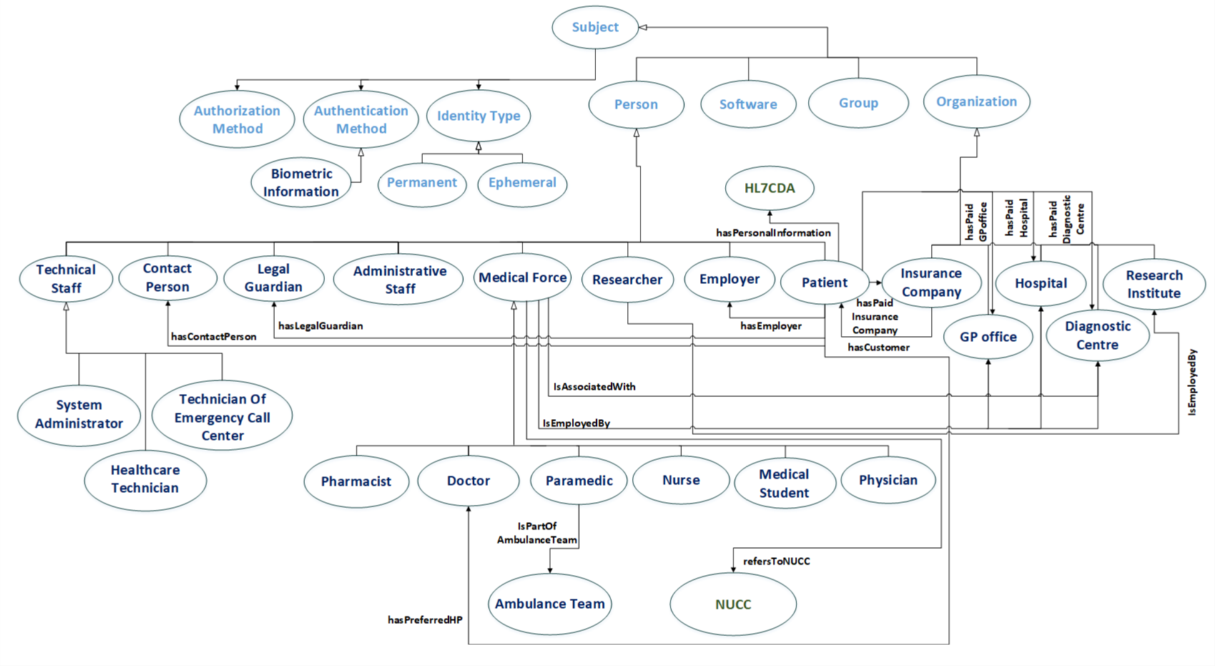


Figure 12. 28 Extension of Security Context Element Subject overview diagram

With respect to concepts related to security awareness we investigated the Common Attack Pattern Enumeration and Classification (CAPEC) taxonomy [12]. In the following Figure 12.29 [13] are demonstrated the main classes of this taxonomy.

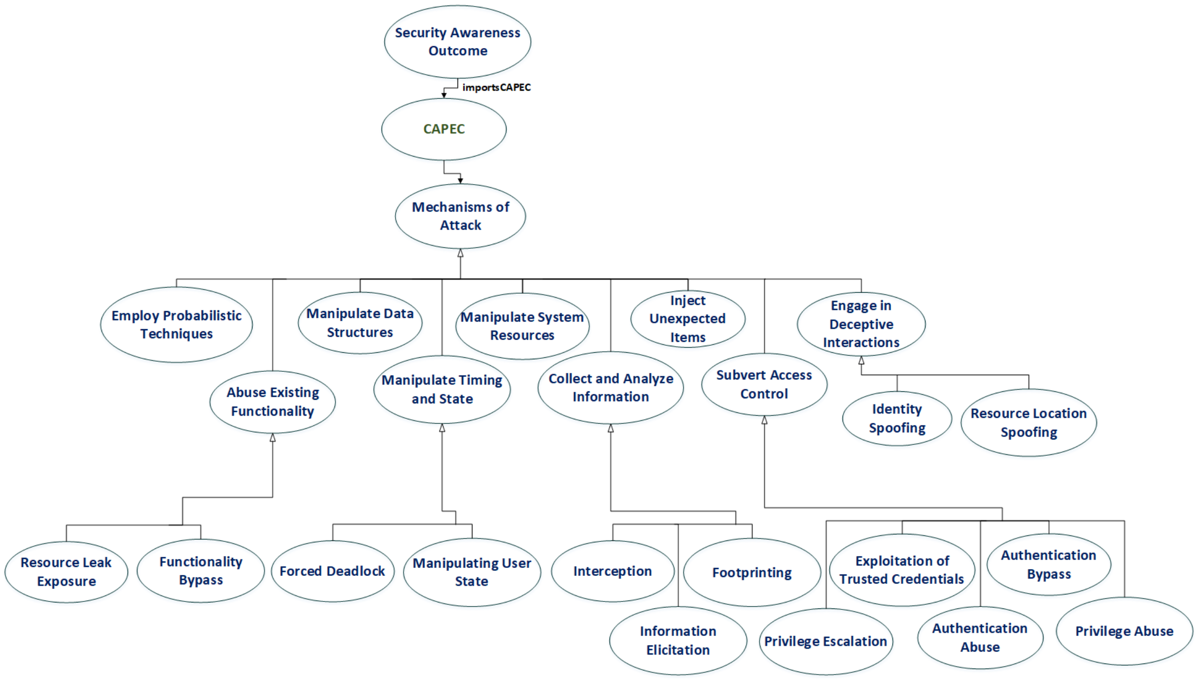


Figure 12. 29 Security awareness component

b) ***Context-aware Security Model Editor and Policy Editor***

Approach and Architecture

This section presents our approach for developing access control rules by means of a context-aware security model (c2). The model acts as a configurable, common vocabulary for application-related access policies, with attributes which can be further tailored to each application's needs and can serve as background knowledge for creating and enforcing access control policies for EHRs. This is crucial since both access control methods (ABAC and ABE) rely on the use of attributes. Therefore, it is important to use attributes in a semantically coherent manner. This common vocabulary is called Context-Aware Security Model (CASM).

CASM is a hierarchical (tree-like) taxonomy of attributes (referred as Concepts), attribute properties, and attribute instance values (or just instances) when they are known beforehand. An attribute is titled with a name, and uniquely identified by a Universal Resource Identifier (URI). It furthermore has an (optional) description which describes its exact semantics. An attribute can have sub-attributes, which are specializations of the parent attribute's meaning. It can also have attribute instances, when they are a priori known, as well as properties that can relate attribute (as a concept) to other attributes or common data types (like numbers, date/time, literals, and Booleans).

Next, we present AMPLE (ASCLEPIOS Models and PoLicies Editors), a web-based, graphical environment for creating and maintaining CASM, as well as using it to define ABAC and ABE policies. In the following sub-section the conceptual architecture of AMPLE as well as some implementation details are provided.

Conceptual Architecture

AMPLE is a unified environment encompassing the CASM editor, and a Models Store (repository). Figure 12.30, provides a visual representation of the conceptual architecture.

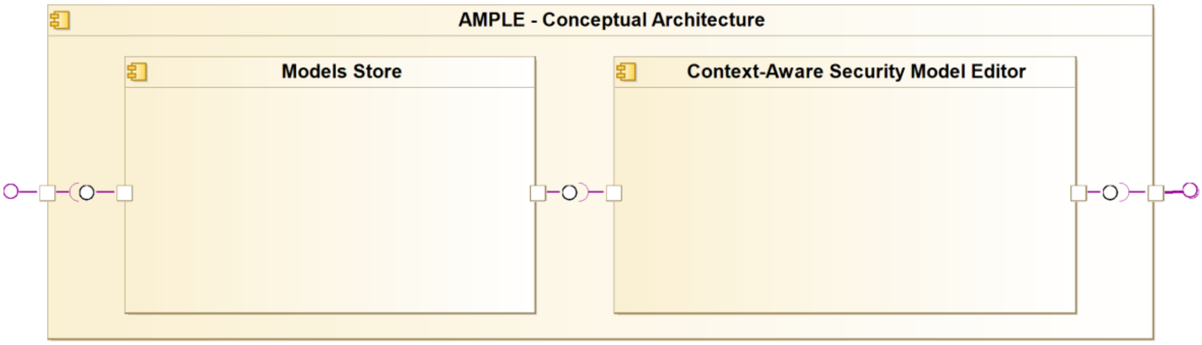

AMPLE - Conceptual Architecture
Models Store
Context-Aware Security Model Editor

Figure 12. 30 AMPLE conceptual architecture

- Context-Aware Security Model Editor: Provides the means for creating and maintaining the Context-Aware Security Model (CASM). CASM paves the path for defining ABAC and ABE policies by using a common vocabulary. CASM Editor offers both a web-based, graphical interface for representing and modifying CASM, as well as the necessary model implementations. CASM is stored in Models Store, thus is made available to other AMPLE tools.
- Models Store: It is a repository for persisting all kinds of models handled in AMPLE; i.e. Context-Aware Security Model, ABAC policies, ABE policies and Policy Validation rules. It internally uses a Resource Description Framework (RDF) triple store for storing the models as well as a layer for serializing model objects (i.e. core elements of the model) to RDF and vice versa.

Techical Architecture

The AMPLE implementation realizes the conceptual architecture presented before, with regard to the provided functionality and overall approach. The actual (technical) structure, components and interconnections of AMPLE parts are explained in physical architecture, presented next. In technical terms, AMPLE is a web-based application, encompassing both a server-side part as well as a client-side part that offers the graphical user interface (as depicted in Figure 12.31). Figure 12.31 also depicts the possibility for third-party Representational State Transfer (REST) clients to interact with AMPLE in order to reuse or modify CASM model. Next, we provide additional details for each of components of the AMPLE physical architecture.

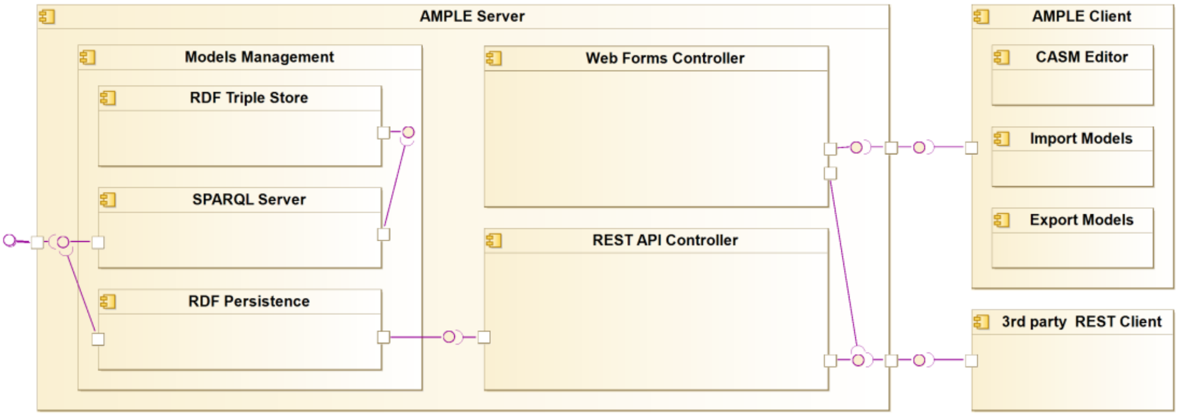


Figure 12. 31 AMPLE technical architecture

AMPLE Server is the core component of the AMPLE physical architecture, and it comprises of the following parts.

- Web Forms controller is responsible for the interaction with the AMPLE client forms, specifically for providing the requested information and collecting the submitted models. Web Forms controllers rely on REST API controllers both for retrieving the requested information and for saving the submitted models. Essentially, it acts as a translation layer between the REST API and the AMPLE client forms, by turning AMPLE client requests into proper REST API requests and vice versa.
- REST API controller accepts REST requests for retrieving information related to CASM (or the whole model) and also for storing model changes. It uses a specific JavaScript Object Notation (JSON) format. REST API controller is used by Web Forms controller (which acts as REST client) but third-party REST clients can also interact with REST API controller, as long as they are capable to handle the JSON messages used and as long as the AMPLE server is configured to accept REST API requests from external clients.
- Models Management is responsible for storing and retrieving CASM-related information. Its internal persistence mechanism is based on an RDF triple store, thus all information is stored and retrieved as RDF triples forming RDF graphs. For this reason, the Models Management component also encompasses a layer that serializes model objects into RDF graphs (representing an object) and vice versa.

The Models Management component comprises of three subcomponents:

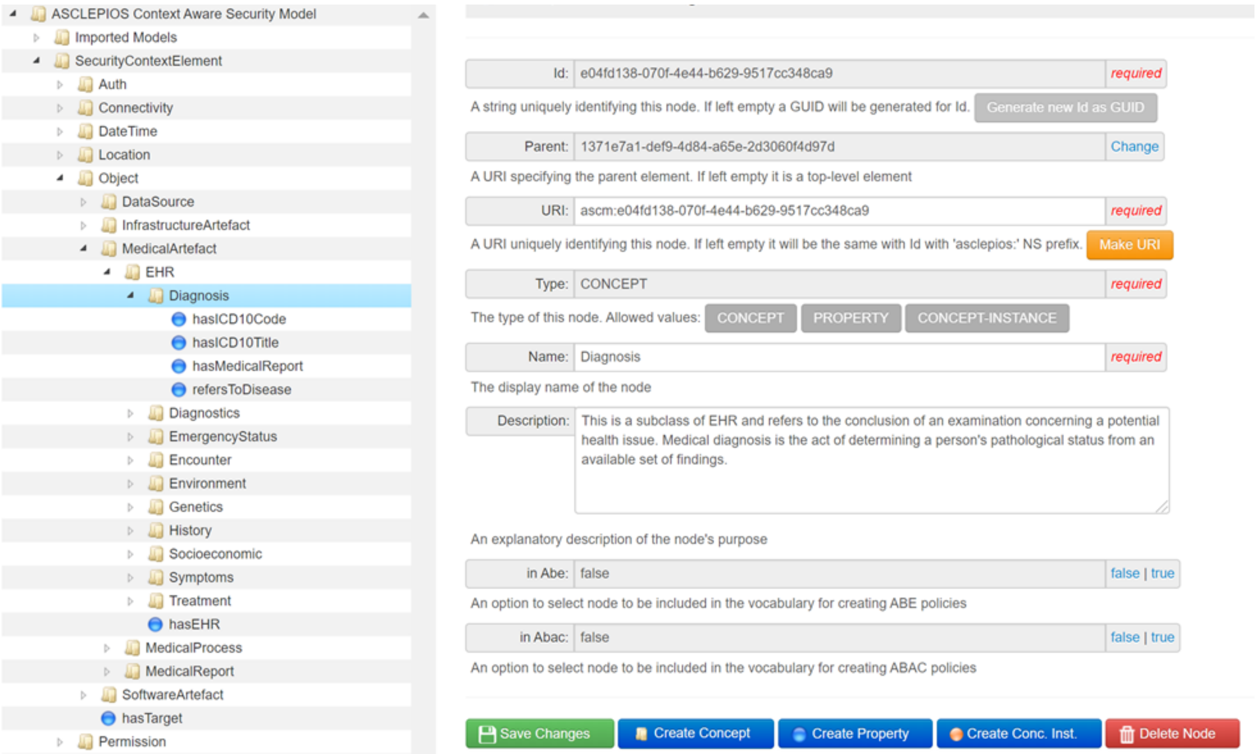
- RDF Triple store, which is responsible for persisting and retrieving RDF graphs describing model objects.
- SPARQL server, which is responsible for accepting and carrying out queries for retrieving and modifying the persisted RDF graphs in RDF triple store. The query language used is SPARQL.
- RDF Persistence, which is responsible for converting model objects into SPARQL queries that are submitted to SPARQL server and persist the state of the model objects into RDF triple store. Reversely, RDF Persistence can build SPARQL queries for retrieving the persisted state of a model object from RDF Triple store and convert the retrieved RDF triples into the corresponding model object, which can subsequently be used in REST API controllers or other AMPLE server components.

The client-side part of AMPLE consists of a set of dynamic web pages that provide the graphical user interface of AMPLE, as well as some common graphical elements like the menu. The web pages are dynamically generated at server-side, using Java Server Pages (JSP), and then are rendered in the user's browser. In response to user actions, web pages can contact the corresponding Web Forms controllers in order to send or retrieve the needed model information.

Implementation and Walkthrough

AMPLE aspires to offer a unified environment of graphical tools for creating, maintaining and validating context-aware access control policies. Specifically, it has been implemented as a web-application, hence allowing its easy usage. To this end various modern Web 2.0 technologies have been used. Figure 12.32 gives a sample snapshot of the CASM Editor.

The screen is vertically divided in two panes. The left-hand pane contains a rendering of CASM in a tree-like fashion. The user can click on the arrow heads on the left side of each element in order to expand it and view its child elements, if any. Clicking on an element loads its details into the details form in the right-hand side of the page. Right clicking on an element in the CASM tree will open the context menu which offers actions related to the selected element.



Id: e04fd138-070f-4e44-b629-9517cc348ca9 required

A string uniquely identifying this node. If left empty a GUID will be generated for Id. Generate new Id as GUID

Parent: 1371e7a1-def9-4d84-a65e-2d3060f4d97d Change

A URI specifying the parent element. If left empty it is a top-level element

URI: ascm:e04fd138-070f-4e44-b629-9517cc348ca9 required

A URI uniquely identifying this node. If left empty it will be the same with Id with 'asclepios:' NS prefix. Make URI

Type: CONCEPT required

The type of this node. Allowed values: CONCEPT PROPERTY CONCEPT-INSTANCE

Name: Diagnosis required

The display name of the node

Description: This is a subclass of EHR and refers to the conclusion of an examination concerning a potential health issue. Medical diagnosis is the act of determining a person's pathological status from an available set of findings.

An explanatory description of the node's purpose

in Abe: false false | true

An option to select node to be included in the vocabulary for creating ABE policies

in Abac: false false | true

An option to select node to be included in the vocabulary for creating ABAC policies

Figure 12. 32 CASM Editor

The details form, in the right-hand side pane of the page, encompasses fields that are common to all element types. The user can create a new attribute (or other element) by first selecting the parent attribute in the CASM tree on the left, and then clicking on the corresponding option, either in the context menu or the buttons under the details form. Right-clicking on a node results in a pop-up context menu which contains the following actions: 1. to create a new child concept or property or property instance; 2. to delete the selected node; 3. to expand the current node's child elements; 4. to deselect the current node and clear the form's fields; 5. to add or remove the selected node and all of its child elements into the ABAC or ABE vocabulary, so as to create the corresponding policies.

For example, to create the concept's property "refersToLOINC", which is a child element of class "Diagnostics", the following steps : 1. The class "Diagnostics" is chosen; 2. The button "New Property" is chosen in the context menu, after having right-clicked on the selected button; 3. The corresponding values of fields "Name", "Description", "Type of property", and "Data Range" are set.

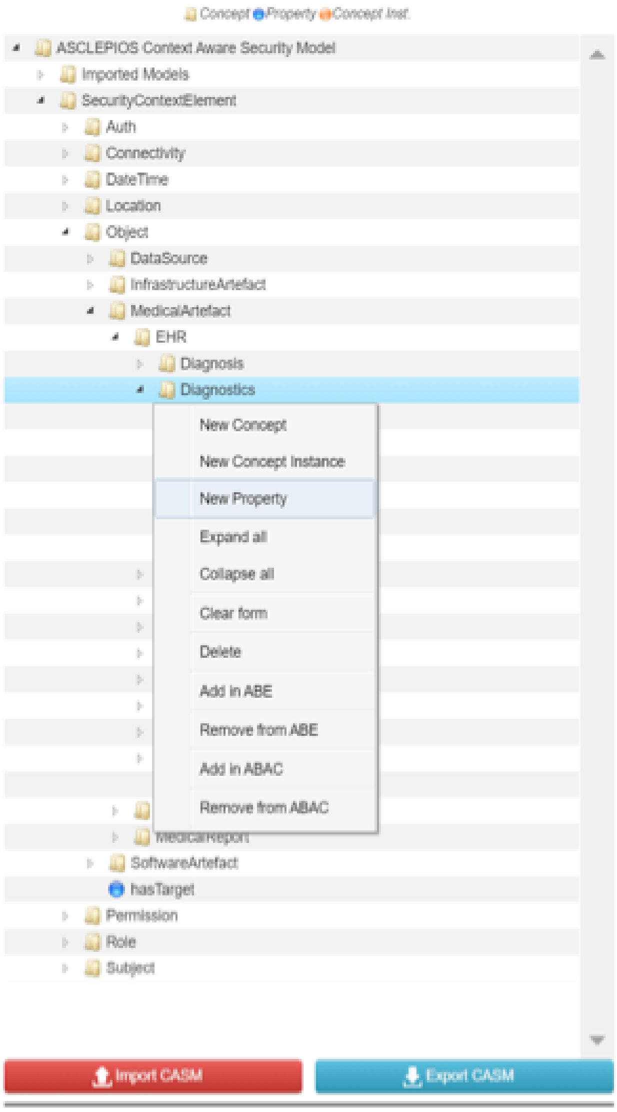


Figure 12. 33 Attribute creation for class "Diagnostics"

In Table 12.1 details of a sub-tree of CASM are provided concerning the hierarchical structure of class "Diagnostics". This class, which represents the practice or techniques of diagnosis, is a subclass of "EHR" and encompasses two child classes which bear the names "Medical Imaging" and "Laboratory Result" accordingly.

Table 12. 1 A partial view of CASM describing the class Diagnostics and its child classes

Class Path (Hierarchically)	Class Description
Object	This class refers to any kind of artefact that should be protected based on their sensitivity levels. These artefacts may refer to relational or other databases, files, software artefacts that manage sensitive data or even infrastructure artefacts used.
Object/MedicalArtefact	This class refers to any medical sensitive data entities stored in schema-based or schema-less databases that should be protected from unauthorised access.

Object/MedicalArtefact/ EHR	This class represents the patient’s Electronic Health Records (EHR). EHR represents a digital collection of medical information about a person. It includes information about a patient’s health history, such as diagnoses, medicines received, tests, allergies, immunizations, and treatment plans.
Object/MedicalArtefact/ EHR/Diagnostics	This is a subclass of EHR and represents the practice or techniques of diagnosis. It involves a number of subclasses and properties that help formally describe the means used for examining a patient.
Object/MedicalArtefact/ EHR/Diagnostics/ MedicalImaging	This is a subclass of Diagnostics and refers to the process of producing a digital image of any part of the human body based on radiographic techniques.
Object/MedicalArtefact/ EHR/Diagnostics/ LaboratoryResult	This is a subclass of Diagnostics and refers to the part of patients’ records that present the result of any diagnostic test performed in a laboratory e.g. result of blood group test.

Apart from a graphical user interface, CASM Editor encompasses a REST API controller for providing its functionality through REST calls. CASM Editor stores CASM changes in Models Store as RDF triples. The following listing provides a sample excerpt from a CASM export in RDF/TTL format.

Table 12. 2 Sample attribute export

```
# Definition of class: EHR
<http://www.asclepios.eu/casm/ASCLEPIOS-OBJECT#1371e7a1-def9-4d84-a65e-
↙2d3060f4d97d>
        a       <http://www.asclepios.eu/casm#ASCLEPIOS-
                 OBJECT> ;
        <http://purl.org/dc/elements/1.1/type> "CONCEPT" ;
        <http://purl.org/dc/terms/URI>
                ascm:1371e7a1-def9-4d84-a65e-2d3060f4d97d" ;
        <http://purl.org/dc/terms/created>
                "2019-12-18T19:40:55.933Z"^^
                   <http://www.w3.org/2001/ ↙
                   XMLSchema#dateTime> ;
        <http://purl.org/dc/terms/description>
                 "This class represents the patient’s
                   Electronic Health Records (EHR). EHR
                   represents a digital collection of medical
                   information about a person. It includes
                   information about a patient’s health
                   history, such as diagnoses, medicines
                   received, tests, allergies,
                   immunizations, and treatment plans." ;
        <http://purl.org/dc/terms/identifier>
               "1371e7a1-def9-4d84-a65e-2d3060f4d97d"
        <http://purl.org/dc/terms/modified>
               "2019-12-18T19:40:55.933Z"^^
                   <http://www.w3.org/2001/ ↙
                   XMLSchema#dateTime> ;
        <http://purl.org/dc/terms/title>   "EHR" ;
        <http://www.asclepios.eu/casm/types#class>
               "eu.asclepios.ample.model.SchemaObject" ;
        <http://www.w3.org/2004/02/skos/core#broader>
                 <http://www.asclepios.eu/casm/ASCLEPIOS
                 -OBJECT# ↙
                 aa205d7c-dba9-45d2-955a-d0ed0167de74> .
```

Discussion

The development of the AMPLE editor provides a valuable tool to EHR systems' administrators and data protection officers to manage the background knowledge required for creating and enforcing access control policies for electronic health records. Since it enables concepts and properties editing to tailor a context-aware security model, these capabilities can set the basis for also validating any aspect of the access control policies that are to be enforced.

Policy validations are required to verify that all the designed access control policies for an EHR system meet certain requirements imposed by legislation or corporate guidelines to reach a minimum level of quality. They can be performed when developing the authorization polices or just before putting them into effect. We highlight with an example the value of offering a complete editing mechanism that will have the ability to validate any designed ABAC and ABE policies.

Consider the need to enforce a high-level constraint to completely restrict the access to any aspects of EHRs that belong to children, if there isn't available first the parents' consent. Also in this example, let the system administrator create only one ABAC policy that combines the following two rules presented in Table 12.3.

Table 12. 3 Example ABAC Policy Rules

Rule 1:
IF (user-classification="Emergency radiology") AND (user-action="READ") AND (resource isA "Laboratory Result")
THEN permit

Rule 2:
IF (user-role="physician") AND (user-action="READ") AND
(patient hasAge < 12) AND (LegalGuardianConsent = “true”) AND (resource isA "Medical Imaging")
THEN permit

Through the AMPLE’s GUI, it becomes evident that the class EHR which represents a digital collection of medical information about a person has several subclasses among which the Laboratory Result and Medical Imaging classes, since these are subclasses of the Diagnostics, a class with parent the EHR class. Therefore, it becomes clear both graphically but also through inferencing that the above policy does not abide to the high-level restriction required in this example, as there is a rule that permits access to one of the EHR aspects (i.e. Laboratory Result) without examining if the patient is a child and if there the appropriate consent has been acquired.

3) ***Validation/Evaluation***

Overall, this chapter introduces the following:

i. It proposes a Context–aware Security Model, as analytically described in (c2). The proposed context model i) formally describes classes and properties with respect to: associations between types of access to sensitive data and situations under which this access should be permitted, and ii) matches policies between private keys and ciphertexts for permitting decryption of sensitive data. Moreover, this model constitutes the necessary background knowledge layer for enabling the ABAC and ABE paradigms by incorporating policies that can be used with ABE schemes, based on the specific needs of healthcare organizations. Finally, we extended the PaaSword security model in order to cope with concepts, challenges and standards from the healthcare domain. This particular context model is used in the Context-aware Model Editor and Policy Editor, as analytically presented in (c3).

ii. It proposes a Context-aware Security Model Editor and Policy Editor, as analytically presented in (c3). This work presented AMPLE, a tool with editing functionalities providing the ability to update or improve, according to the adopter’s needs, our security context-aware model which is used as a common vocabulary for devising access control policies. AMPLE can be used to define access control policies, which can be enforced as part of the ABAC and ABE policy methods. AMPLE yields simultaneously the following unique points: i) offers a visually appealing interface, ii) is open source, iii) provides attributes vocabulary (no typos, or misconceptions on the meaning), iv) offers expression representation, v) offers a web-based application, and vi) provides graphical expressions.

C. Cross-Organizational Access Control

1) Methods and Tools

a) Electronic Medical Records during Acute Care

This section introduces stakeholders of an acute care EMR system and their roles in the ABAC paradigm. We specifically consider the situation when a patient is treated in an Emergency Session (ES), covering the time window since the patient requests emergency treatment until discharge.

We describe the acute stroke care case involving professionals from the emergency call centre, ambulance services and hospitals. The professionals with different roles are organised in teams in each organisation. The time interval in which the teams participate in the patient's ES is the team's Episode of Care (EC), according to FHIR standard concept (FHIR). An EC starts when a team is invited to the ES, and it ends when a team finishes the treatment. After that, access to the data is revoked. During the EC, the team members can read and update the patient's EMR. Bellow, we describe the EC for the call centre team, ambulance team and hospital team.

- **Call centre team**. An emergency call centre professional receives a call from someone on behalf of the patient. During the phone call, the professional follows a triage protocol and needs to read the patient's EMR and add new information about its current condition. The phone call event is the beginning of the patient's ES. Suppose now that the professional decides for requesting an ambulance acute care team to pick up the patient. The ambulance team that accepted the request then also becomes involved in the patient's ES. In another scenario, the patient might use private transportation, so the acute care team designated to treat the patient at the hospital also takes part in the patient's ES. In both cases, as soon as the patient is under treatment of one of the acute care teams, the call centre professional leaves the ES and should no longer have access to the patient's EMR.

- **Ambulance team**. Ambulance acute care team professionals must have access to a patient's EMR between the emergency request until the patient's delivery at the hospital. First, the ambulance professionals notify the EMR system that the patient was picked up. Then, following the triage, the ambulance team requests an adequate hospital to receive the patient. After request and acceptance of the hospital, the ambulance starts the transportation. Finally, after delivering the patient to the hospital, the ambulance professionals have extra time to complete data into the patient's EMR.
- **Hospital team**. As soon as the hospital team is involved in the patient's ES, its members should read the patient's EMR to better prepare for the treatment. During the treatment, the acute care team can add new records to the patient's EMR. In the case of transfer to another hospital, a second ambulance and hospital teams become involved in the ES and access the patient's EMR. The ES and the ability to read the patient's EMR terminate when the patient is transferred or discharged. However, the team members should have extra time to complete the treatment record after the ES is over.

Figure 12.34 illustrates an ES with episodes of care by the call centre, ambulance and hospital teams. For each team, the figure presents the starting and ending time of their involvement in the ES. It also shows when a team invites another team to join the ES.

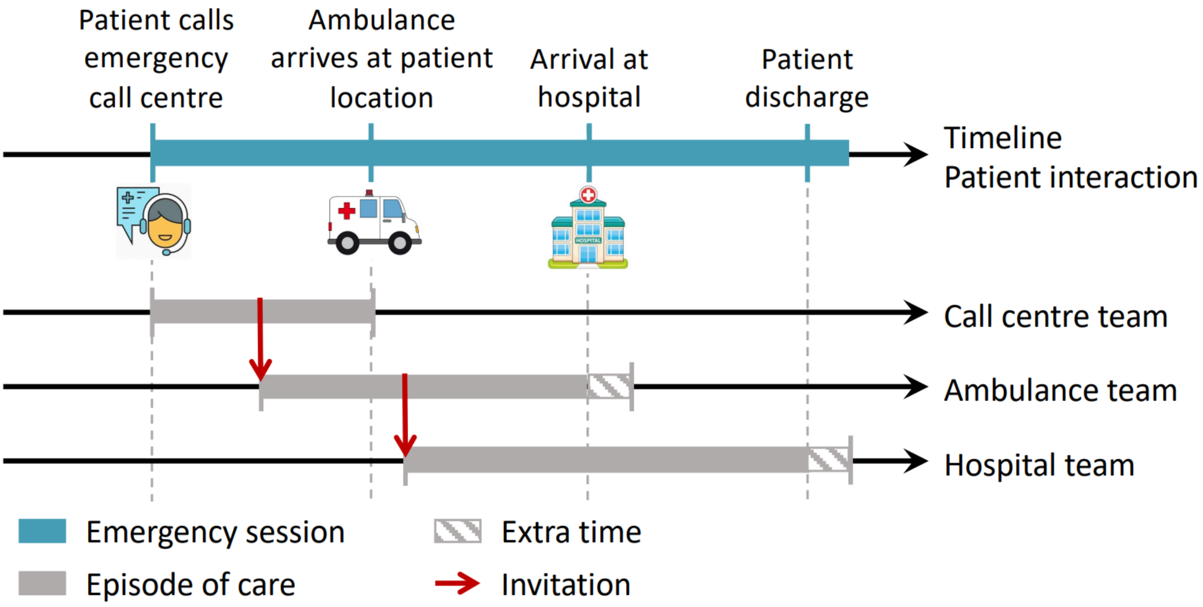


Figure 12. 34 Emergency session and timeline of teams interaction with the patient's EMR.

Note that each team member's data processing actions must be recorded into the audit logs at the user level, as this creates full responsibility for the user and his actions undertaken during an emergency.

b) *Attribute-Based Access Control for Electronic Medical Records*

ABAC defines an access control paradigm by which access rights are granted to the requester by using policies that consist of logical combinations of contextual attributes. Figure 12.35 presents the main architecture entities and their direct communication flow following the ABAC model's reference implementation using the eXtensible Access Control Markup Language (OASIS, a). XACML is an OASIS (OASIS, b) standard that describes both a policy language and an access control decision request/response language. Both languages use XSD (XSD) notations; hence, policy definition and request/response elements are serialised as XML elements. The standard defines five main components that handle access decisions, namely Policy Enforcement Point (PEP), Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Information Point (PIP), and a Context Handler. In our previous work, we extended this reference implementation by providing the appropriate integration hooks to external systems to facilitate integration. We also presented a policy editing component named ASCLEPIOS Models and PoLicies Editor (AMPLE) (c3 as analytically presented in Chapter 12.2) for managing policies and multiple context handlers of different complexity.

Our system includes the architectural components depicted in Figure 12.35 and briefly described below.

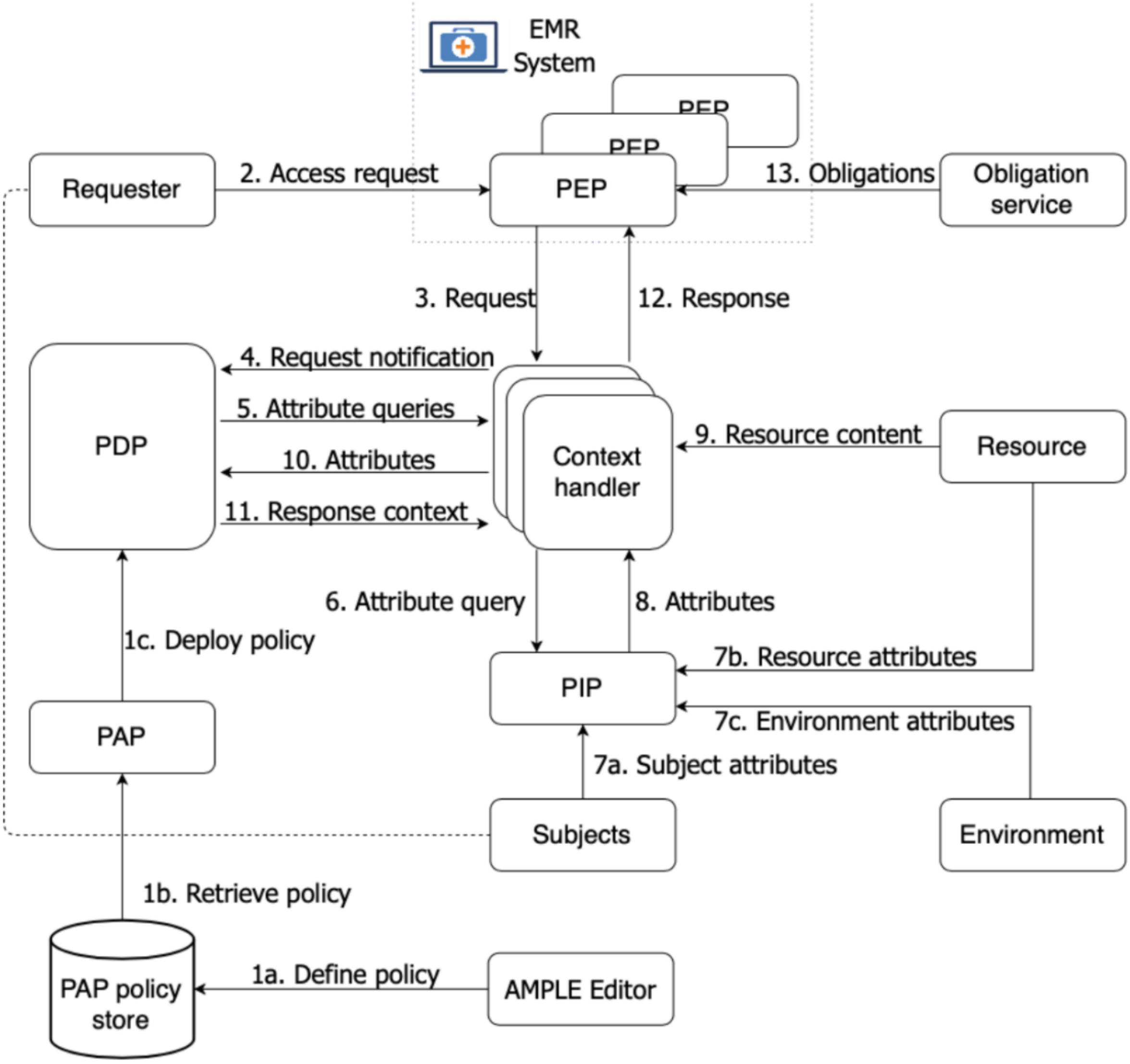


Figure 12. 35 Context-Aware Attribute-based Access Control System architecture and communication flow

- **Electronic Medical Records (EMR) system** is a web system responsible for the management and storing of the encrypted EMR and respective cryptography keys. Moreover, the EMR system offers the data persistence layer and the services to process data, e.g. create, read, update and delete (CRUD), controlled through PEPs.

- **Subjects** refer to any entity that can interact with the EMR system to request data access. A subject has one or more attributes for characterisation in the system. We consider two different types of subjects: patients and healthcare professionals.
- **Resource** is a data, service or system component that needs to be protected through access control. Each resource offers specific actions that require data processing. A request action refers to the subjects' intended action (e.g. read or update) over a specific resource. For example, the patient data in the EMR system are represented in encrypted form as resources protected through ABAC. Also, the respective cryptography keys could be managed by the EMR system and protected with ABAC.
- **Environment elements** provide contextual information of the requester or resource. This information can come from the access requester, such as the timestamp, IP address and geolocation, or from external smart devices.
- **A Requester** embodies the user application. The subject sends access requests through the user application to process any resource of the EMR system.
- **The AMPLE editor** is a graphical web tool that allows the data controller to create, persist and update XACML-based access control policies. These policies are context-aware because they imply evaluating the contextual attributes of subjects, resources, action and the environment before yielding a permit or deny decision.
- **The Policy Administration Point (PAP)** stores a database used for persisting policies and access request decisions. The PAP provides access to the pool of defined policies that have been deployed and activated through the AMPLE editor. Nevertheless, these policies may have static or dynamic parameters that can be updated even at run-time to be immediately enforced.
- **The Policy Enforcement Point (PEP)** constitutes the integration hook to any external system such as an EMR system. It manages and serves incoming access requests for processing the patient's EMR. Different PEPs may be used in various sub-components of the EMR system, or they can be appended to the application server used (e.g., Tomcat). A PEP can receive access requests and freeze the

execution workflow until a decision is yielded. At the same time, it propagates the requests and attributes to the ABAC system's decision-making components.

- **The Policy Decision Point (PDP)** is the core decision place for any incoming access request intercepted by a dedicated PEP. It collects all the necessary contextual information and yields an access control decision, permit or deny, according to the defined policies.
- **The Policy Information Point (PIP)** is responsible for retrieving the necessary attributes for the policy evaluation from several external or internal entities. The attributes aggregated to the PIP may be retrieved from the resource to be accessed (partial or complete EMR), the environment, subjects and the intended action. The attribute values refer mainly to raw information.
- **Context Handlers** are responsible for semantically uplifting the raw information received by a PIP and producing the appropriate level of contextual information for the policies. Thus, they enable the aggregation of dynamic attributes to context-aware policies.
- **The Obligation service** is a directive from the PDP to the PEP on what must be carried out before or after the access request is approved. If the PEP is unable to comply with the directive, even the approved access request must not be realised. The augmentation of obligations eliminates the gap between formal requirements and policy enforcement. An example of an obligation could be sending the ”purpose of access” declaration for all types of access requests. If the PEP does not receive a valid value, the directive does not comply, and the access request is denied.

Note that the Context-Aware ABAC integrated with the EMR system can dynamically digest new policies at run-time. This means that, upon proper authentication, the PAP storage can be updated with new policies to be enforced, and the mapping of context handlers for inferring the context attribute values can be changed on the fly without interfering with the current policies in the system.

c) Methodology for Dynamic and Fine-Grained Access Control Mechanism

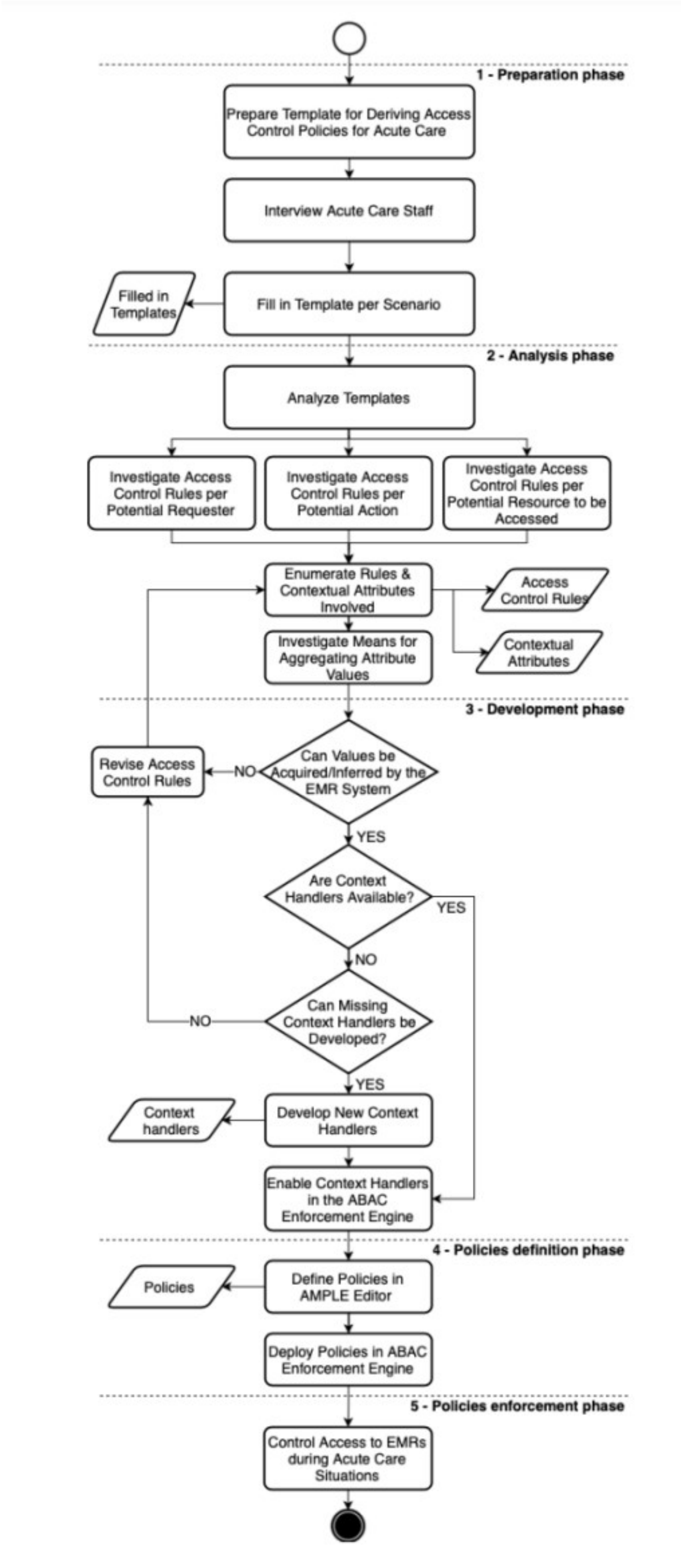
This section proposes a methodology that leverages a fine-grained access control mechanism to the patient's EMR based on the ABAC paradigm. Figure 12.36 depicts the methodology phases described below, namely Preparation, Analysis, Development, Policies definition and Policies enforcement.

In the Preparation phase, we prepare a template to register access control policies and the respective stakeholders for each use case scenario. The template can be found on supplemental material and involves a short description of the objectives and resources that must be protected. Moreover, it provides the placeholders for expressing context-driven access control rules through its tabular format, i.e., to list the requester, action, resource, environment, logical operators that combine rules and the desired access control decision. During the interview with each stakeholder, we fill the template with all the relevant emergency procedures specified concerning the need to access the EMR. Thus, the template constitutes the base for extracting the appropriate contextual information that should bind the access control decisions (i.e., the ABAC policies).

The Analysis phase involves analysing the filled templates by investigating the required access control rules from the requester, the intended actions, and the resources to be accessed. The purpose is to enumerate the rules that must be used along with the contextual attributes considered per rule. Thus, a significant part of the analysis phase involves determining whether the contextual information needed for access control can be acquired or inferred from the EMR system. The selection of the appropriate contextual attributes is of critical importance for defining dynamic access control policies. In our previous work, we have defined CASM (c2), as presented analytically in Chapter 12.2, an ontology that serves as a basis for creating ABAC policies. That ontology is used here to map the contextual attributes involved in access control policies. For a specific policy to be enforced on an incoming access request, the system needs to acquire values for the contextual attributes involved, which happens through context handlers.

The Development phase refers to dedicated software (i.e., context handlers) that can leverage raw data to semantically enriched information. If the contextual attributes cannot be acquired or inferred, then the access control rules are revised.

Any missing context handlers should be developed and enabled before using the corresponding context to access control policies.



1 - Preparation phase
Prepare Template for Deriving Access Control Policies for Acute Care
Interview Acute Care Staff
Fill in Template per Scenario
Filled in Templates
2 - Analysis phase
Analyze Templates
Investigate Access Control Rules per Potential Requester
Investigate Access Control Rules per Potential Action
Investigate Access Control Rules per Potential Resource to be Accessed
Enumerate Rules & Contextual Attributes Involved
Access Control Rules
Contextual Attributes
Investigate Means for Aggregating Attribute Values
3 - Development phase
Can Values be Acquired/Inferred by the EMR System
NO
Revise Access Control Rules
YES
Are Context Handlers Available?
YES
NO
Can Missing Context Handlers be Developed?
NO
YES
Develop New Context Handlers
Context handlers
Enable Context Handlers in the ABAC Enforcement Engine
4 - Policies definition phase
Define Policies in AMPLE Editor
Policies
Deploy Policies in ABAC Enforcement Engine
5 - Policies enforcement phase
Control Access to EMRs during Acute Care Situations

Figure 12. 36 Methodology for defining context-aware ABAC policies

During the Policies definition phase, the data controller of the EMR system defines the context-aware policies using the AMPLE policy editor. Through AMPLE, the policies are defined based on context-aware rules and then they are serialised in XACML, which is an appropriate format for enforcement. The Policies enforcement phase is activated once the policies expressed in XACML are deployed in a dedicated ABAC engine. The ABAC enforcement engine retrieves all the related contextual attributes, infers the missing ones by invoking the relevant context handlers and yields a permit or deny decision according to the policies evaluation.

d) Attribute-Based Access Control Modelling for Acute Care

This section describes the Acute Care Attribute-Based Access Control (AC-ABAC) modelling resulted from applying the proposed methodology. Furthermore, AC-ABAC follows the GDPR requirement for data confidentiality and privacy. According to Art.6 of the GDPR - ”Lawfulness of processing: Processing shall be lawful only if and to the extent that at least one of the following applies: ...d) processing is necessary in order to protect the vital interests of the data subject or of another natural person”. Therefore, Art. 6 imposes that data access during acute care must be granted for those professionals involved in the treatment, and only during the treatment, and then revoked when the treatment is over.

AC-ABAC protects any resource that makes the electronic medical records available for the acute care teams. For instance, the resource could be the patients’ encrypted records and the respective cryptographic keys. We believe that a cryptography scheme combined with dynamic access control would provide medical systems with the confidentiality and data privacy required. The implementation of such encryption protocols is no trivial matter, which others have explained (Michalas, 2019). For simplicity, we kept the cryptographic part out of the scope of this paper so that we focus on the access control modelling.

AC-ABAC consists of policies and contextual attributes definitions for cop ing with dynamic and efficient access control needed in acute care situations. Note that policies considering professionals’ roles, IP address, and secure connection are essential and have been explored in previous research (c3, as presented analytically in Chapter 12.2). Our focus here is to legitimate access to patient data during an emergency session for the acute care teams involved in the patient treatment. In addition, we consider the interaction between the professionals and teams from multiple organisations as an anchor of trust for access control modelling. The results are presented following each phase of the methodology (see Figure 12.36).

Preparation phase

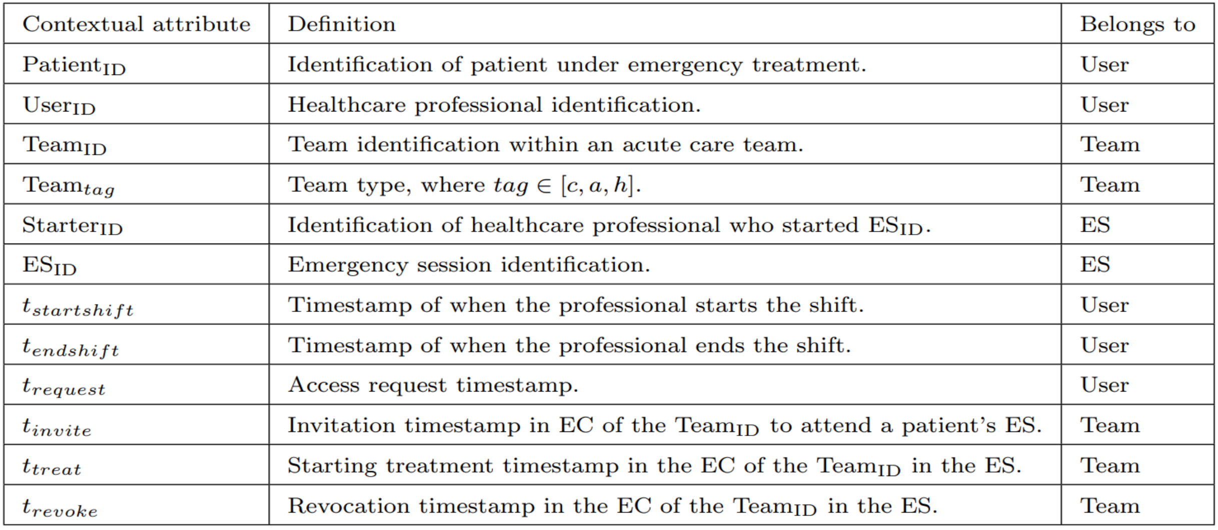
We interviewed professionals from the Amsterdam UMC hospital that work close to the call centre and ambulance service. The template was filled to collect information regarding subjects, actions, resources, and contextual attributes (see also [14]). For members of call centre, ambulance and hospital teams, we listed an entry in the template for reading and updating the patient EMR. Then, we determine the immutable and dynamics attributes related to each type of subject, action and resource, and the respective expected outcome (permit or deny).

Analysis phase

We observed that the subjects are the active healthcare professionals in the acute care teams involved in the patient's ES. Therefore, the resource should be the patient EMR, and the actions should be limited according to the involvement of teams during the treatment timeline. Healthcare professionals should be able to read the EMR as soon as they are involved in the ES. Still, they only should be able to write data on the EMR after they start treating the patient. An exception is the call centre professional, who interacts with the patient by phone and can read and update data since the beginning of the call. Moreover, after the treatment is over, the professionals involved should have extra time to add new data about the recent EC. Every EC in the ES is limited by a timeout value that varies according to the acute care team type.

The combination of contextual attributes legitimates the patient's ES. These characterise the patient, the healthcare professionals, the acute care team involved in the ES and the duration time of each team's EC on the ES. Table 12.4 lists the contextual attributes that are dynamically assigned to professionals and acute care teams during the ES. StarterID is the member of the first team who creates the ESID and associates it to the PatientID. Every team has a Teamtag, where tag characterises the different types of teams for call centre (c), ambulance (a) and hospital (h). Every team member can request access to read or update data on the patient EMR and invite another team to participate in the ES. However, only Teamc and Teamh can start an ES, only Teama and Teamh can have extra time to update after revoke time, and only Teamh can discharge patient.

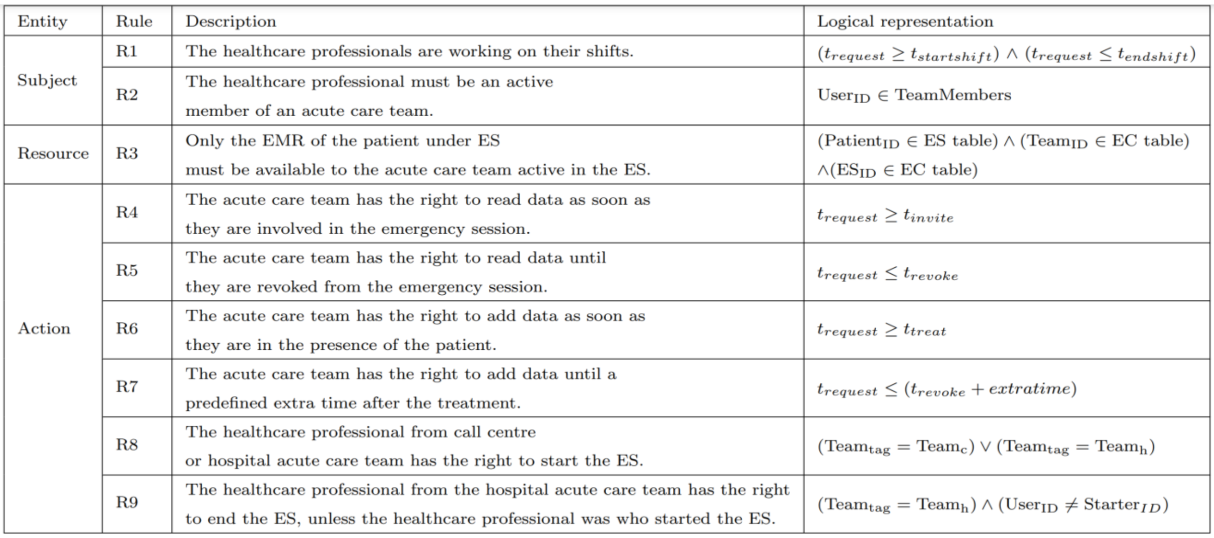
Table 12. 4 Contextual attributes, definitions and the subject of the attribute.



Contextual attribute	Definition	Belongs to
$\text{Patient}_{\text{ID}}$	Identification of patient under emergency treatment.	User
User_{ID}	Healthcare professional identification.	User
Team_{ID}	Team identification within an acute care team.	Team
Team_{tag}	Team type, where $tag \in [c, a, h]$.	Team
$\text{Starter}_{\text{ID}}$	Identification of healthcare professional who started ES_{ID}.	ES
ES_{ID}	Emergency session identification.	ES
$t_{startshift}$	Timestamp of when the professional starts the shift.	User
$t_{endshift}$	Timestamp of when the professional ends the shift.	User
$t_{request}$	Access request timestamp.	User
t_{invite}	Invitation timestamp in EC of the Team_{ID} to attend a patient's ES.	Team
t_{treat}	Starting treatment timestamp in the EC of the Team_{ID} in the ES.	Team
t_{revoke}	Revocation timestamp in the EC of the Team_{ID} in the ES.	Team

Table 12.5 enumerates the rules and contextual attributes values involved per entity. The request for reading or updating data must contain the following attributes: trequest, requester UserID, TeamID and PatientID. When a healthcare professional joins a team, it is created an entry in the TeamMembers table, which contains the TeamID and the UserID of the professional. When an ES is started, it creates an entry in the ES table with the PatientID and the StarterID. When a team joins an ES, it is created an entry in the EC table with the TeamID that is responsible of the episode and the ESID that it belongs to. Moreover, each entry on the EC table contains the t_request, t_invite, t_treat and t_revoke attributes describing the team participation timeline in the ES. These attributes are evaluated according to these tables and the contextual attributes defined on Table 12.4.

Table 12. 5 Modelling rules, request's attributes and contextual attributes involved for each entity.



Entity	Rule	Description	Logical representation
Subject	R1	The healthcare professionals are working on their shifts.	$(t_{request} \geq t_{startshift}) \wedge (t_{request} \leq t_{endshift})$
	R2	The healthcare professional must be an active member of an acute care team.	$\text{User}_{\text{ID}} \in \text{TeamMembers}$
Resource	R3	Only the EMR of the patient under ES must be available to the acute care team active in the ES.	$(\text{Patient}_{\text{ID}} \in \text{ES table}) \wedge (\text{Team}_{\text{ID}} \in \text{EC table})$ $\wedge(\text{ES}_{\text{ID}} \in \text{EC table})$
Action	R4	The acute care team has the right to read data as soon as they are involved in the emergency session.	$t_{request} \geq t_{invite}$
	R5	The acute care team has the right to read data until they are revoked from the emergency session.	$t_{request} \leq t_{revoke}$
	R6	The acute care team has the right to add data as soon as they are in the presence of the patient.	$t_{request} \geq t_{treat}$
	R7	The acute care team has the right to add data until a predefined extra time after the treatment.	$t_{request} \leq (t_{revoke} + extratime)$
	R8	The healthcare professional from call centre or hospital acute care team has the right to start the ES.	$(\text{Team}_{\text{tag}} = \text{Team}_{\text{c}}) \vee (\text{Team}_{\text{tag}} = \text{Team}_{\text{h}})$
	R9	The healthcare professional from the hospital acute care team has the right to end the ES, unless the healthcare professional was who started the ES.	$(\text{Team}_{\text{tag}} = \text{Team}_{\text{h}}) \wedge (\text{User}_{\text{ID}} \neq \text{Starter}_{ID})$

Development phase

Following the steps in phase 2, Figure 12.36, we investigated means to aggregate the contextual attribute values through context handlers. The context handlers must be able to dynamically either infer the attribute values from the request or acquire them from the environment. Following the methodology, we have developed the necessary context handlers to aggregate each contextual attribute from PIP since none were available. Note that user interactions with the EMR System aggregate the specific contextual attributes listed in Table 12.4. After an action is taken, the contextual attributes' values are created or updated in the PIP, often by the EMR System. Therefore, during policy evaluation, the context handlers acquire the contextual attribute values from the PIP.

The following actions trigger the changes in the PIP: When the healthcare professional starts and ends the work shift, it creates t_startshif t and t_endshift. When the organisation's administrators manage teams by adding or removing members, the PIP updates the teams, indexing with TeamID in the TeamMembers table. The ES attributes and the involved teams are updated when the teams act on the EMR System. For example, when Starter_ID initiates the ES, it creates an entry on the ES table with ES_ID, and also associates the Patient_ID and Starter_ID, so that all information about the ES becomes available on the PIP through the appropriate context handler. Every team that participates in the ES has an EC that starts with tinvite, has ttreat and ends with trevoke. The 'previous' and 'next' teams are coined regarding the acute care timeline. For example, when the ambulance picks up the patient, it may revoke access to the previous team, which is probably the call centre.

The PIP is responsible for engaging the appropriate context handlers to aggregate the relevant contextual attributes values. This is performed based on Patient_ID, which indexes the resource EMR. From the Patient_ID, the PIP can retrieve the active patient's ES_ID, teams involved in the ES and their timestamps, and members of each team. After acquiring the contextual attributes' values, the context handler sends them to the PDP for policy evaluation.

Policies definition phase

Following the steps in phase 4, Figure 12.36, we created policies based on the rules expressed in Table 12.5 to protect against non-legitimate requests for accessing the patient's EMR. Table 12.6 summarises the policies created to read and update the patient EMR and authorise the start and end of an ES. The rules combination algorithm of each policy is defined as PERMIT unless DENY, which means that if any rule yields a DENY, the policy outcome decision will be denied. Figure 12.37 represents the hierarchy of the rules on a policies decision tree.

We used AMPLE to create the rules and define the policies. Moreover, we manually defined the dynamic parameters that the context handlers use to evaluate each rule since APAM does not support this definition yet, where we create rules that both sides of the equation are parameters that the values of the contextual attributes will replace. This is obtained as follows. Consider a rule t_request ≥ X, where X represents a dynamic value. The context handler will replace the parameter X for the contextual attribute value of some context value, for example, tinvite, which can be acquired from the PIP. Therefore, the dynamism of the access policy is introduced by design. The rule does not involve any static values since this can only be known and enforced at run-time.

Table 12. 6 Policy is a combination of enumerated rules according to the requested action (see Table 12.5)

Action	Policy
Read	R1 ^ R2 ^ R3 ^ R4 ^ R5
Update	R1 ^ R2 ^ R3 ^ R6 ^ R7
Start ES	R1 ^ R2 ^ R8
End ES	R1 ^ R2 ^ R3 ^ R6 ^ R9

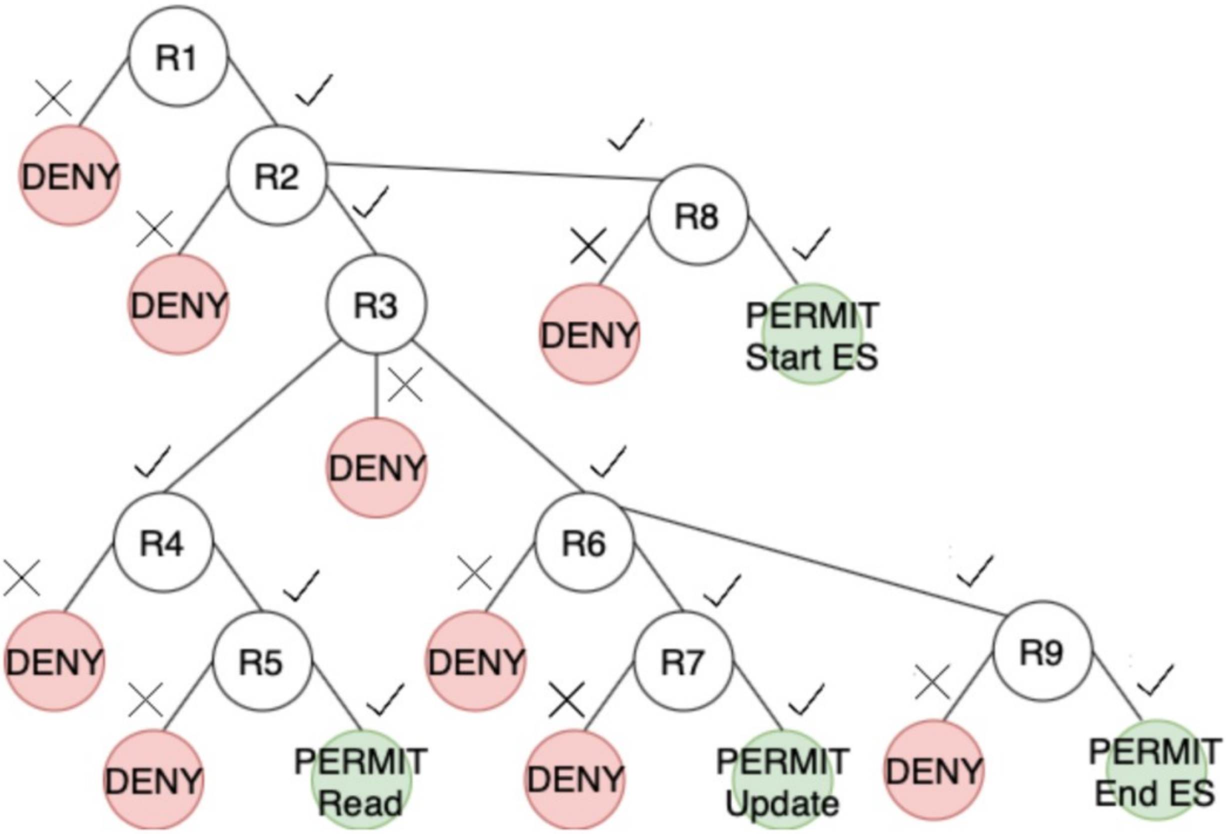


Figure 12. 37 Policies decision tree

Policies enforcement phase

Following the steps in phase 5, Figure 12.36, we deployed the PDP policies and added the PEP to the EMR System. After receiving the required contextual attributes and the policy evaluation, the PDP yields a decision to the context handler: PERMIT or DENY. The context handler then notifies the PEP about the decision, and – if it is a PERMIT – the PEP allows the data access request on the EMR System.

2) <u>***Evaluation/Validation***</u>

a) Implementation and evaluation

In this section, we present the implementation of a prototype and the evaluation of the policies. First, we present the acute care information workflow of the AC-ABAC model. Then, through simulations, we validate the defined policies' correctness and analyse the request evaluation performance in different scenarios.

The prototype includes Contextual-Aware ABAC deployment presented in Figure 12.35, a web application simulating the EMR system to be protected and a custom database that serves as PIP with a REST-API. The EMR system simulation is a web application with available endpoints that allows read, update, start ES and end ES requests. The PIP contains the attributes values that are aggregated from the EMR System. However, in this prototype, we populated the PIP database to generate attribute values from simulated interactions between users and the EMR System under emergency. The context handler uses the REST-API to retrieve and process the contextual attributes stored on the PIP. Both web application and the PIP's REST-API were developed with the Django Framework [15].

Regarding ABAC, the open-source WSO2 Balana engine (Balana) was used as an implementation of the XACML access control. The context handlers were developed and connected to the PIP and enabled in the ABAC Enforcement Engine. With all ABAC components set up, the PEP is invoked whenever an incoming access request to a protected resource is detected, and the evaluation process begins. The Docker image of the prototype, the defined policies and context handlers of the AC-ABAC model, and the results of the experiments can be found on Github [16].

Acute care information workflow

Here we describe the acute care information workflow used in the AC-ABAC model. Guided by the methodology, we understood when and which information we infer during the acute care workflow. Figure 12.38 presents a ES flow where the call centre team starts the ES and invites an ambulance team, the ambulance team invites a hospital team, and the hospital team ends the ES. Each team has a starting point that represents the moment where the team entries the ES. The acute care teams interact with the ABAC engine to obtain access rights, and a team member notifies the EMR system about the events on the patient's ES. The access permissions are granted for the teams during a period of time and are updated according to the subsequent events on the patient's ES. Leave ES represents when an EC of the team ends, while an End ES represents the end of the entire ES. The use case can be extended to support more teams participating in the ES, for example, when the patient needs ambulance transfer to a second hospital.

Table 12. 7 Description of each scenario tested in the experiments.

Scenarios	Description
S1	A team member in the ES requests to read the EMR when $t_{invite} \leq t_{request} \leq t_{treat}$
S2	A team member in the ES requests to read the EMR when $t_{treat} \leq t_{request} \leq t_{revoke}$
S3	A team member in the ES requests to update the EMR when $t_{treat} \leq t_{request} \leq t_{revoke}$
S4	A team member in the ES requests to update the EMR when $t_{revoke} \leq t_{request} \leq (t_{revoke} + extratime)$
S5	A professional is not active on the shift, but is a team member participating in the ES
S6	A professional is active on the shift, but is not currently a team member
S7	A professional is active on the shift and is a team member, but the team is not part of the ES
S8	A professional is active on the shift, is a team member, is part of the ES, but requests to another patient's EMR.
S9	A team member in the ES requests to read the EMR when $t_{request} > t_{revoke}$
S10	A team member in the ES requests to update the EMR when $t_{request} < t_{treat}$
S11	A team member from the ES requests to update the EMR when $t_{request} > (t_{revoke} + extratime)$
S12	A team member from a call centre or hospital team requests to start an ES
S13	A team member from a ambulance team requests to start an ES
S14	A team member from the hospital team requests to end an ES and $\text{User}_{\text{ID}} \neq \text{Starter}_{\text{ID}}$
S15	A team member from the hospital team requests to end an ES and $\text{User}_{\text{ID}} = \text{Starter}_{\text{ID}}$

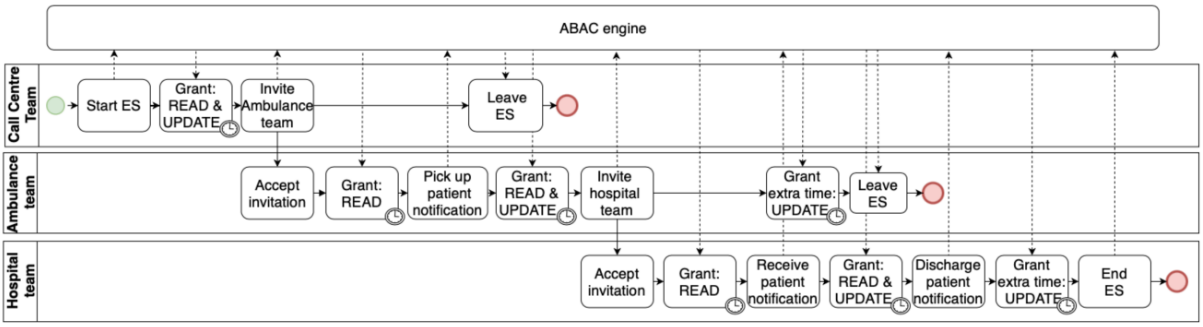


Figure 12. 38 Emergency session flow presented as Business Process Model and Notation (BPMN) diagram. The teams have access rights granted to read and update according to the timeline of events.

Correctness evaluation

This section analysed the correctness of the policies, following satisfiability modulo theories (SMT) using the simulations. This is done by evaluating the policy implementation with a test input (i.e., access request) and validating the corresponding output (i.e., PERMIT or DENY). Regarding the security of the model, the formal security of the XACML standard used in our ABAC model was already proved by [17]

We have simulated legitimate and non-legitimate requests in different scenarios in the prototype to evaluate the policies correctness. Table 12.7 presents the description of fifteen scenarios that were evaluated (S1-15), and their expected and obtained outcomes are summarised in Table 12.8. Some scenarios may be unrealistic because we evaluated each policy's different rules outcomes to demonstrate that the security mechanism works.

Scenarios 1-4 consist of must-be-permitted access requests to the patient's EMR. Scenarios 5-11 are must-be-denied access requests to the patient's EMR. Finally, scenarios 12-15 describe the requests to start and end an ES. Table 12.8 presents the policies per action, as the combination of rules evaluated in each scenario. It also indicates the rules that fail in each of the must-be-denied scenarios. Table 12.8 also presents the outcomes obtained with the simulation, which corresponded to the expected values in all cases.

We acknowledge that false-positive and false-negative results might happen due to race conditions. For example, while the PIP updates the contextual attributes, the evaluation might consider outdated contextual attributes. Note, however, that this hardly occurs since the database updates in a matter of milliseconds.

Performance evaluation

Using our application simulating the EMR system, we implemented a Python script that simulates requests issued by a "Requester" through the application client to the EMR system server. The Context-Aware ABAC prototype intercepts all the requests to the EMR system server and yields a response. Here we assess the performance of the

AC-ABAC model implementation regarding the time needed to evaluate an access request, evaluate the policy, and deliver the response (permit or deny).

Table 12. 8 Policies correctness evaluation in different scenarios. The outcome represents the obtained decision after the policy evaluation.

Scenario	Rules									Action	Outcome
	R1	R2	R3	R4	R5	R6	R7	R8	R9		
S1	✓	✓	✓	✓	✓	-	-	-	-	Read	PERMIT
S2	✓	✓	✓	✓	✓	-	-	-	-	Read	PERMIT
S3	✓	✓	✓	-	-	✓	✓	-	-	Update	PERMIT
S4	✓	✓	✓	-	-	✓	✓	-	-	Update	PERMIT
S5	X	✓	✓	-	-	-	-	-	-	Read & Update	DENY
S6	✓	X	✓	-	-	-	-	-	-	Read & Update	DENY
S7	✓	✓	X	-	-	-	-	-	-	Read & Update	DENY
S8	✓	✓	X	-	-	-	-	-	-	Read & Update	DENY
S9	✓	✓	✓	✓	X	-	-	-	-	Read	DENY
S10	✓	✓	✓	-	-	X	✓	-	-	Update	DENY
S11	✓	✓	✓	-	-	✓	X	-	-	Update	DENY
S12	✓	✓	-	-	-	-	-	✓	-	Start ES	PERMIT
S13	✓	✓	-	-	-	-	-	X	-	Start ES	DENY
S14	✓	✓	✓	-	-	✓	-	-	✓	End ES	PERMIT
S15	✓	✓	✓	-	-	✓	-	-	X	End ES	DENY

The requests implemented the fifteen scenarios presented in Section of Correctness evaluation. Table 12.7 and repeated 100 times. We measured the total time since the PEP received the request until it delivered the response (permit or deny) and the time dedicated inside the PDP for the policies' evaluation. The experiments were executed in a DELL PowerEdge R630 server with Intel Xeon ES-2640 v4 Processor and 256GB of RAM at the cloud of University of Westminster [18].

Figures 12.39 and 12.40 present the results of the performance experiment. Figure 12.39 presents the total time to process the request in each scenario, as well as the portion dedicated to policy evaluation (average and standard deviation calculated over 100 runs). As expected, in grey, the time for evaluating the policy dominates the total request evaluation time. This happens because the time spent inside the PDP includes the waiting time for retrieving the policy from the PAP and the contextual attributes from the context handlers. Each scenario presents a different request evaluation time because they use different policies. Moreover, the policies are defined as ”permit unless denied”, and the rules are evaluated in sequence, as listed in Figure 12.37. So, when one of the rules results in a denial, it stops the execution of the subsequent rules. Note that the scenarios that evaluated the same rules presented similar average request evaluation times (see details in Table 12.8). The exceptions are scenarios S5-S8 and S10, which did not evaluate all the policy rules. In each of these scenarios, a different rule causes the request to be denied, so a different number of rules, and the necessary attributes, are evaluated - this results in different processing times. Figure 12.40 shows how the number of evaluated contextual attributes can affect policy evaluation time. Note that the policy evaluation time increases when more attributes need to be evaluated, as expected. However, the result also shows that the number of attributes is not the only factor affecting policy evaluation time. For example, although in S1 and S3, the number of evaluated attributes is the same (fifteen), policy evaluation takes longer in S1. This indicates that different contextual attributes might require different efforts to be inferred.

Regarding the results, the longest average time to evaluate a request was 194.89 ms for S14 and S15. In both scenarios, the user requests to end an ES, which is the most complex policy of our modelling because its evaluation involves the validation of five rules that combine sixteen contextual attributes. However, start and end ES requests happen only once per patient while reading and updating requests happen more frequently. The average time to evaluate a request to read was 185.82 ms in S1, and 162.36 ms a request to update in S3. We suggest that these times to process such complex requests are acceptable, particularly considering the security improvement added to the system when using more fine-grained and context-aware access control policies. This performance is also acceptable with other security-related delays that may include data encryption and decryption [19]. Finally, the obtained performance is also similar to other ABAC approaches [20].

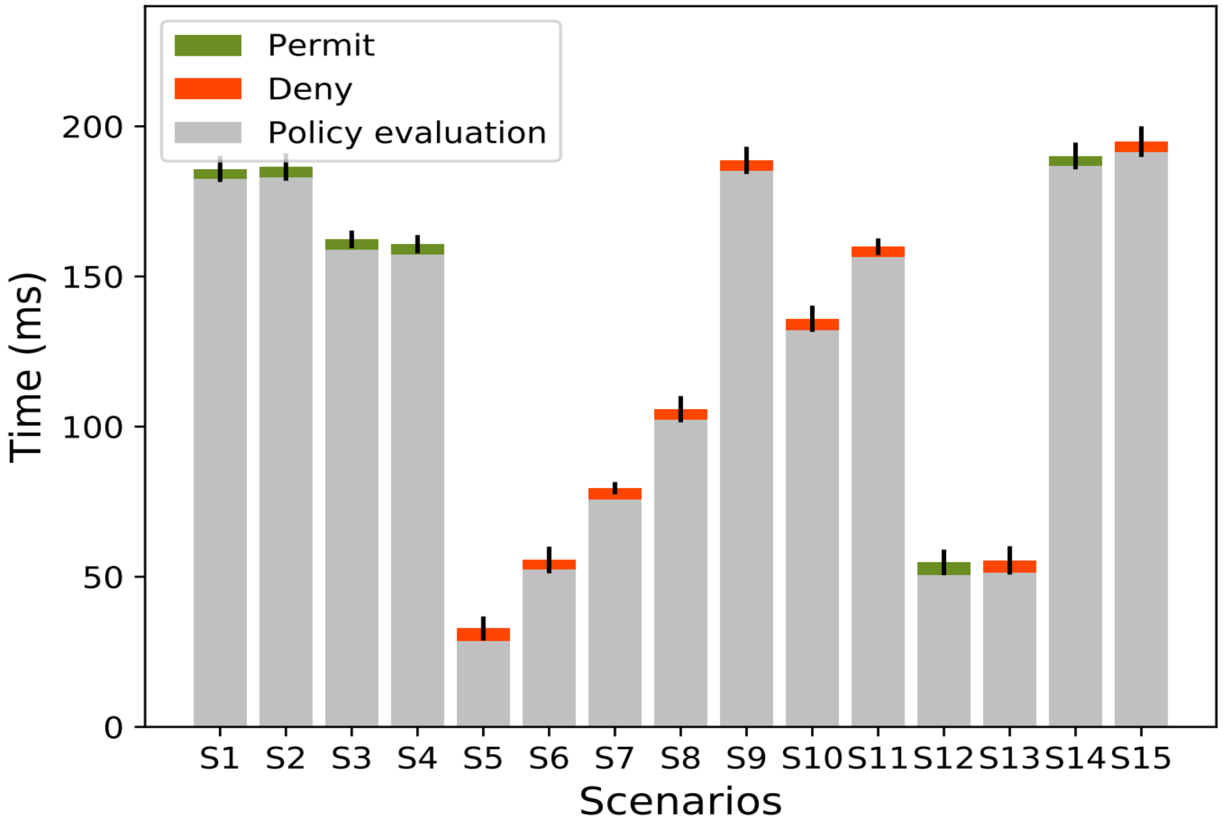


Figure 12. 39 Request and policy evaluation time. Must-be-permit scenarios in green and must-be-deny in red, policy evaluation times in grey.

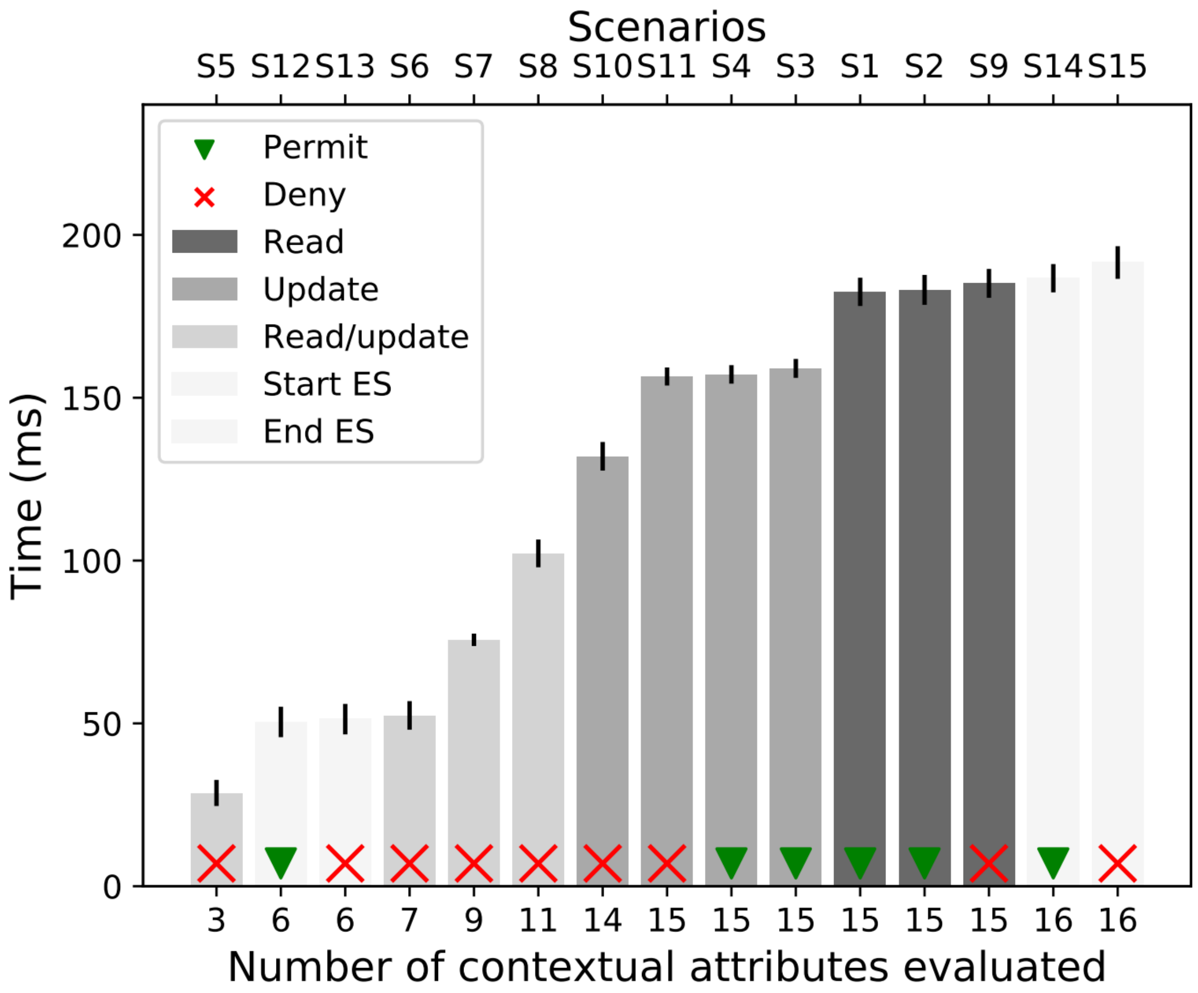


Figure 12. 40 Policy evaluation time per number of attributes evaluated. The policies are differentiated per action.

b) <u>Discussion</u>

We followed the steps needed to understand the access control dynamism required for this acute care application through the proposed methodology. The preparation phase of the methodology facilitated collecting the requirements and understanding the stakeholders in a structured manner imposed by the templates. In the second analysis phase, we had to make a choice of contextual attributes to be used to create the access control policies. To guarantee the availability of a patient's EMR at all times, we decided to leave out contextual attributes regarding location, such as GPS coordinates and IP addresses. The iterative approach adopted in the development phase helped refine realistic rules and contextual attributes. In the policies definition phase, we noticed that the AMPLE editor (c3, as presented analytically in Chapter 12.2) does not define rules with both parameters as contextual attributes. Therefore, to create the rules, we manually modified the XACML rules after creating them on the AMPLE editor. We plan to explore the possibility of direct create dynamic parameters for those rules on the AMPLE editor (c3, as presented analytically in Chapter 12.2) as future work. Finally, during the policies enforcement phase, we observed that race condition regarding outdated security tokens might occur. Such inconsistencies can be minimised by regenerating tokens frequently after modifying the team composition.

Regarding patient identification, AC-ABAC model assumes that the patient is registered beforehand, so there is a Patient_ID. However, it is possible that the patient cannot be found or identified during the emergency (e.g. unconscious patient). In such cases, the EMR system should give a temporary identification (e.g. 'John Doe' or 'Joanna Doe') to the patient so that during the ES, the teams can share the collected information. The proper registration or attribution of the episodes of care can be done after the ES has ended.

Furthermore, we highlight that the defined policies can dynamically change at run-time without any need to re-compile or restart the authorisation engine. For example, imagine that during the COVID-19 pandemic, there was a shortage of ambulances due to many people going to the hospital. In such a case, the paramedic teams of the military forces could provide emergency response. The proposed model could be instantly updated with a policy to add the military teams without compromising the rest of the operational policies in the system.

Regarding the experiment results, the different times found for the request evaluation in the various scenarios indicate that the access control system could be susceptible to timing attacks [21]. In a timing attack, the attacker tries to discover vulnerabilities in the security of a system by studying the variation in its response time to different input parameters. In the case of ABAC, an attacker could analyse the response time according to his attributes and discover which are correct because they lead to a longer response time. Moreover, the attacker could identify the policy by knowing which correct attributes and perform exploitation on the access control. A solution for this is simply to answer all the requests with nearly-constant time.