

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Zafeiroula Georgiopoulou

University of Piraeus



**Systems Security Laboratory
Department of Digital Systems
University of Piraeus**

Ph.D. Thesis

Piraeus, July 2022

Abstract

This thesis deals with cloud computing security in terms of trust, privacy and authentication. In cloud computing environments, successful trust management can compensate the countermeasures that have been adopted for mitigating the security and privacy risks that the cloud comes across. This thesis proposes a trust model that is taking into account specific parameters. These parameters are presented together with a detailed analysis of how, each of them, could be applied/utilized by the trust model for quantifying the trust of the cloud providers to their users. In the context of finding measures to eliminate the risks, the factors that affect the trust of the cloud provider to the users were defined and a corresponding trust model with the respective metrics was developed. The model was simulated in the environment of a university. This thesis also analyzes how a cloud computing service provider will achieve compliance with the General Data Protection Regulation (GDPR) by proposing technical and organizational measures. Furthermore, this thesis is endeavoring to assist organizations to protect the privacy of their users and the security of the data that they store and process. Users may be the customers of the organization (people using the offered services) or the employees (users who operate the systems of the organization). To this direction, a privacy impact assessment (PIA) method, that has been developed with other researchers of the Systems Security Lab, has been adopted for use by the cloud providers supporting them to explicitly take into account the specific organizational characteristics.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Field of Science: Cloud Computing Security

Key Words: Cloud Computing, Trust, Trust Management, Trust Models, Privacy, Trust metrics, GDPR, Privacy principles

Advisory Committee

Costas Lambrinouidakis, Professor (Supervisor) University of Piraeus

Sokratis Katsikas, Professor, Norwegian University of Science and Technology

Christos Xenakis, Professor University of Piraeus

Examination Committee

Costas Lambrinouidakis, Professor (Supervisor) University of Piraeus

Sokratis Katsikas, Professor Norwegian University of Science and Technology

Christos Xenakis, Professor University of Piraeus

Stefanos Gritzalis, Professor University of Piraeus

Maria Karyda, Associate Professor Aegean University

Emmanouil Magkos, Associate Professor Ionian University

Aggeliki Tsoxou, Associate Professor Ionian University

Περίληψη

Η συγκεκριμένη διδακτορική διατριβή πραγματεύεται την ασφάλεια σε επίπεδο εμπιστοσύνης, ιδιωτικότητας και αυθεντικοποίησης σε νεφούπολογιστικά συστήματα. Στο πλαίσιο εύρεσης μέτρων για την εξάλειψη των κινδύνων ορίστηκαν οι παράγοντες που επηρεάζουν την εμπιστοσύνη του νέφους προς το χρήστη και αναπτύχθηκε αντίστοιχο μοντέλο εμπιστοσύνης με τις κατάλληλες μετρικές. Το μοντέλο προσομοιώθηκε στο περιβάλλον ενός πανεπιστημίου. Στο πλαίσιο επίσης της παρούσας διατριβής αναλύθηκε πώς ένας πάροχος υπηρεσιών νεφούπολογιστικού νέφους θα επιτύχει τη συμμόρφωση του με το Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR) προτείνοντας τεχνικά και οργανωτικά μέτρα. Παράλληλα μελετήθηκε μέθοδος και μετρική αποτίμησης ιδιωτικότητας λαμβάνοντας υπόψη την φύση του οργανισμού και την εφαρμογή του GDPR.

Acknowledgements

Costas Lambrinoudakis has been a unique teacher, mentor, and supervisor since the first days I met him around 2009. The initiation, continuation and completion of this effort is all related to his great advice, scientific inspiration, and encouragement with a perfect blend of understanding, insight, and personal interest. I'm proud and grateful for having a very strong relationship with him and hope-believe to continue the same way in the future. He has been a great example for my scientific, professional, and personal steps.

Appreciation also goes to the members of my advisory committee, Professors Sokratis Katsikas and Chris Xenakis for their directions and significant advices for keeping me up with the Ph.d.'s objectives.

Many thanks to my colleague Eleni Laskarina Makri for the fruitful cooperation, fun and interesting discussions all these years.

My family has been another valuable contributor from the first days of this thesis. Their proudness, love, help and encouragement has given me strength and inspiration throughout my research.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

(Signature)

.....

Zafeiroula Georgiopoulou

Ph.D. Thesis, University of Piraeus, Department of Digital Systems.

© 2022 – All rights reserved

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Chapter 1 : Introduction	15
Chapter 2 : Problem Identification	17
2.1 Goals and Contribution.....	17
Chapter 3 : Trust Models in Cloud Computing	19
3.1 Trust in Cloud	19
3.2 Literature Review	20
3.2.1 Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment	20
3.2.2 A Collaborative Trust Model of Firewall-through based on Computing	21
3.2.3 Secure Trust Model Based on Trusted Computing	22
3.2.4 Trust Management system for Grid and Cloud Resources.....	23
3.2.5 SLA-based Trust Model for Cloud Computing.....	24
3.2.6 A Trusted Computing Environment Model in Cloud Architecture	24
3.2.7 Evaluation of Behavioral Security in Cloud Computing	25
3.2.8 Cross-Tenant Trust Models in Cloud Computing	25
3.3 Summary & Comparison of trust computing models.....	26
Chapter 4 : Trust Management Model in Cloud Computing Environments	27
4.1 Introduction	27
4.2 Trust Parameters	27
4.3 Trust Model and Metric.....	29
4.3.1 Overview.....	29
4.3.2 Trusted Access Point	30
4.3.2.1 Data input for Trusted Access Points.....	30
4.3.2.2 Metric of Access Point Trust Value TAP	31
4.3.3 Location	33
4.3.3.1 Data input for Location.....	33
4.3.3.2 Metric of Geo-location Trust Value TL	35
4.3.4 Data Access	35
4.3.4.1 Data input for Data Access	35
4.3.4.2 Metric of Data access Trust Value TDA.....	36
4.3.5 Resources.....	40
4.3.5.1 Data input for Resources	40
4.3.5.2 Metric of Resources Trust Value TR.....	40
4.3.6 Authentication	43
4.3.6.1 Data input for Authentication	43
4.3.6.2 Metric of Authentication Trust Value TA.....	43
4.3.7 Feedbacks	45

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

4.3.7.1	Data input for Feedbacks.....	45
4.3.7.2	Metric of Feedback Trust Value TF	46
4.3.8	Access Point Security	46
4.3.8.1	Data input for Access Point Security	46
4.3.8.2	Metric of Access Point Security Trust Value TAS	47
4.3.9	Service Level Agreement	48
4.3.9.1	Data input for SLA.....	48
4.3.9.2	Metric of SLA per special term Trust Value TSLA1, SLA2.	48
4.3.10	Total Trust Value.....	49
4.3.11	Overall Trust Weights	49
4.4	Applying the proposed trust model	49
4.4.1	University on IaaS.....	50
4.4.2	Simulation Results	51
Chapter 5 : Personal Data Protection: Proposed Technical and Organizational measures for Cloud Providers		55
5.1	Introduction	55
5.2	GDPR REQUIREMENTS	55
5.2.1	Material and territorial scope	55
5.2.2	Data protection principles	56
5.2.3	Consent.....	57
5.2.4	Children – Parental Consent	57
5.2.5	Sensitive data and lawful processing	58
5.2.6	Information notices	58
5.2.7	Subject access, rectification and portability	58
5.2.8	Rights to object.....	59
5.2.9	Right to erasure and right to restriction of processing.....	59
5.2.10	Profiling and automated decision-taking	59
5.2.11	Accountability, security and breach notification	60
5.3	Countermeasures depending on the Cloud Architecture.....	60
5.3.1	GDPR Roles and Cloud Architectures.....	60
5.3.2	Infrastructure as a Service	61
5.3.3	Platform as a Service	63
5.3.4	Software as a Service.....	65
5.3.5	Comparative analysis	67
5.4	Conforming to GDPR in a PaaS environment	69
5.4.1	Details for the provider and its deployment.....	69
5.4.2	Material and territorial scope	70

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

5.4.3	Data protection principles.....	70
5.4.4	Consent.....	70
5.4.5	Children – Parental Consent.....	70
5.4.6	Sensitive data and lawful processing.....	71
5.4.7	Information notices.....	71
5.4.8	Subject’s access, rectification and portability.....	71
5.4.9	Right to erasure and right to restriction of processing.....	71
5.4.10	Profiling and automated decision-taking.....	72
5.4.11	Accountability, security and breach notification.....	72
5.4.12	Results of conforming.....	72
Chapter 6 : Utilizing a Privacy Impact Assessment Method using Metrics		73
6.1	Introduction.....	73
6.2	Literature Review.....	73
6.3	The Proposed Security and Privacy Impact Assessment Method.....	75
6.3.1	Scope of the Proposed Method.....	75
6.3.2	Theoretical Background.....	76
6.3.2.1	Data Sets Definitions.....	76
6.3.2.2	The Role of Privacy Principles, Privacy and Security Requirements.....	76
6.3.3	Quantification of Security and Privacy Requirements.....	79
6.3.3.1	Security Requirements and Data Sets’ Sensitivity.....	79
6.3.3.2	Privacy Requirements and Principles.....	81
6.3.4	The Proposed PIA Method.....	85
Chapter 7 : Conclusions and Future Work		87
7.1	Conclusion.....	87
7.2	Future Work.....	87
References		88

List of figures

Figure 1: Cloud Definition.....	16
Figure 2: Architecture of the model.....	23
Figure 3: Modes of Geolocation Data Generation and Collection	33
Figure 4: A Common Security and Privacy	76
Figure 5: Privacy Audit Methodology Structure Methodology	77
Figure 6: The overall Data Set Sensitivity	80

List of tables

Table 1 Thesis Contribution	18
Table 2 Customer's Trust Table	20
Table 3 Modes of Geolocation Data Generation and Collection	28
Table 4 Trust Value per Device Type	32
Table 5 Trust Value per Operating System	32
Table 6 Geo-location Trust.....	35
Table 7 Data Categorization.....	36
Table 8 Trust Values for Highly Restricted Data access.....	37
Table 9 Trust Values for Restricted Data access.....	37
Table 10 Trust Values for Internal Data access.....	37
Table 11 Trust Weights per Data Categorization.....	38
Table 12 Trust Weights per Session Time.....	38
Table 13 Trust Values for Unauthorized actions.....	39
Table 14 Trust Weights Data Access	39
Table 15 Trust Values for bandwidth deviation.....	40
Table 16 Trust Values for User's Memory usage.....	41
Table 17 Trust Values for Cloud Memory usage	41
Table 18 Trust Values for CPU Usage	41
Table 19 Trust Values for Ports	42
Table 20 Proposed Trust Weight per Resource Categorization	42
Table 21 Trust Value for Negative Logins	43
Table 22 Trust Value for Authentication Method Used.....	44
Table 23 Weights for Trust Value of Authentication	45

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Table 24 Trust Value for Antivirus..... 47

Table 25 Trust Value for Software Installed..... 47

Table 26 Proposed Weights of Trust for Access Point Security 48

Table 27 Proposed Trust Weights for Overall Trust..... 49

Table 28 Trust Values of Student’s Data 51

Table 29 Trust Values of Malicious User 52

Table 30 GDPR Requirements & IAAS Cloud Applicability 62

Table 31 GDPR Requirements & PAAS Cloud Applicability 64

Table 32 GDPR Requirements & SAAS Cloud Applicability 66

Table 33 Recommended and Obligatory measures for data processors..... 67

Table 34 Recommended and obligatory measures for data controllers..... 67

Table 35. Indicative Characteristics and Values of the Organization 82

Table 36. The Proposed PIA Method..... 85

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Chapter 1 : Introduction

During the last decades, the vast growth of Information Technology has led to a huge increase of computational and storage needs from all organizations. This made the use of Cloud computing more and more popular. The main advantages that led to this popularity are cost efficiency, unlimited storage, backup and recovery, easy maintenance, and quick deployment. The major obstacle to the widespread deployment of cloud systems is the feel of insecurity by many people and organizations, making them reluctant to use cloud services.

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

[1]

A system can be defined as cloud if it fulfills the following characteristics:

(1) On-demand self-service. Computing and storage resources can be provisioned and deprovisioned based on cloud user’s need without any human interaction with the cloud provider.

(2) Broad network access: Resources are provisioned over the network and accessed through specific access points.

(3) Resource pooling. Cloud providers provide a huge number of resources that are pooled to serve cloud users-customers.

(4) Rapid elasticity. Resources can be elastically provisioned and released, to cover cloud needs in an automatic manner.

(5) Measured service. Resource usage is monitored, controlled and measured providing transparency.”

[1]

Cloud Computing can be classified into three service models which are:

(1) Infrastructure as a Service (IaaS): Provides hardware resources as computing facility, storage, memory etc. Known provider of IaaS is Amazon with EC2 and S3.

(2) Platform as a Service (PaaS): The term platform is related to systems (e.g. operating system) that can be used to develop and build custom applications. Known provider of PaaS is Microsoft Azure.

(3) Software as a Service (SaaS): Provides any type of software (application or service) through cloud. Known provider of SaaS is Salesforce. [13]

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Independently of service model, cloud computing environments can be classified in four deployment models which are:

(1) Private cloud: Cloud infrastructure is dedicatedly used by one organization and can be hosted and used by the organization itself or a third party.

(2) Community Cloud: Resources are used by a community of organization having a common goal or usage. It can be owned, maintained, and provisioned by one or more members of community or a third party.

(3) Public Cloud: Infrastructure is available to many organizations and is maintained by a cloud provider.

(4): Hybrid Cloud: Combination of two or more clouds of any of the previous types which preserve their autonomous character but can collaborate to host application and data. [14]

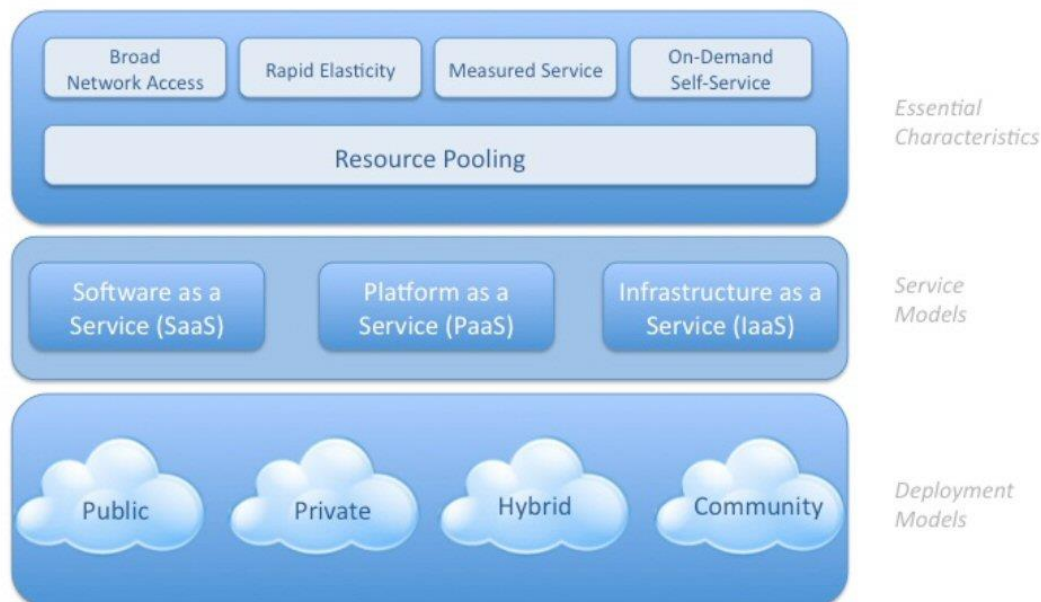


Figure 1: Cloud Definition

The main objective of this thesis is to identify security solutions that will overcome Cloud Computing trust management, privacy, and protection of personal data. More specifically in Chapter 2 the problem of Cloud Computing Security is analyzed, highlighting the goals and contribution of the thesis to this field. In Chapter 3, a literature review of existing trust solutions in Cloud Computing systems is provided, defining the advantages, disadvantages, and corresponding deficiencies of its one. Having as input the results of the literature review, in Chapter 4 an adjustable cloud specific trust management solution is presented defining parameters, metrics and modelling. In Chapter 5, guidelines for protecting personal data in Cloud Computing Environments are presented. The goal is to assist cloud data controllers to achieve compliance with the General Data Protection Regulation. In Chapter 6, a Privacy Impact Assessment method, developed in collaboration with other researchers in the Systems Security Lab, is adopted in order to support the data

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

controllers to assess the impact of modern Cloud Computing Environments and applications on customers' privacy.

Chapter 2 : Problem Identification

Cloud computing is wide and offers a range of technical and organizational advantages. However, the applicability in organizations requires attention in terms of security, management of sensitive and personal data and privacy. More specifically, cloud computing environments face all security risks of conventional distributed systems, but also the ones that are coming from virtualization, dynamic resource management, shared resources, and all the known cloud security threats. [4]

Due to the diversity of cloud computing, security solutions and models for conventional systems cannot reassure the security, trust, privacy, and personal data protection of cloud computing environments. In conventional systems, the resources used for storage and management of information can be clearly defined. Same applies to network, access points and people who have access. Previous systems are composed of a network of access points and access persons where information is transmitted in a clear and specific manner which results to be easily identifiable the untrusted or unsafe behavior. In cloud computing environments the location of data and who has access is not as clear as in conventional distributed systems. Based on the above, the research and existing solutions for distributed systems, regarding trust management modeling, personal data protection and privacy, cannot be applied to cloud . [12]

2.1 Goals and Contribution

The goal of this thesis is to cover a wide range of security issues that arise from the adoption of cloud computing. These are the lack of proper privacy, protection of personal data and trust management. More specifically we initiated our research by studying, analyzing and evaluating trust models for cloud. Based on the deficiencies concluded from this study we proceeded to the design and development of an adjustable Trust Management Model that quantifies trust and can be adjusted based on the parameters and the nature of cloud computing environments. Furthermore, within this thesis we provide technical and organization measurers to cloud providers in order to support them in the process of GDPR compliance. Another primary contribution is the adoption of a privacy impact assessment methodology, that has been developed in collaboration with other researches in the Systems Security Lab, that will further assist the protection of the users' privacy. More specifically, the scientific contribution of the thesis can be summarized as follows:

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- i. Detailed review of the existing trust management models for cloud computing environments including a critical comparison of the proposed solutions. Development of an adjustable, versatile and stable trust management model for managing trust between provider and client-user.
- ii. Review of exiting GDPR compliance proposals for cloud computing environments. Proposal of the technical and organizational measures that a cloud provider should employ in order to comply to GDPR.
- iii. Adoption of a privacy impact assessment methodology for protecting users' privacy .
- iv. Validation of all of the above.

The following table summarizes the contribution of this Ph.D. thesis:

Table 1 Thesis Contribution

	SHORT DESCRIPTION	CONTRIBUTION
I	Literature Review of Trust Models for Cloud Computing.	Error! Reference source not found.
II	Trust Management Parameters in Cloud Computing Environments	[93]
III, IV	GDPR Compliance: Proposed Technical and Organizational measures for Cloud Providers	Error! Reference source not found., Error! Reference source not found.
V	A proposed privacy impact assessment method using metrics based on organizational characteristics.	[92]
VI	Utilizing a privacy impact assessment method using metrics in the healthcare sector	[96]
VII	Trust Model in Cloud Computing Environments	[To be published]

Chapter 3 : Trust Models in Cloud Computing

3.1 Trust in Cloud

One of major obstacles to the widespread deployment of cloud systems is the issue of mutual trust between the user and the cloud provider. When data are stored on the cloud, users feel that they are losing control and they are suspicious on issues like, who has access on them, how their data are processed or/and copied etc. The trust mechanisms that can be applied, act as countermeasures to the previous concerns, since trust achieves to establish entities' relationship quickly and safely. However existing trust models that are utilized, for instance, for a datacenter that is restricted in the perimeter of an organization, are not appropriate for cloud computing environments. The main reasons for that are listed next:

- Data processing: When a customer transfers his data to the cloud the primary processor of the data is not the physical owner any more but the provider. This fact makes things different in terms of trust, since a new threat parameter is raised. In other words the physical processor of the data should always be totally trust-full. However the cloud provider can never be fully trusted.

- Data location: In conventional systems the geo-logical area of data is always known. When deploying services in cloud computing systems the physical location of data is no longer always known or fully trusted. A trust model that does not take into account the location of data in transit can no longer be considered as applicable in cloud systems.

- Data access: The location from which users access the cloud is unknown and cannot be localized.

- Number of users: In conventional systems it is not very hard to define the number of people that can access the system. However in cloud computing environments neither the provider nor the customers can feel confident about the number of people that can access the systems.

- Composite services: A common scenario in cloud is that of sub-contracting. In other words a customer pays for a service and the provider of that specific service pays some other provider for a part of the service that he is supposed to be delivering to the customer.

Trust is an abstract and subjective term. In general it is the process of recognition of an entity's identity and the confidence on its behavior. In the cloud context the term 'entity' includes the cloud provider and his personnel, the cloud user and the data owner. Trust can be achieved through trust mechanisms that apply trust

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

models. A trust model is a management method or protocol that includes trust establishment, trust renewal and trust withdrawal. Trust management of cloud computing systems cannot be performed with the conventional trust models. This is due to the special characteristics of the cloud systems – i.e. their size, location, lack of perimeter, number of users and lack of confidence – that yield the existing trust models for distributed systems inappropriate.

3.2 Literature Review

In the next section we present a comprehensive overview of the existing cloud trust models including their advantages and disadvantages.

3.2.1 Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment

In [15] Li et al. presents a domain-based trust model that supports two cloud roles: cloud customer and cloud provider. The cloud is divided in trust domains. Each trust domain includes all the resources that belong to the same provider. On each domain a trust agent is installed to manage trust. In this model each customer stores and manages a customer’s trust table like the one below:

Table 2 Customer’s Trust Table

Domain Name	Service type	Trust value/ trust degree	Generation Time
DOM. 1	COMPUTATION	TV1	2016-01-01 12:00
DOM. 2	STORAGE	TV2	2015-02-14 12:00

Trust is sensitive to context and for that reason the customer’s trust table has a column for the “service type” (computation, storage etc.). In addition to the actual service types there is also a service type named “trust recommendation” which is used in case a customer uses the service for first time and it is provided by other familiar domains. Every time that a service is used a new trust value is calculated, updates at the same time the “trust recommendation” value of the corresponding providers. Providers rely on their domain trust agent to manage trust. The agent stores and maintains the domain trust table which records trust values for the other domains. In the proposed trust model, there is a threshold value that can be defined for trusting or not trusting each cloud entity or trust domain. The decision is taken as follows: A search for locating a value in the corresponding local trust table is performed. If a value is found and if it exceeds the threshold, the entity (cloud user or provider) will agree to continue the transaction. If no corresponding value exists, the entity will request for a trust value within familiar domains and the original trust will be calculated using the received

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

trust values recommendation from familiar and corresponding recommendation weight that based on confidentiality of each neighbor. The trust value is being updated after every transaction or after some specific time period that is different per cloud role. For instance, for customers it sets a time-stamp and periodically deletes expired records.

The proposed trust model has been verified through a simulation experiment. The experiments set up two evaluation factors: trust accuracy and transaction success rate. The disadvantage of the proposed model is that it cannot be used in environments with more than one cloud providers where “sub-contracting” exists and trust is turned into a chain (cross-cloud). Also, it cannot support large-scale environments

3.2.2 A Collaborative Trust Model of Firewall-through based on Computing

In [16] another domain –based trust model is proposed, namely the “Collaborative Trust Model of firewall-through”, which separates the Cloud in different autonomous domains. The trust relationships are divided into within-domain relationships and inter-domain. The described model divides the cloud into different domains, assigning to each domain entities with neighboring location according to physical address. A trust table that keeps the trust values of nodes which have traded with other nodes within the domain, is maintained. This model can support trading between nodes of the same domain directly since trust values are stored for past trades, between neighboring nodes. Each domain maintains three trust tables, namely: the DITT(Domain inside trust table), the DOTT(Domain outside trust table) and the RVT(risk-value table). The DITT stores trust values for all the nodes inside the domain, calculated as the average weight of recommended trust value of nodes which already have traded with this node. The DOTT stores the value of the overall confidence by the definition of risk. This model adopts a time decay function $T(t) = 1/(1 + \lambda(T-t))$ where T is the current time, t is the last transaction time, λ is a constant that equals to $1/604800$, for gradually decreasing the trust value between nodes that have not traded each other for a long time. So the trust value is calculated as follows:

- If nodes performed transactions in the past, the following formula defines trust based on historical values as the sum of:

$$tv = (\text{historical trust value}) + k_1 * \varphi(N_s) \text{ when the transaction was successful}$$

$$tv = (\text{historical trust value}) - k_2 * \varphi(N_{us}) \text{ when the transaction failed}$$

Finally $tv = tv * T(t)$ Where $0 < k_1, k_2 < 1$ stands for the update coefficient and $\varphi(x) = e^{-1/x}$.

- If nodes did not perform any transaction in the past then the calculation depends on whether the nodes are in the same domain or not. If they are in the same domain the trust value in DITT is maintained by a domain agent and then adds the decay of time.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

$$tv = f(x) - xixT(t)$$

When nodes are not in the same domain, the trust value can be calculated by sending a request to the domain agent who searches the DOTT for a trust value.

A major advantage of the above model is that a different security policy can be defined per domain. Also, in order to calculate the trust, the model takes into account important factors like the transaction context, the historical data of entity influences. Last but not least, the model has the unique characteristic that it is compatible with firewalls in order not to violate local control policies.

3.2.3 Secure Trust Model Based on Trusted Computing

Cin Zhixi in [17] proposes a trust model for trusted computing based in peer-to-peer systems. The model is based on the hypothesis that each peer's platform (member of the cloud) is equipped with a Trusted Platform Module (TPM). The Trusted Platform Module was proposed by The Trusted Computing Group (TCG) an industry consortium which has developed international standards for using Trusted Computing techniques. The TPM is a hardware security component built into many computers and computer-based products. The TPM applies machine authentication, hardware encryption, signing, secure key storage, and attestation. Machine authentication is a core principle that allows clouds to authenticate known machine and thus offer a higher level of security. In TPMs the feature of attestation is applied, to provide information on what is executed on a machine by monitoring the software while it is loaded. In the proposed model a starting point is the registration of every peer to an offline issuer to obtain a DAA certificate. DAA is a Direct Anonymous Attestation protocol that is used to implement anonymous attestation, maintaining the anonymity of the platform. The peers that have the same issuer are organized into a group, leading to two types of trust relationships: trust within the group and trust relationship between groups. In a system of m groups there is a maximum matrix a where a_{ij} represents the rating value rated by group G_i to group G_j . . Within a group of n peers, each peer N_i has a rating S_{iq} for a peer of the same group N_q . The architecture of the model is shown in Fig. 3 below:

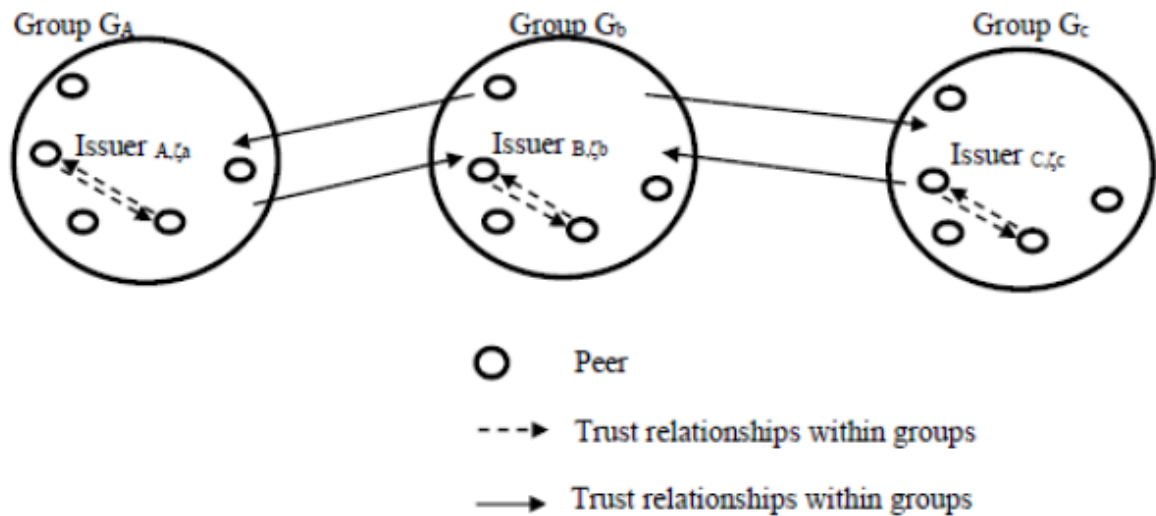


Figure 2: Architecture of the model

The trust value-rating is influenced by the responses given by all members of a group, irrespective of whether the peers are in the same group or not. The peer that will request a service will select the peer with the higher trust value.

The main contribution of this model is that it supports anonymity. It is also noticeable that a solution for encryption is presented on trust level and is applied through a protected hardware storage.

3.2.4 Trust Management system for Grid and Cloud Resources

In [18] Manuel et al. propose a trust model that approaches trust management from the security aspect and from the reputation of the resources involved. It can be applied in grid and cloud systems. The model is based on a resource broker that evaluates the trustworthiness of cloud resources. It computes trust using three components: “Security Level Evaluator”, “Feedback Evaluator” and “Reputation Trust Evaluator”. Security Level Evaluation has been carried out based on authentication type, authorization type and self-security competence mechanism. The authentication types that are supported are Simple Password Authentication, X.509 Authentication and Kerberos with relevant trust values 1, 2 and 3 respectively. The authorization types and the corresponding trust values are Simple Password with trust value 1, Identity Based with trust value 2 and role based with trust value 3. The Feedback Evaluator is responsible for user’s feedback, including its verification and the storing in the relevant repository. The Reputation Trust Evaluator computes the trust depending on the capabilities of the resources. The evaluation is based on computational parameters (processor speed and free ram) and network parameters (bandwidth and latency). Finally the overall trust value can be defined as the sum of the trust values calculated for security level, user’s feedback and reputation.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

The resource with the higher trust value is selected. The major contribution/advantage of this model is that it separates trust into three different levels presenting also a clear metric for trust evaluation.

3.2.5 SLA-based Trust Model for Cloud Computing

Alhamad et al. proposed a SLA based trust model [19] for cloud computing. Major participants in the model are:

- The SLA agents: Main module of the model since it classifies the customers-consumers into classes. The classification is done according to their needs. Furthermore, it designs the SLA metrics, negotiates with cloud providers, selects the providers based on nonfunctional requirements, and monitors the activities of consumers and the parameters of the SLA.

- The cloud consumer: This module is responsible for requesting services from cloud providers. The main part of the cloud consumer is the trust management model that handles trust relationships between the customer, the providers and the other customers. The sources for calculating trust are the local experiences, the opinions of other cloud services and the reports of the SLA agent. Credibility metrics are used to achieve reliable results for the model. Customers can assign relevant weights. The trust value will be utilized for ranking the providers and the whole list of ranked providers will be sent to the SLA agent.

- The Cloud services directory: Cloud providers can advertise themselves in this module and the consumer can select, through this module, providers that meet their needs.

No implementation or evaluation is described for this model, resulting to a lack of knowledge as far as its functionality and effectiveness are concerned. Its major advantage is that it is SLA based.

3.2.6 A Trusted Computing Environment Model in Cloud Architecture

A model called a multi-tenancy trusted computing environment model (MTCEM) is proposed by Yong et al., [20]. MTCEM is dedicated to IAAS cloud environments providing a two-level transitive trust mechanism. MTCEM supports the security duty separation and includes three types of participants, Cloud Service Provider, customers and auditors. Main responsibility of CSP is to maintain infrastructures trusted, while the customer's responsibility is to keep trusted the guest OS on the Virtual Machines provided by the CSP. The auditor monitors the services provided by the CSP on behalf of the customers.

A prototype system is implemented by the authors to prove that MTCEM is capable of being implemented on hardware and software. However, no evaluation of the prototype's performance has been presented.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

3.2.7 Evaluation of Behavioral Security in Cloud Computing

In [21] a trust model that considers behavioral security in Cloud computing is presented. The model focuses on the trust of the service provider to the user and includes the following participants-relationships: Enterprise Service Provider (ESP)-Enterprise User (EU), Cloud Service Provider (CSP)- Cloud User (CU), Cloud Service Provider (CSP)-Enterprise Cloud User (ECU), as well as on the trust of Internet Service Providers to its users: ISP-CU, ISP-ECU, ISP-CSP. It defines principles for trust evaluation:

- Expired behavior in evaluating can be approximated as a strange user.
- Behavior evaluating effect is in proportion to behavior time and abnormal degree of behavior.
- The credibility of trust evaluation is in proportion to number of times of user access cloud resources.
- Slow-rise in trust evaluation for prevention of fraud risk.

The main concept is "divide and treat" based on a hierarchical structure model for decomposing complicated user behavior trust (UT) into small sub-trust (ST) namely security behavior sub-trust (SST), contract behavior sub-trust (CST), expense behavior sub-trust (EST) and identity reauthentication sub-trust (IST).

The main advantage of this model is that it is taking into account evidence about user's behavior. However, no trust metric is presented and no simulation.

3.2.8 Cross-Tenant Trust Models in Cloud Computing

In [22], a cross-tenant trust model (CTTM) which supports various types of trust relationships and combines authorization domains of each tenant, is presented. The main goal of the model is to combine trust with authorization and role based access. It is based on the hypothesis that cross-tenant trust relation should be reflexive, but not transitive, symmetric or anti-symmetric. Four types of trust relationships are defined in the model that enable and control cross-tenant access:

- Type- α : trustor can give access to trustee.
- Type- β : trustee can give access to trustor.
- Type- γ : trustee can take access from trustor.
- Type- δ : trustor can take access from trustee.

Afterwards a role-based extension (RB-CTTM) of the model is presented to pass from simple authorization to role based.

The main advantage of this model is that it attempts to apply trust-based authorization on user's data. No simulation has been presented, but an implementation in OpenStack is described as future work.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

3.3 Summary & Comparison of trust computing models

Several trust models and trust management methods are presented in contemporary literature. An overview of the most scientifically interested was presented in the previous section. Proper trust management in cloud should overcome security and privacy issues related to data location, storage, confidentiality, availability and integrity, by establishing safe and quickly trusted relationships between cloud provider and the cloud customers. Cloud customers need to feel confident about their privacy protection and the confidentiality and availability of their data. On the other hand, service providers are concerned about the faithfulness, identity and integrity of the users.

An initial list of requirements that could be employed for assessing a trust model is the following:

- **Trust metric:** In a trust model it is necessary to define a method of quantifying trust. Since trust is an abstract term a method of measuring the trust value of a cloud provider or of a cloud customer should be defined. It is also necessary to define the quantified levels of trust as a part of the trust model.
- **Abnormal behavior:** A major factor in the assessment of trust should be the abnormal behavior of users in the cloud. A behavior that deviates from the average or an old behavioral history or even a short-term access, should result to zero trust. As a result, it is considered necessary for cloud trust models to define which behavior is conceived as normal and which not. Furthermore, the weights and criteria (time, history, weights of normal vs abnormal) should also be described.
- **Identity Management/ Authentication:** In order to collect the trust related feedback, a model needs to ensure that the identities of the users are real. To this end it is necessary to authenticate the users. Thus, another requirement for the model is to apply an identity management / authentication scheme.
- **Data Security:** Trust management and relevant models are implemented as part of the overall security management scheme of the cloud. So a trust model should specify the minimum requirements for achieving an acceptable level of data security.
- **SLA:** A Service Level Agreement is the formal agreement among the provider and the user that clearly sets the requirements of both parties. The SLA should be part of the trust management process.

Chapter 4 : Trust Management Model in Cloud Computing Environments

4.1 Introduction

Based on our previous literature review research [34], we propose a list of trust parameters and a configurable model with its corresponding metric, together with an in-depth description of how trust management can be applied per parameter.

4.2 Trust Parameters

Defining the correct trust parameters is a key point for successful trust management. They should take into account all the aspects and factors of a cloud architecture that could affect trust. The proposed list of trust parameters follows next.

A user typically connects to the cloud from a pre-defined range of devices. By device we mean any electronic device that a cloud user could employ for accessing cloud services (Laptops, desktops, mobile phones, tablets, etc.). The range of devices that have been already used for connecting to the cloud, and thus fulfill the security policy criteria of the provider, will be referred as “Trusted Access Points”.

A trust security policy should take into account the access point and extra attention should be paid in the case of new devices. The unknown devices must be identified and should fulfill the security policy’s minimum requirements. For instance, mobile devices can be prohibited from the security policy **Error! Reference source not found.**

Determining the geo-location of a device is the process of defining, in a precise manner, the latitude/longitude coordinates of the device together with some other characteristics like country, city, address, zip code and time zone. Based on Isaca’s definitions **Error! Reference source not found.**, Geolocation data are generated and collected either in an active mode, referred as user-device-based geolocation, or in a passive mode, referred as table look-up or data correlation server-based geolocation. Table 3 **Error! Reference source not found.** summarizes these modes and the technologies that each mode employs.

Table 3 Modes of Geolocation Data Generation and Collection

Mode	Collection Method	Technologies Involved
Active: User—Device-based	Uses firmware and software on user’s computer or wireless device. Location determined via GPS chip and/or triangulation using cellular tower information. Request-response model	GPS Assisted GPS (A-GPS) Wi-Fi—Wireless positioning 3G/4G Mobile applications—iPhone, Android devices, BlackBerry®
Passive: Data-lookup—Sever-based	Involves use of third-party geolocation service providers, e.g., Quova®, NetGeo, Bering Media. Based on non location-specific IP address acquired from user device or service set identifiers (SSIDs) for wireless networks. Correlation with stored IP or SSID databases obtained from purchase records, user-provided information, network analysis of trace routes and domain name system (DNS) host names	IP location—Whois lookup, DNS LOC, geographic names in domain name user or application information, timing data using ping inference based on routing data, e.g., traceroute monitoring of Internet service provider (ISP) networks 3G/4G Wi-Fi—Wireless positioning

A far as privacy issues are concerned, the proposed model will need the IP Geolocation. Assuming that we have an accurate method for retrieving the location of a cloud client, we will consider how this affects the trustfulness of the client, justifying the fact that a trust security policy should take into account geolocation information [37]-[39],[23].

In all types of systems (cloud and conventional), a user follows a similar pattern of actions (behavior). In other words, the behavior of a user is expected to be similar within different sessions **Error! Reference source not found. Error! Reference source not found.**A trust security policy should take into account the behavior characteristics of its users. More specifically it is necessary to monitor the data that a user is typically

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

accessing and to consider cases of abnormal behavior. The typical user behavior, in terms of the data that he is accessing and the actions that he is performing, will be referred as “Trusted Behavior”.

A cloud user typically consumes specific resources while using the cloud. By Resources we refer to network and hardware components that the user consumes while connected to cloud. The various resources utilized by a user during a specific session will be monitored and will be referred as “Trusted Resources”.

Another major parameter of the proper trust management is the authentication behavior of the cloud user. In cases of outsourcing, feedback on consumers who had transactions with other service providers is required. Specifying a common feedback trust metric, regarding trustfulness, between providers, will facilitate the consideration of this information.

Since trust management is part of the security policy, it is evident that the security of the access point – user’s computer, phone tablet, etc. – should be considered as an important parameter in the trust metric. The most important items that should be checked are the following:

- a) *Use of antivirus*
- b) *Use of firewall*
- c) *Operating System’s Updates and Patches are installed*
- d) *List of Software installed*

4.3 Trust Model and Metric

4.3.1 Overview

In order to apply trust and help security professionals in cloud environment it is obligatory to quantify trust. The factors that influence trust are the following and were analytically presented in previous section:

- Access Point
- Geo-Location
- Data Access
- Resources
- Authentication
- Feedback
- Access Point Security
- SLA Special Terms

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

In our metric a weight will be defined for every factor to depict the importance of each one. The weights are:

- W_{AP} : Weight of Trusted Access Point
- W_L : Weight of Geo-location characteristics
- W_{DA} : Weight of Data Access
- W_R : Weight of Resources
- W_A : Weight of Authentication
- W_F : Weight of Feedback
- W_{AS} : Weight of Access Point Security
- $W_{ST1...N}$: Weights of Special terms.

Weight values will range from 0 to 1, while the sum of all weights should be 1:

$$W_{AP} + W_L + W_{DA} + W_R + W_A + W_F + W_{AS} + W_{ST1} + W_{ST2} + \dots + W_{STn} = 1$$

The value of each weight should reflect the criticality of the respective factor for the specific information system / environment under study. Thus, depending on the Threats that a specific information system is facing, the identified vulnerabilities that these threats may explore, but also the consequences (impact) that may be caused, from a potential security incident to the owner of the information system, each of the aforementioned factors will affect (may be the cause of an incident) the trust level of the system in a different way.

To this respect the aforementioned weightings for a specific information systems / environment will be specified by utilizing the results of a risk analysis for the cloud system.

4.3.2 Trusted Access Point

4.3.2.1 Data input for Trusted Access Points

Cloud users use access points to connect to cloud using a precollected range of devices. Access points are all the electronic devices that Cloud permits usage to access it. (Laptop's, desktops, mobile phones tablets etc.). Partially trusted range of devices can be defined all the devices that a user has already connected in the past since they fulfill the security policy criteria to have access.

In favor of Trusted Range of Devices, a table with main characteristics per device should be maintained in a central repository within the perimeter of cloud provider:

- User ID

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- Unique ID of Device
- Type
- Operating System
- Date of Last Session

Collection and definition of each characteristic:

- a. User ID: A unique number that will be assigned to every user that is preassigned in the cloud.
- b. Unique ID of Device: Every device that a client uses to access the cloud is defined with a unique number. This unique number is the result of a salted (Type of Device +MAC address).
- c. Type: Categorization of device. (Mobile, Laptop, Desktop, Tablet etc.)
- d. Operating System: The type of Operating System of Device will be saved since it changes the Security Values. A device working on Android cannot be adequately safe with one that works on Windows Server.
- e. Date of Last Session: The last date time the specific device accessed the cloud.

Every time a user endeavors to access cloud an identification and authorization process will be raised. The identification refers to the case of checking if the user has already been whitelisted for the device by checking the central's repository's table. When a user accesses the cloud from an unknown device a security flag of attention should be raised that shall initiate a process of whether the device can be included in the previous trusted access point range not based on his overall behavior during the cloud access.

The unknown devices must be identified and should fulfill the security policy's minimum requirements. For example, mobile devices can be prohibited from security policy.

In real world a way to implement the above is to develop an Applet that will be deployed on every client upon first negotiation. The applet will be responsible on every logon on the cloud service to send to Provider the MAC address with the OS details and Update the value in the "Trusted Range of devices Repository". Issues that should be noticed are what happens with low resources devices. (Mobile, tablets etc.)

4.3.2.2 Metric of Access Point Trust Value TAP

At the initial configuration of trust metric, a trust value in scale of 100 will be assigned to types of devices and operating systems and an importance weight of device type and operating system.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Based on empirical data, the trust value for each device type T_{DT} should respect the following guidelines:

Table 4 Trust Value per Device Type

Device Type	Trust Value T_{DT}
Desktop	90
Server	90
Laptop	80
Tablet	50
Mobile	30

while the trust value for the operating system of the device T_{OS} will be determined according to the following guidelines:

Table 5 Trust Value per Operating System

Operating System	Trust Value T_{OS}
Windows over version 8	90
Windows below version 8	10
Windows Server over version 2012 R2	90
Windows Server below version 2012 R2	10
Apple Mojave v 10.14 and above	90
Apple High Sierra v 10.13 and above	90
Apple Sierra v 10.12 and above	70
Apple Yosemite v10.10 and above	70
Apple El Capital v 10.11.6 and above	70
Apple Mavericks v10.9 and above	70
Apple Mountain Lion v 10.8 and above	70
RedHat 6.x and above	60
CentOS 6.x and above	60

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Ubuntu 12.04 LTS	60
Apple iOs 11 and above	40
Android 4.4 (KitKat) or later	40
Windows 7 or later in S mode	40

In the overall metric regarding trust value of access point the weight defined for device type and operating system (W_{DT} & W_{OT}) will be changing based on the vulnerabilities we have on software and hardware level as concluded from the results of risk analysis. In other words, the weight we give to device type and operating system will change based on how possible we believe is in attack to happen to each of them. The main reason for the previous, is the adaptiveness we want to achieve in our model based on the nature of systems we want to support.

To evaluate trust, our model will identify if the access point is in the range of trusted devices and if the previous is valid the trust value will be the weighted sum of Device's type and Operating System as retrieved during the authentication. In case the device is not in the trusted range of devices the trust value from previous description will be divided by 1.25 to narrow down the trust we assign. The mathematical representation of the above will be:

- If AP is trusted $T_{AP} = (W_{DT} * \text{Trust Value for Device Type} + W_{OT} * \text{Trust Value for Operating System})$
- If AP is not trusted $T_{AP} = (W_{DT} * \text{Trust Value for Device Type} + W_{OT} * \text{Trust Value for Operating System}) / 1.25$

To avoid that a malicious pretends using a trusted device we suppose that other security measures cover this part (e.g. authentication)

4.3.3 Location

4.3.3.1 Data input for Location

Geo-location is the process of defining in a precise manner the latitude/longitude coordinates of a device, including some other characteristics like country, city, address, zip code and time zone. Based on Isaca's definitions Geolocation data is generated and collected in one of two ways—in an active mode referred to as user-device-based geolocation or in a passive mode referred to as table look-up or data correlation server-based geolocation. Figure 3 summarizes these modes and the technologies each employs.

Mode	Collection Method	Technologies Involved
Active: User—Device-based	<ul style="list-style-type: none"> • Uses firmware and software on user’s computer or wireless device • Location determined via GPS chip and/or triangulation using cellular tower information • Request-response model 	<ul style="list-style-type: none"> • GPS • Assisted GPS (A-GPS) • Wi-Fi—Wireless positioning • 3G/4G • Mobile applications—iPhone, Android devices, BlackBerry®
Passive: Data-lookup—Sever-based	<ul style="list-style-type: none"> • Involves use of third-party geolocation service providers, e.g., Quova®, NetGeo, Bering Media • Based on nonlocation-specific IP address acquired from user device or service set identifiers (SSIDs) for wireless networks • Correlation with stored IP or SSID databases obtained from purchase records, user-provided information, network analysis of trace routes and domain name system (DNS) host names 	<ul style="list-style-type: none"> • IP location—Whois lookup, DNS LOC, geographic names in domain name user or application information, timing data using ping inference based on routing data, e.g., <i>traceroute</i> monitoring of Internet service provider (ISP) networks • 3G/4G • Wi-Fi—Wireless positioning

Figure 3: Modes of Geolocation Data Generation and Collection

For Privacy and resource purposes on our model we will use Ip Geolocation.

Every time a user is trying to access cloud measurements regarding his location will be collected. A platform will be deployed on cloud’s Provider side that through an agent will store the geo location characteristics of the user. A relevant table will be maintained with the following characteristics:

- User ID
- Location
- IP address
- City
- Country
- Zip
- Time zone
- Date and time

The above will be aggregated from the “Location Agent”, defining an aggregate location per user. Then an allowed perimeter with latitude/longitude coordinates will be defined providing that in the initial a configuration an acceptable distance will be set. When a user accesses the cloud from an unknown location a security flag of attention should be raised until the device is included or not, to trusted access location range. Method’s to overpass Ip spoofing should be considered.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

4.3.3.2 Metric of Geo-location Trust Value TL

During the initial configuration of trust metric, a trust value in scale of 100 will be assigned using as scale level the distance from previous locations named from now on as distance trust table. The Trust values will be defined on distance ranges basis of kilometers (e.g. 0-10 km: Trust value is 100, 10-20 km: Trust value is 90 etc.) A proposed table is presented below as base of configuration:

Table 6 Geo-location Trust

Range Distance in kms	Trust Value
0-5	100
5-8	90
8-20	60
20-350	50
Above 350	10

If the user is new then the distance used will be the one from the location the user is declaring to be located (address, city, country given) and the one retrieved. To evaluate trust for location our model will identify the location of user and define distances from previous locations the user has used cloud in the past. Based on the minimum calculated distance the trust value will be selected from the distance trust table where the distance is in the relevant range. If a user is out of the allowed perimeter (e.g. at a country out of Europe) the Trust value will be 0.

To avoid the scenario of malicious user knowing the location of user we suppose that the authentication mechanism in cloud will cover such problems.

The mathematical representation of the above:

$$T_L = \text{Value Defined in table for minimum Distance}$$

4.3.4 Data Access

4.3.4.1 Data input for Data Access

Even in non-cloud systems actions/data that the user is usually processing are almost common. Based on behavioral metrics a user typically is doing similar actions every time cloud is accessed. Cloud must apply appropriate audit techniques to store every time a user is accessing cloud the type of his action, in a central

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

repository from a user Audit Platform and its corresponding Agent named as Audit Data Agent. A table will be maintained containing the following info:

- User id
- Unit of the Application/OS
- Authorized or not
- Type of Action (read, write, delete)
- Description of Action
- Date and Time

The audit trail for Data access will be aggregated in an overall manner of the user by the Audit Data Agent. The overall aggregated values can be:

- The average volume of accessing each data categorization.
- Duration of access to the system.
- Unauthorized modification or view access endeavors.

Audit Trail methods and techniques will not be a part of this research since we will use method described in preexisting literature.

4.3.4.2 Metric of Data access Trust Value TDA

In order quantify trust for data access we have three separate calculations, T_{DAV} (Trust Data Access Volume), T_{DATS} (Trust Data Access Time Session), T_{DAM} (Trust Data Access Modification) Starting with the Data Access Volume we will separate the data of any cloud computing environment into three general data categories as described in the table below.

Table 7 Data Categorization

Data Type	Description
Highly restricted	Highly Confidential information whose inappropriate disclosure ¹ would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act.
Restricted	Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of "personal data" under the Data Protection Act

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Internal	Information not considered being public which should be shared only internally
----------	--

For each category of the previous we defined trust values on deviation volume basis per session. The volume ranges may change based on the nature of cloud. More specifically for Highly Restricted data:

Table 8 Trust Values for Highly Restricted Data access

Highly Restricted Deviation in Mbs	Trust Value for T _{DAS}
0-10	100
10-50	90
50-100	60
100-200	50
Above 200	10

Table 9 Trust Values for Restricted Data access

Restricted Deviation in Mbs	Trust Value for T _{DAS}
0-50	100
50-100	90
100-200	60
200-1000	50
Above 1000	10

Table 10 Trust Values for Internal Data access

Internal Deviation in Mbs	Trust Value for T _{DAS}
0-50	100
50-200	90
200-500	60
500-1000	50

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Above 1000	10
------------	----

For every category of data (highly restricted, restricted, internal) a weight in the calculation will be defined changing the factor to which they will change the final trust value for data access per session. The weights we propose are the below:

Table 11 Trust Weights per Data Categorization

Data Categorization	Weight
Highly Restricted	0.6
Restricted	0.3
Internal	0.1

The mathematical representation of the previous is the following:

- $T_{DAS} = \text{Sum}((\text{Weight of each Data Category}) * (T_{DA} \text{ of (Current Session's Data access per category)} - (\text{Average Data access per category normalized to current session's time})))$

To evaluate trust in terms of data access it is vital to consider another factor also, as mentioned above, the time that the user is connected to cloud and the corresponding deviation from the normal behavior. A corresponding table with trust values will be used here.

Table 12 Trust Weights per Session Time

Deviation of session time in minutes	Trust Value for T_{DATS}
0-5	100
6-15	90
16-30	60
31-60	40
61-100	30
Above 100	10

The mathematical representation of the previous is:

- $T_{DATS} = T_{DATS} ((\text{Current Duration of Session}) - (\text{Average Duration of Session}))$

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Finally, it is important to take under consideration the unauthorized behavior. The ranged deviations from the average unauthorized endeavors will lead to trust value. The corresponding trust table is the below:

Table 13 Trust Values for Unauthorized actions

Number of unauthorized actions	Trust Value for T_{DAM}
0-2	100
3-5	80
6-8	60
9-10	40
Above 10	10

The mathematical representation of the previous is:

- $T_{DAM} = T_{DAM} \left(\frac{\text{Current Session's unauthorized modifications or view data endeavors}}{\text{Average unauthorized modifications or view data endeavors}} \right)$

In the beginning of this section, we defined that in order to calculate trust in terms of Data Access we take into account the following factors:

- The average volume of accessing each data categorization.
- Duration of access to the system.
- Unauthorized modification or view access endeavors.

In the previous we defined how trust will be calculated in our model for each of the above.

To calculate overall trust for data access a corresponding weight will be defined for every factor. Relevant proposed table is the below:

Table 14 Trust Weights Data Access

Trust Metric for T_{DA}	Weights for T_{DA}
Data category accessed - W_{Das}	40%
Data access time - W_{DATS}	20%

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Unauthorized actions- WDAM	40%
----------------------------	-----

In the same logic we referred in previous sections, the weights above may differentiate based on the nature of cloud.

The overall trust value for data access will be the weight sum of each inputs

$$T_{DA} = W_{Das} * T_{Das} + W_{DATS} * T_{DATS} + W_{DAM} * T_{DAM}$$

4.3.5 Resources

4.3.5.1 Data input for Resources

A user of cloud typically consumes and provides specific resources while using cloud. In this part of the model measurements will be done during a user's session in cloud that will collect information regarding resources used. More specifically a monitor will record the following info in a table:

- User ID
- Device ID
- Total Time of Session
- Average Bandwidth of cloud network used
- Average Memory of device used as a percentage of total memory
- Average Memory of cloud network used
- Average CPU threads of user's device
- Network Ports that are accessed from the user
- Bytes sent
- Bytes received

In a specific part of the security policy thresholds will be defined fir resource limits. During every session when a cloud user gets above the resource a security flag will be raised resulting to subsequent actions.

4.3.5.2 Metric of Resources Trust Value TR

Trust value related to resources can be calculated as the deviations from the normal values per resource –time of session, bandwidth, memory of device used, memory of cloud network, CPU threads and network ports - defining first a scaling method of 100. At the initial configuration of the trust calculation weights for each input is decided and trust values on range level of each input.

Table 15 Trust Values for bandwidth deviation

Deviation in Mbps	Trust Value for T_{RB}
0-1	100
2-10	80
10.1-20	50
20.1-100	20

Table 16 Trust Values for User's Memory usage

Memory usage in MB	Trust Value for T_{RMU}
0-100	100
101-500	70
501-1000	40
Above 1001	10

Table 17 Trust Values for Cloud Memory usage

Memory usage in MB	Trust Value for T_{RMC}
0-100	100
101-500	70
501-1000	40
Above 1001	10

Table 18 Trust Values for CPU Usage

Deviation CPU usage in GHz	Trust Value for T_{CPU}
0-0.5	100
0.6-1	70
1-2	40
Above 2	10

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

The above may change based on the hardware configurations of the cloud.

Every system needs prespecified list of ports to work. Based on the definition ports will be separate in three lists. Ports request of user in normal situations, seminormal (e.g. system administrator), abnormal ports requests

Table 19 Trust Values for Ports

Port	Trust Value for T_{RP}
Normal Ports List	100
Semi-Normal	60
Abnormal	20

Weights to calculate the total trust values for resources are:

Table 20 Proposed Trust Weight per Resource Categorization

Trust for T_R	Weight for T_R
T_{RB}	20
T_{RMU}	20
T_{RMC}	20
T_{RCPU}	20
T_{RP}	20

The mathematical representations of the previous are:

- $T_{RB} = T_{RB} ((\text{Current Session's Bandwidth Usage in Mbps}) - (\text{Average Session Bandwidth Usage in Mbps on of the specific user}))$

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- $T_{RMU} = T_{RMU} ((\text{Current Memory usage of User's device}) - (\text{Average Memory usage of User's device}))$
- $T_{RMC} = T_{RMC} (\text{Current PCT of cloud memory consumed}) - (\text{Average PCT of cloud memory consumed})$
- $T_{RCPU} = T_{RCPU} ((\text{Current PCT of cloud CPU threads consumed}) - (\text{Average PCT of cloud CPU threads consumed}))$

Based on the ports used is trying to consume the corresponding trust values will be retrieved by searching the categorization of ports and corresponding trust values. The mathematical representation of the previous is:

$$T_{RP} = \text{Min}(\text{Trust value of ports used})$$

The total resources trust value will be the weighted sum of the previous:

$$T_R = W_{RB} * T_{RB} + W_{RMU} * T_{RMU} + W_{RMC} * T_{RMC} + W_{RCPU} * T_{RCPU} + W_{RP} * T_{RP}$$

4.3.6 Authentication

4.3.6.1 Data input for Authentication

Another major division of our trust model is the authentication behavior of the cloud user. Every time a client is endeavoring to access cloud measurements will be retrieved regarding authentication by the Authentication Trust Platform that based on our model will be installed on the Cloud Provider's Side. A table will be maintained that will store the following information:

- User id
- Negative Logins
- Tokens used and if the measurement on their weakness regarding for example dictionary attacks.
- Wrong authentication method used, in clouds with multiple authentication methods applied.

A trust authentication value per user will be calculated/updated based on defined values on every authentication process. When a user gets below a value, he will be on mistrusted user from the Authentication process. Log in will be banned and further processes will be required to reestablish trust authentication.

4.3.6.2 Metric of Authentication Trust Value TA

Trust metric for authentication can be defined as the measurement of authentication behaviors that deviate for average normal. During the initial configuration of the trust metric process weights on negative logins, token authentication method and on usage of wrong authentication method.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Trust value will be defined for number of negative logins in ranges. The trust Value will be auto updated on every negative login per session.

Trust values for number of negative logins are the ones presented in table below:

Table 21 Trust Value for Negative Logins

Number of negative logins	Trust Value for T_{AL}
0	100
1	90
2	80
3	70
4	60
5	50
Above 5	20

The mathematical representation of the previous is:

- $T_{AL} = T_{AL}$ for Number of Negative Logins

Below we present based on several sources the trust values for the selected authentication method:

Table 22 Trust Value for Authentication Method Used

Authentication Method	Trust Value for T_{AT}
Simple password	50
Complex password	70
Password with lifetime	60
OTP (One-time password)	75
MAC Address	70
IP address	65
Face recognition	75
Gestures scan	60
Multi-factor Authentication	85

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Any Other method	20
------------------	----

Per authentication method supported in cloud a trust value will be defined.

- T_{AT} = T of authentication method

When a cloud user is trying to use an authentication method other than the one selected for his account a trust value will be defined.

- T_{AW} = If Wrong authentication method is used, a fixed value will be defined.

As mentioned in previous the total trust value for authentication will be calculated using the weights below:

Table 23 Weights for Trust Value of Authentication

Authentication	Weight in calculation of T_A
Negative logins	30
Authentication Method	60
Use of wrong authentication method	10

Total trust for authentication will be:

$$T_A = W_{AL} * T_{AL} + W_{AT} * T_{AT} + W_{AW} * T_{AW}$$

4.3.7 Feedbacks

4.3.7.1 Data input for Feedbacks

The consumers or service providers in cases of outsourcing who have had transactions with the service providers provide feedback on various aspects of the services provided by the service providers. The feedback received for a service provider from various consumers is aggregated over a period. This forms the reputation of the specific service provider and the consumer first confirms the behavior of the service provider as being trustworthy or not, before proceeding to use the service provider. Cloud is separated in N-Spaces of feedback F. These spaces will be the physical address of user's retrieved from the geo-location recognition that we described before. Each user's feedback overall value f will be included in a space F. A feedback-oriented table will be maintained in cloud's space that will have the following values:

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- User ID
- Date of Last update
- Provider ID Feedback
- Feedback Trust Table

Process of Collecting Feedbacks:

Right after the completion of a service provided in the cloud another process “Feedback Collection” will be raised. For this reason, a feedback agent will be deployed on Provider. The agent will trigger the process by sending a Feedback request to user

- a. Authentication Method for collecting feedbacks.
- b. Previous interactions
- c. Feedback of Neighbors – Domain Based
- d. Old values, less weighted. Methods for renewal

4.3.7.2 Metric of Feedback Trust Value TF

Trust metric for feedback will be the feedback itself as described in previous

4.3.8 Access Point Security

4.3.8.1 Data input for Access Point Security

As trust management is part of security policy it is evident that security of access point – user’s computer, phone tablet etc. – should be considered as a factor of trust metric. A Security Evidence collector should be deployed on the Provider’s side. Providing that user agrees an agent will collect information regarding Security. A table will be maintained that will contain the following information:

- Antivirus used or not
- Firewall in Place
- Installation of Operating System’s Updates and Patches
- List of Software installed

Based on the previous a Security factor value will be assigned to every user as the average sum of the access point security measures deployed. As part of the security policy a threshold should be defined for Access Point Security. Devices with threshold under a specific limit should be rejected to enter cloud.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

4.3.8.2 Metric of Access Point Security Trust Value TAS

An access point security trust will be calculated as weighted sum of each input applying the same logic we had in previous. A weight will be defined for each input after a risk assessment at the initial configuration. A trust table with values will be defined for antivirus and firewall existence and which one, another factor for trustfulness is the required updates for the corresponding operating system and one for software installed that need to be reupdated periodically inserting updates and software.

An agent will check if antivirus and firewall is installed and which one specifically that will retrieve the corresponding trust value defined. Based on several reviews we define for now the following trust values but obviously this table need periodical update.

Table 24 Trust Value for Antivirus

Antivirus-Firewall	Trust Value $T_{\text{Antivirus}}$
Bitdefender	90
Norton	90
McFee	90
Kaspersky	90
Avast	90
Panda	90
Avira	90
Other Anti-virus/Firewall	70
No Antivirus/Firewall	20

The same logic applies to Operating System’s major updates. If the OS is updated trust value will be 90 and if not 20.

Last one is software installed on the access point. Here we decided that we will go upside-down. In other words, most trusted will be the access point that has no software we consider as suspicious. In the table below we have a list of suspicious software that will be updated periodically.

Table 25 Trust Value for Software Installed

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Software	Trust Value T_{Software}
None of the below	90
uTorrent, Vuze, Deluge, BitTorrent,	60
John the Ripper, Metasploit, Nmap, Wireshark, OpenVAS, IronWASP, Nikto, SQLMap, SQLNinja, Wapiti, Maltego, AirCracking, Reaver, Ettercap, Canvas, Sniper, Metasploit, Nessus	20
Dropbox, Angry Birds, Facebook, Microsoft OneDrive, Google Drive, Box, Whatsapp, Twitter, Skype, SugarSync	80
Brutus, RainbowCrack, Wfuzz, Cain and Abbel, THCHydra, Medusa, OphCrack, L0phtCrack	30

The relevant weights to calculate overall trust value is the one below:

Table 26 Proposed Weights of Trust for Access Point Security

Access Point Input	Weight in calculation of T_{AS}
$T_{\text{Antivirus}}$	35
T_{OS}	35
T_{Software}	30

Mathematical representation of previous is:

$$T_{AS} = W_{\text{Antivirus}} * T_{\text{Antivirus}} + W_{OS} * T_{OS} + W_{\text{Software}} * T_{\text{Software}}$$

4.3.9 Service Level Agreement

4.3.9.1 Data input for SLA

Depending on the type of organization that our model is applied one or more special factors can be included that is not in the above categories. For such kind of cases a relevant special monitor will be created that will collect the needed info. A custom table will be maintained with a corresponding security threshold defined in policy. User's or devices that are above the threshold should be rejected from cloud

4.3.9.2 Metric of SLA per special term Trust Value TSLA1, SLA2....

Per SLA special term a definition of trust metric should be included in the calculation of the total trust value after the implementation of risk assessment by a security professional.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

4.3.10 Total Trust Value

Overall Trust will be the weighted sum of the previous. The mathematical representation of the previous is:

$$T = W_{AP} * T_{AP} + W_L * T_L + W_{DA} * T_{DA} + W_R * T_R + W_A * T_A + W_F * T_F + W_{AS} * T_{AS} + W_{ST1} * T_{SLA1} + W_{ST2} * T_{SLA1} + \dots + W_{STn} * T_{STn}$$

4.3.11 Overall Trust Weights

Final step of parametrization of the proposed trust model is to define overall trust calculation weight per metric. In the table below we present the defined weights.

Table 27 Proposed Trust Weights for Overall Trust

Metric	Weight
Access Point	20
Geo-Location	20
Data access	20
Resources	15
Authentication	15
Feedbacks	0
Access Point Security	10
SLA	0

Above weights can again be changed base on the nature of cloud environments and the risk analysis result.

4.4 Applying the proposed trust model

The proposed trust model is applicable to any form of cloud IaaS, PaaS, SaaS and is fully configurable based on the nature of the organization. To demonstrate how the model applies in the below we will present the example of a University that rents a cloud server as Infrastructure as a Service to host an information system with information regarding its active students.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

4.4.1 University on IaaS

The server is accessed by academical personnel and students themselves. In order to apply the model, the necessary information was collected through the following template.

General Information	
Name of University	University of X
Responsible Person	XXX (<i>the name deleted for privacy reasons</i>)
Contact Information of responsible person	XXX (<i>the contact information deleted for privacy reasons</i>)
Name of Server	XXXXXX
Purpose of Server Usage	It is used to host an information system where all student's info is registered.
Data Sets	
Personal Data	Name, Surname, Date of Birth, Identity Card (personal and blood donor's), Father's Name, Mother's Name, Gender, Country of Birth, Address, Contact Information, email, Home Phone Number, Mobile Phone Number, National Insurance Number
Sensitive Personal Data	Diseases
University Characteristics	
Data Volume <ul style="list-style-type: none"> 1: Few 2: Many 	Value=2 Huge data volume, due to the number of students
Data Lifetime <ul style="list-style-type: none"> 1: No data is not kept at all 2: Data are kept for a specific period 3: Data are kept forever 	Value=2-20 years of data retention.
Data Type <ul style="list-style-type: none"> 1: Public Data 2: Private Data 3: Sensitive Personal Data 	Value=3-The university processes sensitive personal data.
Method of Data Collection <ul style="list-style-type: none"> 1: With written consent of subject 2: With electronic consent (e.g. accepting "terms and conditions") 3: Through another entity 	Value=1-The user's consent is given via a document, which the user signs.
Organization Size <ul style="list-style-type: none"> 1: Small-Medium Company 2: Large Company - Nationwide 	Value=2-Huge university with a host of users.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

<ul style="list-style-type: none"> • 3: Multinational company 	
Number of Users <ul style="list-style-type: none"> • 1: Under 100 users • 2: 100-1.000 users • 3: 1.000 users - ... 	Value=3-50.377 registered users
Legal Framework of country the organization is established <ul style="list-style-type: none"> • 1: Comply with the laws • 2: Deviations from Legal Framework exist 	Value=1-The university complies with the National legal framework (legal basis of data processing).
Legal Framework of country the organization operates <ul style="list-style-type: none"> • 1: Comply with the laws • 2: Deviations from Legal Framework exist 	Value=1-No cooperation with other countries. No transmission of data to third countries or international organizations.
Awareness / Culture of Employees <ul style="list-style-type: none"> • 1: They are aware • 2: They are not aware 	Value=1-University periodically does security awareness training to students and academical personnel.
Incident History <ul style="list-style-type: none"> • 1: Maintained • 2: Not maintained 	Value=1-The university preserves the history of security and privacy incidents. It is described in their security and privacy policy.
IaaS Characteristics	
Server	PowerEdge R640 Server
CPU	Intel® Xeon® Gold 5220S 2.7G, 18C/36T, 10.4GT/s, 24.75M Cache, Turbo, HT (125W) DDR4-2666
Memory	128GB LRDIMM, 2666MT/s, Octo Rank
Hard Disk	3.84TB SSD vSAS Mixed Use 12Gbps 512e 2.5in Hot-Plug AG drive,3 DWPD 21024 TBW

After collecting the required information regarding the usage of IaaS we started applying one by one the relevant metrics and at the same time decided that we will use the default for the weights as defined in previous section in trust value calculation.

4.4.2 Simulation Results

In the two tables below, we will present information regarding access information of a student and a malicious user as produced during the implementation. We suppose that at this stage our trust model is not used to forbid users from accessing IaaS. Below are the trust values with the relevant information collected.

Table 28 Trust Values of Student's Data

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Metric	Data Input	Trust Value
T _{DT}	Laptop not used in the past	80
T _{OS}	Windows 10	90
T _{AP}	$80\% * T_{DT} + 20\% * T_{OS}$	$64 + 18 = 82 / 1.25 = 65.6$
T _L	Distance from previous location=20km	60
T _{DAS}	User is logging in and is accessing data 10 mbs data regarding his remarks	100
T _{DATS}	The total session time deviation is 1 minute less than average	100
T _{DAM}	Student did not try to access data he did not have access to do so	100
T _{DA}	$40\% * T_{DAS} + 20\% * T_{DATS} + 40\% * T_{DAM}$	$40 + 20 + 40 = 100$
T _{RB}	Consumes 5mbps which is 0.01 above average	100
T _{RMU}	Consumes 35.7 Mb which is 0.01 above average	100
T _{RMC}	Consumes 33.4 Mb which is 0.02 above average	100
T _{RCPU}	Consumes 2.1% of CPU which is 0.7 above average	70
T _{RP}	Student uses port 138 and 443	$20\% * 30 + 80\% * 90 = 78$
T _R	$20\% * T_{RB} + 20\% * T_{RMU} + 20\% * T_{RMC} + 20\% * T_{RCPU} + 20\% * T_{RP}$	$20 + 20 + 20 + 14 + 16 = 90$
T _{AL}	Student had zero negative logins	100
T _{AT}	Student is using one-time passwords	75
T _{AW}	Authentication method used is correct	100
T _A	$30\% * T_{AL} + 60\% * T_{AT} + 10\% * T_{AW}$	$20 + 45 + 10 = 75$
T _{Antivirus}	Laptop has Avira installed	90
T _{OS}	Operating System is updated	90
T _{Software}	uTorrent is only installed on student's laptop	60
T _{AS}	$35\% * T_{Antivirus} + 35\% * T_{OS} + 30\% * T_{Software}$	$32 + 32 + 18 = 82$
T	$20\% * T_{AP} + 20\% * T_L + 20\% * T_{DA} + 15\% * T_R + 15\% * T_A + 10\% * T_{AS}$	$13 + 12 + 20 + 14 + 12 + 8 = 79$

Total trust value based on our model will be 79 for the student.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Table 29 Trust Values of Malicious User

Metric	Data Input	Trust Value
T _{DT}	Laptop not used in the past	72
T _{OS}	Windows 10	90
T _{AP}	$80\% * T_{DT} + 20\% * T_{OS}$	$64 + 18 = 82 / 1.25 = 65.6$
T _L	Distance from previous location = 2000km	10
T _{DAS}	User is logging in and is accessing data 1000 mbs data regarding highly restricted data and 600 mbs regarding restricted data	$60\% * 10 + 30\% * 50 = 21$
T _{DATS}	The total session time deviation is 70 minutes less than average	30
T _{DAM}	User tried to access unauthorized data 10 times	40
T _{DA}	$40\% * T_{DAS} + 20\% * T_{DATS} + 40\% * T_{DAM}$	$8 + 6 + 16 = 30$
T _{RB}	Consumes 30mbps which is 12 above average	50
T _{RMU}	Consumes 604 Mb which is 600 above average	40
T _{RMC}	Consumes 1500 Mb which is 1302 above average	10
T _{RCPU}	Consumes 30% of CPU which is 29 above average	10
T _{RP}	User uses port 137,138,139,1433	30
T _R	$20\% * T_{RB} + 20\% * T_{RMU} + 20\% * T_{RMC} + 20\% * T_{RCPU} + 20\% * T_{RP}$	$10 + 4 + 1 + 2 + 6 = 23$
T _{AL}	Malicious user had 20 negative logins	20
T _{AT}	Malicious user is using simple password	20
T _{AW}	Authentication method was not the correct one	20
T _A	$30\% * T_{AL} + 60\% * T_{AT} + 10\% * T_{AW}$	$6 + 12 + 2 = 20$
T _{Antivirus}	Laptop has Avira installed	90
T _{OS}	Operating System is updated	90
T _{Software}	Wireshark is only installed on user's laptop	20
T _{AS}	$35\% * T_{Antivirus} + 35\% * T_{OS} + 30\% * T_{Software}$	$32 + 32 + 6 = 70$
T	$20\% * T_{AP} + 20\% * T_L + 20\% * T_{DA} + 15\% * T_R + 15\% * T_A + 10\% * T_{AS}$	$13 + 2 + 6 + 4 + 3 + 7 = 35$

Total trust value based on our model will be 35 for the malicious user.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Chapter 5 : Personal Data Protection: Proposed Technical and Organizational measures for Cloud Providers

5.1 Introduction

Organization that provide cloud computing services need to provide technical and organizational rules that reassure personal and sensitive data protection. Recently a regulation came up to European Union members that require specific steps that lead to personal data protection. We used the regulation as guide and found specific measures for providers to comply and subsequently comply with personal data. The General Data Protection Regulation (GDPR) has a clear goal: to introduce a higher, more consistent level of personal data protection across the European Union, which will give citizens back control over their personal data and simplify the regulatory environment for business. The regulation, applies to all companies that hold or process EU residents' data, including cloud computing users, providers and their sub-contractors. The existing National legal framework, based on the 95/46 EU Data Protection Directive, has not achieved harmonization of personal data protection rules between member states. These variations, and at times conflicting rules, are complicating businesses' requirements and procedures, especially as data increasingly flows across borders in today's digital age. By implementing it as a regulation, the GDPR aims to ensure that the same data protection rules will apply uniformly across the EU. In addition, while many of the GDPR's concepts and principles have been based on the 95/46 Data Protection Directive, it introduces significant new rules and enhancements. The emphasis is on how personally identifiable information (PII) is handled and protected by institutions within the EU—and, in certain cases, outside the EU. For the cloud providers, the new obligations are extensive and challenging.

5.2 GDPR REQUIREMENTS

During the process of conforming to GDPR in cloud computing environments several requirements of the regulation should be considered, as presented in detail during the following sections [96].

5.2.1 Material and territorial scope

GDPR applies to cloud 'controllers' (who decide how and why personal data is processed) and 'processors' (who process personal data on controller's behalf). More specifically an EU based cloud

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

controller or processor should comply to GDPR requirements. To the previous add clouds which are not based in EU but offer services to European Union citizens or include monitoring actions that take place in the European Union.

As a check of whether a cloud needs to fulfill GDPR requirements or not, it is suggested to implement an audit-alert mechanism that will check if a cloud user (Software as a service) or the data uploaded/processed in the cloud (Infrastructure as a Service) falls under GDPR. When an alert is triggered specific automatic or/and manual actions with technical and organizational measures, as described below, should be taken to ensure GDPR compliance.

5.2.2 Data protection principles

Cloud providers must ensure the following GDPR principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability. More specifically the personal data of the data subject must be processed according to the law requirements, in a fair and transparent manner. The specific requirement highlights the need for the data controller to adopt privacy policies that are friendlier to data and thus promoting privacy rights. Cloud providers should collect, store and process personal data for specific and legitimate purposes, prohibiting any processing that lies outside the initial scope. The only window that GDPR leaves open for further processing is under the aspect of public interest and scientific research. Furthermore, to comply with the principle of minimization, personal data stored in cloud premises should be adequate, relevant and limited to what is necessary in relation to the purpose for which they have been collected. Cloud controllers must keep personal data accurate and up to date. When the data are not any more required, in relation to the initial processing purpose, they should be immediately erased, thus conforming to the storage limitation principle. Finally, integrity and confidentiality should be reassured to avoid unauthorized or unlawful processing or/and accidental loss, destruction, or damage.

To conform to the above cloud providers must maintain full documentation of personal data held, where it came from and with whom they are shared with, including the reason of processing. Data minimization should be considered in the organization and the purpose of collecting information should be defined in the security policy. Scheduled data reevaluation should be performed periodically. Furthermore, to ensure purpose limitation it is necessary to perform periodic audits to cloud clients and employees. Also, periodic data accuracy compliance checks should be done. Finally, vital for cloud providers is to apply storage limitation scan mechanisms and transfer restriction. To ensure integrity and confidentiality, data encryption, encrypted networks, firewall, data fragmentation, and anonymization techniques should be utilized. Pseudo

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

anonymization, a privacy enhancing technique, should also be implemented if possible, avoiding immediate linkability of data to the data subjects. In terms of accountability and lawfulness of processing, appropriate audit mechanisms on data operations (access, edit, delete, export etc.) are proposed to be implemented. The legitimate interest should be documented and included with accurate, clear and specific terms in the Service Level Agreement – SLA.

5.2.3 Consent

Cloud providers that collect / process any form of personal data need always a legal basis. In certain cases this legal basis can be the consent of the data subject. In other words, the cloud controller needs at any time to be able to demonstrate that the data subject has consented to the processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

The consent management mechanisms should be supported through some software application which will support the provision, updating, revoking and maintaining of users' consents. Restriction on clear and plain language consent should be included in order to be intelligible and easily accessible (e.g. native language of data subject). Alerting for updating the users' consents will be necessary when a change in the purpose or manner of personal data processing is happening.

5.2.4 Children – Parental Consent

In case that a cloud service is offered directly to a child under 16 years old, parental consent is required (Article 6(1)). The specific consent is considered to be lawful only if it is given or has been authorized by the holder of parental responsibility over the child. [53]

Cloud providers that have as users children, should enforce mechanisms for parental control. Alert mechanism that will require further actions should be implemented when a child is trying to use cloud or his parents are giving rights to store and process its data. After the alert is generated an authentication mechanism should be generated to make sure that the legitimate parent is giving the consent and the language of consents should be children friendly in order to make children's able to understand that parental approval is required. Software like the one described in 2.3 should be used but having also the above functions.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

5.2.5 Sensitive data and lawful processing

According to GDPR sensitive data are the ones revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for uniquely identifying a natural person
- Data concerning health or a natural person's sex life and/or sexual orientation

Cloud providers that collect/process such data categories should take further actions in order to satisfy GDPR requirements.

To this extend, the types of sensitive data that are processed should be identified and analytically described in the security policy of the cloud, providing also the reasoning for their necessity. In technical terms, it will be vital to implement a cloud-perimeter protection mechanism that will perform file and data scan, especially in cases of hardware as a service architecture where data storage is offered as a service. [56]

5.2.6 Information notices

Cloud providers must provide information through their privacy policy and/or upon request of the data subjects about the:

- Identity and contact details of the controller
- Data involved, purpose of processing and legal basis
- Recipient or categories of recipients
- Details of data transfer outside EU
- Data retention period
- Right of individuals

Regarding information notices a suggestion is to adopt some tool for generating and automatically sharing, template documents for the information notices, requests and responses.

5.2.7 Subject access, rectification and portability

Cloud providers should provide to the data subjects confirmation whether his/her personal data are being processed, access the data and supplemental information regarding rectification or reassurance, source of data and portability.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Full reporting and document templates are required. Techniques of alerts and corresponding deletion or non-availability of data that are subject to retention should be used. Cloud providers must be able to export data mechanism in a safe manner and in a common format/technology that can be widely adopted to support portability (e.g. xml, tab ,csv). They should also be able to provide mechanism for validity of the request of the data subject. Provide a mechanism to respond to requests on personal data access. Maintain the technological ability to trace and search personal data.

5.2.8 Rights to object

Cloud providers must give data owners the right to object against a data processing in an easy and safe way. In terms of technical proposal this can be converted to a mechanism applied for data subject objection and automated further actions.

5.2.9 Right to erasure and right to restriction of processing

Erasure or restriction of processing must be applied in cloud when any of the below is valid:

- Data are no longer necessary for the purpose for which they were collected or processed.
- Individuals withdraw their consent.
- Controllers cannot demonstrate that there are overriding legitimate grounds
- Unlawful processing.

When data are put in public domain the cloud provider need to notify the other controllers that the data owner want to restrict the access or that his data need to be erased.

Cloud providers must have in place special eraser software to make sure that data cannot be retrieved from the hard disk of storages. Also, in cases where the information is required to be kept for some period it is necessary to have restriction mechanisms in place that will not have available the information, blocking the data to a different system. [51]

5.2.10 Profiling and automated decision-taking

Profiling consists of three aspects: Automated processing (processing using computers) of personal data with the aim of evaluating personal aspects relating to a person or group of people (including analysis or prediction). The guidelines make it clear that the definition is very broad and that the processing does not need to involve inference to be caught – “simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose” (Deloitte 2018).. The guidelines describe profiling as having three distinct stages each of which fall within the GDPR definition of profiling: (1) data collection (2) automated analysis to identify correlations and (3) applying the

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

correlation to an individual to identify characteristics of present or future behavior. A decision based solely on automated processing is a decision with no human involvement in the decision process. The guidelines warn that involving a human in the process to circumvent the rules on solely automated decision making would not work, as the human involvement must be meaningful and not just a token gesture. The individual needs to have the authority to change the decision considering all the information available.

Individuals must be told when a decision has been taken solely using automated decision making and they must have the right to request a review of the decision. The review should be done by a person with appropriate authority and capacity to change the decision and should involve a thorough review of all relevant data and any additional information provided by the individual. Organizations using automated decision making should also carry out regular reviews and use appropriate procedures to prevent errors.

5.2.11 Accountability, security and breach notification

GDPR's article 24 codifies the accountability obligation. It requires controllers to:

- Implement appropriate technical and organizational measures (including the introduction of data protection by design and by default principles where relevant) to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR
- Review and update measures where necessary through notably internal and external assessment such as privacy seals. Those measures should take into account the nature, scope, context and purposes of processing and the risk to the rights and freedoms of natural persons.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Thus, cloud providers should have in place mechanisms for network protection, encryption and notification to the supervisory authorities and the data subjects. [42]

5.3 Countermeasures depending on the Cloud Architecture

5.3.1 GDPR Roles and Cloud Architectures

Cloud participants, in GDPR terms, can be separated into two main roles: the data processors and the data controllers. Most of the times, cloud providers act as data processors on behalf of their customers/users who are the data controllers.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

“Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.” (Article 4 – (8)) “Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”. (Article 4 – (7))

Cloud can appear in three main architectures/models:

- Infrastructure as a Service (IaaS): Provides hardware resources as computing facility, storage, memory etc. Known provider of IaaS is Amazon with EC2 and S3.
- Platform as a Service (PaaS): The term platform is related to systems (e.g. operating system) that can be used to develop and build custom applications. Known provider of PaaS is Microsoft Azure.
- Software as a Service (SaaS): Provides any type of software (application or service) through cloud. Known provider of SaaS is Salesforce.

In the following sections we will attempt to separate the countermeasures required depending on the cloud architecture.

5.3.2 Infrastructure as a Service

A cloud provider who offers Infrastructure as a service falls under GDPR, as most of the times acts as a data processor.

An IaaS cloud provider needs to support material and territorial scope in specific terms. More specifically, the storage location of personal data should be available at any moment, with full transparency, from the IaaS cloud providers[52]. It will be very useful to also support data transfer functionality and options for auditing the geographical flow of information [50].

An IaaS provider needs to have in place incident response mechanisms to promptly identify/respond incidents that create suspicion and indicate unauthorized access but only on the infrastructure level. Data protection principles are only partially applicable to IaaS cloud providers. An IaaS cloud service provider does not need to do anything about the lawfulness of processing since he has not a direct relationship with the data subjects, nor has knowledge on the data that his customer (data controller) has collected from the data subjects. However, they should have in place measures designed to identify the root cause of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Personal data processing should be done only for supporting GDPR purposes and to serve daily operation like security, attacks on systems networks, bots, administration of daily processes and comply with local legislations. The above processing can be shared with sub-contractors only if the IaaS publishes the list of subcontractors accompanied with full documentation and reasoning of sharing.

To support the transparency principle, audit mechanisms must be provided by cloud providers, recording in an automatic way the requested resources, the users and the sources of activity.

Purpose limitation in an Infrastructure as a Service cloud architecture can be supported by splitting the infrastructure into individual clusters. Cloud hardware resources provided to a data controller, should be isolated to avoid flow of personal data information. Cloud providers should also be able to offer to their customers the ability to create virtual cloud networks and thus facilitate communication between the isolated resources and at the same time supporting isolation from public internet.

Accuracy, from the side of an IAAS cloud provider, should be supported by offering relevant tools to their customers (data controllers). Software scanning must be enabled to actively monitor data content, integrity and automatically generate alerts to customer for malicious data. Encryption techniques can also help in the accuracy.

GDPR can support integrity and confidentiality to ensure that the appropriate security of personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage...” Article 5(1)(f). Hardware and network level access control in a cloud infrastructure is proposed to comply with GDPR with the concept of least privilege. Encryption on storage can also help in security of personal data applying encryption on block level, object level and metadata with separate keys and up to date technologies.

An IaaS is not obliged to have the consent of data subjects since they do not have direct relationship with the service offered. The same logic applies to parental consent. The only part that could be related to but without any required obligation is to take extra measures in the authentication process to mitigate the unauthorized access especially for non-adults.

In terms of Sensitive data an IaaS cloud provider should comply with all the aforementioned data protection measures and have in place a software for scanning data files in order to quickly identify sensitive information stored in their datastores.

Information notices is not an obligation of GDPR for cloud providers. Only for the offered marketing and client support services they could employ a mechanism for generating automatically templates for the documents that the cloud controllers need to provide to authorities and to data subjects.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Subject access rectification and portability falls under IaaS oligarchy to GDPR. IaaS providers must provide information regarding the data processed, the possible data transfers with the relevant recipients, including information regarding rectification and reassurance. To support this, providers needs to have in place mechanisms for supporting data portability through the appropriate export mechanisms.

The right to object, erasure and restriction is mostly relevant to cloud processors and not providers-controllers themselves. The only case that an IaaS provider may request a cloud processor to embed network restrictions and isolations for specific parts of the infrastructure is after a data subject objects to a cloud processor. Also, a software for secure erasure must be in place in the Infrastructure used. Profiling and automated decision-taking is out of scope for an IaaS Cloud provider.

Finally, an IaaS cloud provider is subject to accountability, security and breach notification. A cloud provider is obliged to have installed firewalls and network protection measures. Incident management mechanisms and procedures should also be in place to actively monitor potential data breaches in order to be able to notify the supervisory authority in 72 hours and to minimize the impact of the data breach. Standard certification of the infrastructures provided could help (e.g. ISO 27001).

Table 30 GDPR Requirements & IAAS Cloud Applicability

GDPR Requirement	Obligation
Material & territorial scope	Obligatory
Data protection principles	Obligatory
Consent	Recommendation
Children – Parental Consent	Recommendation
Sensitive data & lawful processing	Recommendation
Information notices	Recommendation
Subject access, rectification and portability	Provide information regarding the data transfers & information regarding rectification and reassurance
Right to object	Recommendation
Right to erasure & to restriction of processing	Recommendation
Profiling and automated decision-taking	Recommendation
Accountability, security and breach notification	Recommendation

5.3.3 Platform as a Service

Platform as a Service cloud providers should comply with GDPR. This Section describes, one by one, the measures that a PaaS provider must or should offer to its customers in order to comply with GDPR or to help them to do so in favor of shared responsibilities.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Analytic information regarding the geographical source, flow and process of information should be available from the PaaS provider at any time. This information should be available online, by mail alert and official documentation. Besides the informative part, PaaS providers must help their customer to maintain their data in specific geographic location accepting relevant terms in their SLAs [46].

Data protection principles should be maintained in a stricter way compared to IaaS cloud providers. PaaS helps cloud customers to protect and safeguard their data, including personal data, in support of organizational security commitments and GDPR compliance requirements. The employment of several service-level security measures for ensuring the confidentiality, integrity and availability of the processed data is strongly recommended. The security measures should be multilayered in physical, logical and data levels, indicatively including: 24-hour restricted access to datacenters, multiple authentication processes (such as badges, smart cards, and biometric scanners) for physical access, on-premises security guards, monitoring using video surveillance, motion sensors, and security breach alarms, automated fire prevention and extinguishing systems, access control lists, IPsec policies on hosts, restrictive firewall rules and host-based firewall rules, edge router security, network segmentation to provide physical separation of critical back-end servers and storage devices from public-facing interfaces, strict control of admin access to customer data, antimalware software, data isolation using Active Directory authorization, role-based access controls and workload-specific isolation mechanisms, use of encryption and other cryptographic security measure[52].

Data subject consent management is not a requirement that a PaaS cloud provider should comply with. Some big PaaS providers offer supporting tools to collect consent. Parental consent is also not required.

PaaS cloud providers must employ tools for sensitive data identification and relevant measures for classifying and protecting them. Data retention tools may be also necessary. Rule based controls could be also provided to alert the administrators of the cloud processor that a PaaS user stores information that has been classified as sensitive. Regarding sensitive data it is strongly recommended to have audit controls against global data privacy standards such as ISO 27018.

In terms of information notices, PaaS providers need to maintain full documentation of their platforms and of the security mechanisms they employ to support requests for information notices from authorities.

PaaS Cloud users maintain the right of access, rectification and portability under the enforcement of GDPR. All information hosted in PaaS environments must be exportable in a universal and readable way through tools that the cloud service provider will supply.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Right to object is also applicable to PaaS providers and they must provide tools for restriction of data storage, retention or deletion after the data subject objects.

Profiling and automated decision-taking is out of scope for a PaaS Cloud provider.

Furthermore, a PaaS cloud provider is subject to accountability, security and breach notification. In the security measures, it is imperative to include firewalls and network protection tools. Incident management should be also in place to actively monitor data breaches and thus to support the notification of supervisory authorities in 72 hours. Standard certification of the infrastructures provided could help (e.g. ISO 27001).

Table 31 GDPR Requirements & PAAS Cloud Applicability

GDPR Requirement	Applicability for Cloud Provider
Material & territorial scope	Analytic information regarding the geographical information should be available online, by mail alert and official documentation.
Data protection principles	Measures identify the cause of the Personal Data Breach, mitigate adverse effects and prevent a recurrence
Consent	Recommendation
Children – Parental Consent	Recommendation
Sensitive data & lawful processing	Must employ tools for sensitive data identification and relevant measures for classifying and protecting them.
Information notices	Maintain full documentation of platforms & security mechanisms
Subject access, rectification and portability	All information hosted must be exportable & readable
Right to object	Obligatory
Right to erasure & to restriction of processing	Provide tools for restriction of data storage, retention or deletion
Profiling and automated decision-taking	Recommendation
Accountability, security and breach notification	Include firewalls, network protection tools & incident management

5.3.4 Software as a Service

Under the GDPR, SaaS cloud providers face direct obligations relating to data processing activities. They will need to ensure that their product agreements with customers comply with the upcoming data regulations. Failure to do so could result in customers, their customer’s customers, and local data protection authorities imposing fines against them. The data controller and data processor coexist and they both have responsibilities, requirements and rights.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

A SaaS provider needs to maintain documentation of data location and information flow. It is proposed to have in place a mechanism that will generate alerts to software administrators when EU citizens are using the software to notify software owners that they should comply to GDPR [49].

Data protection principles to SaaS cloud providers apply to all layers of cloud from physical protection, infrastructure and up to software data protection. Measures regarding physical protection must cover unauthorized access of personnel in the data centers, including physical access control mechanisms like cards, cameras and biometrics. On network level, encryption mechanisms are suggested, and it is necessary to use firewalls, Intrusion Detection and Intrusion Prevention controls. Furthermore, network segregation is required, mac filtering and network access control. Storage encryptions techniques should be on level of hardware applying also on the same level software scan tools. On the software data level, the best practices proposed by global standards should be applied. Vulnerability assessments of the software and penetration testing must be periodically conducted. Software must include audit mechanisms to log and alert for data view, usage and edit with alert customization rules. It is also imperative to apply encryption between communication and storage levels in terms of database and hardware itself. Pseudonymization and anonymization is also proposed when applicable [47].

Software delivered in form of SaaS is not necessary to embed consent management techniques. It would be useful and probably recommended, but it is not obligatory since it is out of the scope of the software itself. The same applies to children consent but it would be useful to have a way for parental consent.

Sensitive data and relevant documentation of where it could be stored from software partition level, up to physical infrastructure required would be more than obligatory. It is also required to have in place encryption techniques and all the measures referred above on data protection levels.

In terms of information notices there is a need to maintain full documentation of their platforms and security mechanisms applied to support requests for information notices from authorities.

Subject access, rectification and portability must be fully documented by data controllers, but SaaS data processors must give to controller's tools to maintain this information. It is also imperative to have mechanisms for data export to support portability in universal formats.

SaaS providers should avoid profiling users based on their sensitive information whether these are directly collected from them or inferred as part of their undergoing automated profiling. Data minimization principle should drive service design as data controllers should be able to understand the minimum amount of data you will need for it. The best way for doing that is to consider Data Protection by Design and by Default, building services always examining what data are strictly needed, how to use them and why. Do not

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

experiment with algorithms and training models by collecting first data and then decide how to use them, but rather only use well tested models that you know will suffice to your scope, before deploying them [44] .

Accountability, security and breach notification notices should be raised from SaaS providers to let know the data controller about the leakage. Intrusion detection must be included in the infrastructure of SaaS and relevant DPO must react. Full documentation of data leakage and audit information should also be included.

Table 32 GDPR Requirements & SAAS Cloud Applicability




































GDPR Requirement	Applicability for Cloud Provider
Material & territorial scope	Maintain documentation of data location, information flow and alerts
Data protection principles	Measures on physical network and software level
Consent	Recommendation
Children – Parental Consent	Recommendation
Sensitive data & lawful processing	Sensitive data and relevant documentation of where it could be stored from software partition level, up to physical infrastructure required
Information notices	Maintain full documentation of platforms & security mechanisms
Subject access, rectification and portability	Provide information regarding the data transfers & information regarding rectification and reassurance
Right to object	Recommendation
Right to erasure & to restriction of processing	Recommendation
Profiling and automated decision-taking	Data minimization principle
Accountability, security and breach notification	Raised from SaaS providers to let know the data controller about the leakage

5.3.5 Comparative analysis

GDPR compliance varies according to the nature of the cloud service provided (SaaS, PaaS, IaaS) and the role that the cloud provider has (data controller and data processor).







Starting with data processors and based on the analysis we presented in the previous sections we summarize our results to the comparative table below.

Table 33 Recommended and Obligatory measures for data processors

Requirements	IaaS	PaaS	SaaS
Material & territorial scope			
Data protection principles			
Consent			
Children – Parental Consent			
Sensitive data & lawful processing			
Information notices			
Subject access, rectification and portability			
Right to object			
Right to erasure & to restriction of processing			
Profiling and automated decision-taking			
Accountability, security and breach notification			
 Recommended/ Obligatory  Recommended			

The following table provides a summary of the requirements for cloud providers acting as data Controllers separated on the type of service.

Table 34 Recommended and obligatory measures for data controllers

Requirements	IaaS	PaaS	SaaS
Material & territorial scope			
Data protection principles			

Consent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Children – Parental Consent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive data & lawful processing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Information notices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Subject access, rectification and portability	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Right to object	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Right to erasure & to restriction of processing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Profiling and automated decision-taking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Accountability, security and breach notification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Recommended <input type="checkbox"/> Obligatory			

5.4 Conforming to GDPR in a PaaS environment.

The proposed GDPR measures, as described in the previous sections, are the necessary ones for conforming to the GDPR. To demonstrate this we have applied them in a PaaS environment that offers services for building, testing, deploying, and managing applications through cloud managed data centers.

5.4.1 Details for the provider and its deployment

The provider is based in a European country and his clientele spreads all over the globe. He offers services for application vendors that do not want to invest in hardware and software for development, testing, deployment and back up infrastructure. He also offers the relevant security measures for safeguarding the systems. Currently he serves about 2500 clients all over EU with several types of software. In the next sections we will provide an analytic description of the necessary measures for helping the provider or/and his customers to comply with GDPR.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

5.4.2 Material and territorial scope

During the implementation of material and territorial scope we installed on the provider's datacenters software that triggers an alert every time a cloud user tries to connect to the cloud. The previous takes as input the user's assertion for his origin, the user's location and the data content that that user uploaded or edited. If any of the previous indicates an EU citizen, the security team of the PaaS infrastructure will employ the following countermeasures in any of the actions of the specific user within the cloud.

5.4.3 Data protection principles

For ensuring that the cloud provider conforms to GDPR, regarding the data protection principles, we check them one by one and apply relevant security measures. First of all, it is necessary to understand what kind of data they collect and to update the documentation with information on the kind of the personal data, their source, to whom and the reasoning of sharing and processing. We also used known data minimization techniques to remove unnecessary data stored in their hardware and to ensure that the data collected is clearly defined and documented in the security policy. We also applied a mechanism for performing document data reevaluation and used the same mechanism to audit cloud clients and employees. Through their domain controllers we applied storage limitation and transfer prohibition. Provider changed his networks to support SSL/TLS to have data transferred encrypted and made tighter the firewall rules. Furthermore, data were separated to support unlikability and anonymization.

Furthermore, in order for the provider to satisfy the GDPR requirements of accountability and lawfulness of processing, appropriate audit mechanisms were implemented including all the information regarding activity, resources, active directory reporting, operating system logs, storage analytics, process data and security alerts.

5.4.4 Consent

PaaS cloud provider employed a consent management system, including procedures for giving, revoking and updating consent of his customers to fully support consent lifecycle. The provider maintains an up-to-date and complete record of consent, including detailed information on the subject of consent, the timeline, method of consent, validity period and record deletion after the expiration date.

5.4.5 Children – Parental Consent

Since the clients of the specific cloud provider can be children, the requested consent requires a digital signature in order to validate the date of birth of the parent.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

5.4.6 Sensitive data and lawful processing

After an analytic investigation the PaaS provider updated its security policy with a detailed description of the data processed. Also, he has employed special software for scanning files and data for information that could be classified as sensitive.

5.4.7 Information notices

In cooperation with the Data Protection Officer we have audited existing information notices and updated them with the following information:

- The name and contact details of the organization, its representative, and its Data Protection Officer
- The purpose of processing of individual's personal data and its legal basis
- The legitimate interests of the organization (or third party, where applicable)
- Any recipient or categories of recipients of an individuals' data
- The details regarding any transfer of personal data to a third country and the safeguards taken
- The retention period or criteria used to determine the retention period of the personal data
- The satisfaction of all data subjects' rights
- The right to withdraw consent at any time (where relevant)
- The right to lodge a complaint the supervisory authority
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data
- The existence of an automated decision-making system, including profiling, and information about how this system has been set up, the significance, and the consequences

5.4.8 Subject's access, rectification and portability

To support subject's access, rectification and portability rights, we reviewed customer support's processes, procedures and training. We have supported the process by developing template response letters, formatting capabilities, and exporting data in structured, machine readable formats. Finally, we developed data subject access portals, to allow direct exercise of subject access rights.

5.4.9 Right to erasure and right to restriction of processing

The PaaS cloud provider complied with this GDPR article by extensive training of its staff and its suppliers in order for them to recognize erasure requests and know how to deal with them.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

5.4.10 Profiling and automated decision-taking

The PaaS provider is not applying any profiling and automated decision-taking.

5.4.11 Accountability, security and breach notification

To satisfy the aforementioned GDPR requirements several technical measures, as described below, have been employed:

An access control policy has been defined and is being enforced by the appropriate access control mechanisms. An IT person is responsible for assigning access rights to systems, applications and information. The same person is also responsible for revoking or modifying rights based on the defined access control policy. A ticket management system has been also implemented to track all requests and changes. This enables traceability. Furthermore, it is mandatory for the PaaS provider to actively monitor all critical IT infrastructure components and alarms triggered when unexpected behavior is being detected.

The data centers of the PaaS cloud provider should exhibit physical access control through biometric tokens.

Encryption has been applied to hard disks, storage media, backup data and any other media used for any kind of sensitive data. Encryption should also be applied during communication of sensitive data. To ensure that encryption is not vulnerable, we have decided that the encryption keys required will be handled by staff with special authorization only.

To avoid security breaches due to malicious code, the appropriate antivirus scanners and spam filters have been employed. Furthermore, procedure have been established for performing security updates and training using active monitoring to ensure that antivirus scanners and spam filters are active and updated.

Finally, a breach notification procedure has been established for notifying the supervisory authority or/and the data subjects if a security breach occurs.

5.4.12 Results of conforming

The PaaS GDPR compliance is a demanding process where several issues need to be addressed and resolved. In the previous section we have addressed each of them and implemented a GDPR compliant solution giving details per requirement. It is inevitable that further actions and relevant updates will be necessary in the future in order to maintain compliance status.

Chapter 6 : Utilizing a Privacy Impact Assessment Method using Metrics

6.1 Introduction

In order to prevent privacy breaches, several laws, standards, regulations and directives [58] have been applied to most developed countries. The intent is to compel organizations to fully inform their users and obtain their prior consent before collecting, storing or processing their personal data in any way. At the same time, privacy principles [59], privacy requirements and security requirements [60],[61] are also helpful since they assist the development of an integrated security and privacy protection framework.

In cloud computing environments end-users have little or no knowledge of the physical location of their data, of the processing processes of cloud providers and of the security measures taken. Therefore, Cloud computing raises a vast number of privacy related concerns in terms of provider trustfulness, personal data protection, data loss and data breach. A privacy breach would have tremendous results to data security, legal compliance, user trust and overall cloud reputation. In order to facilitate the selection of the appropriate privacy protection measures in cloud computing environments we propose the adoption of a Privacy Impact Analysis that has been developed in collaboration with other researchers of the Systems Security Lab, as presented in following sections [92],[96].

6.2 Literature Review

In the advent of computer science era, individuals use computers on a daily basis to satisfy their “digital needs”, for instance to perform electronic transactions via the net. To do so, they do not hesitate to provide the personal data required for accessing the applications. Yet, can people be really protected when they “offer” their personal data so willingly? To answer this question, it is first necessary to estimate the consequences from a potential privacy breach, employing a *Privacy Impact Assessment (PIA)* method. Having estimated the impact, the stakeholders may adopt remedial actions for eliminating or minimizing the consequences [62]. Furthermore, failure to apply a PIA method may result in a breach of privacy laws - regulations.

Considering the aforementioned PIA benefits, it can be inferred that through the application of a PIA method the most widely known privacy principles are maintained. In 1980 [59] the OECD organization proposed eight privacy principles, which were globally accepted, namely: purpose specification principle, collection limitation principle, data quality principle, use limitation principle, openness principle, individual

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

participation principle, accountability principle, security safeguards principle. Their aim was to minimize the risk of personal data disclosure and consist the basis of privacy protection [68] Ann Cavoukian [69],[70],[71] strongly supports the notion of privacy-by-design, according to which privacy should be maintained throughout the entire lifecycle of an IT system, from the conception of a new system up to its implementation. According to Oetzel and Spiekermann [72],[73] the notion of privacy-by-design is really important in a PIA method as PIAs try to follow these privacy principles in order to achieve privacy-by-design, which is one of the most crucial concerns of today's privacy community.

The idea of a PIA method is relatively new. Its evolution is presented in [92] while more information can be found in [63],[64],[65],[66],[67],[72],[73],[74],[75],[77],[79],[80],[82],[83],[84],[85],[88].

Throughout the years, the rapid improvement of PIA methodologies highlights their importance on privacy and data protection. However, there is no explicit way to quantify the privacy impact. In 2011, David Wright [80][84] highlighted this need, by stating that "*Making privacy impact assessments mandatory is not the end of the story. Audits and metrics are needed to make sure that PIAs are actually carried out and properly so and to determine if improvements to the process can be made*". More recently, in 2013, Kush Wadhwa and Rowena Rodrigues [81] agreed with David Wright's statement, which practically means that the specific need still exists.

In July 2016, Sushant Agarwal [82] highlighted the fact that although there are a series of modular and well-structured online PIA tools (GS1 tool, iPIA tool, SPIA tool, etc), they all fail to provide a metric to assess progress in the implementation of privacy controls. In his research, he developed a structured metric to measure privacy risk. Before Agarwal, Oetzel and Spiekermann [69],[70] had already proposed a qualitative metric (low, medium, high) for measuring privacy risks, but their effort was quite unstructured and difficult to measure explicitly [82] In order to evaluate privacy risk, Agarwal defined it as the product of impact and likelihood. To be more specific, Agarwal assessed the impact using Solove's taxonomy and the likelihood using Lipton's work. For the calculation of the impact, he used four different dimensions of privacy, splitting them into categories and subcategories. For the likelihood, he used actors (companies, 3rd parties, others) and data characteristics (amount of data, sensitivity of data, value of data involved). This paper proposed a structured privacy risk metric, but failed to delve deeper into the organizations' characteristics which can have a considerable negative impact on the users' privacy.

In June 2015, Commission Nationale de l'Informatique et des Libertés (CNIL) published a PIA methodology, which is in line with EU's General Data Protection Regulation (GDPR) [58] According to CNIL [90] the PIA methodology rests on two pillars: firstly, the fundamental principles and rights and, secondly, the management of data subjects' privacy risks. To be more specific, the methodology consists of

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

four steps: the definition and description of the content of the processing of personal data under consideration, the identification of existing or planned controls, the evaluation of privacy risks and the decision to validate the manner in which it is planned to comply with privacy principles and treat the risks, or review the preceding steps. In December 2017, CNIL published a free and open source PIA software [91] in order to help data controllers to follow their methodology.

In conclusion, it can be inferred that an effective way to measure the privacy impact is by using metrics. Metrics can help organizations to calculate the significance of threats and lead them to take measures to mitigate the risks. Despite the remarkable efforts to define metrics by various researchers [73][74][86], so far, there has been no detailed PIA method to use metrics and, at the same time, take into account the organization characteristics. Furthermore, there is no method that integrates security and privacy assessment.

6.3 The Proposed Security and Privacy Impact Assessment Method

6.3.1 Scope of the Proposed Method

The proposed method aims to assist cloud providers to protect the privacy of their users and the security of the data that they store and process. Users may be the customers of the organization (people using the offered services) or the employees (users who operate the systems of the organization).

The novelty of the method is that it handles security and privacy requirements simultaneously, since it utilizes the results of risk analysis together with those of a PIA. A further novelty of the method is that it introduces metrics for the quantification of the requirements and also that it takes into account the specific characteristics of the organization.

It should be stressed that we do not aim to propose a specific method for information security or privacy risk management, but instead to allow an organization to utilize an existing methodology for risk management and privacy impact assessment while, at the same time, to facilitate the integration of the derived security and privacy requirements with the privacy principles dictated by the legal and regulatory framework. All of that in the context of the specific organization (i.e. taking into account the specific characteristics, perceptions and wills of the organization). As demonstrated in Figure 4 below, independent methodologies for the elicitation of the security and privacy requirements can be utilized producing the risk factor (both in terms of security and privacy) for the system assets. This risk factor ‘feeds’ the proposed method (through the security safeguards principle) in order to calculate the overall criticality for the specific organization (taking into account the privacy principles and the organizational characteristics).

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Our approach is therefore very similar to the one of ISO 27005 that does not provide any specific method for information security risk management but it simply allows the organization to adopt any methodology under the framework of the standard.

6.3.2 Theoretical Background

6.3.2.1 Data Sets Definitions

A huge amount of data is stored and processed in information systems and/or portable devices such as mobile phones or tablets. However, the criticality of the data is not always the same. For instance, some applications may only use publicly available data, others may involve personal data (like names, addresses etc.) and others may also process sensitive data (like health data). Clearly, its case exhibits different criticality and must be handled differently [91] To facilitate that, through the proposed method, the data that an organization stores/process either internally (e.g. employees' data) or externally (e.g. users' data) are classified [90] the following categories [

- **Personal Data** (e.g. name, surname, age, address, telephone number, email, education, etc.)
- **Sensitive Personal Data** (e.g. racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, etc.)
- **Operational Data** (e.g. logging users' actions, etc.)
- **Financial Data** (e.g. data related to the payroll of the organizations' employees, data related to payments by organization's users for the provided services)
- **Other Data** (e.g. any data that cannot be classified in any of the above categories)

6.3.2.2 The Role of Privacy Principles, Privacy and Security Requirements

The privacy principles together with all privacy requirements, must be satisfied by the organization in order to claim "privacy-preserving" services. Undoubtedly, equally important is the satisfaction of the security requirements. In [60], an integrated methodology for facilitating organizations to specify the appropriate security and privacy preserving measures for their information systems has been proposed (depicted in Figure 4). More specifically, Figure 4 identifies the steps that the organization should go through in order to identify the security and privacy requirements, for the system under study, taking into account the privacy principles, as well as the stage at which the organization should select the appropriate safeguards for satisfying the

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

aforementioned requirements. Clearly, the selection of the safeguards is based on the identified security and privacy requirements and, in fact, comes to satisfy the “Security Safeguards” Principle.

In addition to that, in [61] a four-level classification of the existing privacy principles, based on their significance and on the sequence that a potential audit procedure should be carried out, has been proposed (depicted in Figure 5). All the steps are interdependent and should be followed in strict order since failure to audit any step implies that it is meaningless to continue the audit procedure. At the same time, it has been identified that there is need for certain privacy principles to be maintained throughout the entire auditing procedure.

More specifically, the first step is the most important one since the “Purpose Specification Principle” defines the scope of data collection and use. If this privacy principle is not satisfied the other privacy principles will not be applied in the right way, violating the data privacy. The second step includes the satisfaction of “Data Collection Limitation Principle” and “Data Quality Principle”. If the purpose from the step 1 has been specified, the data collection and use must be limited and related to the purpose.

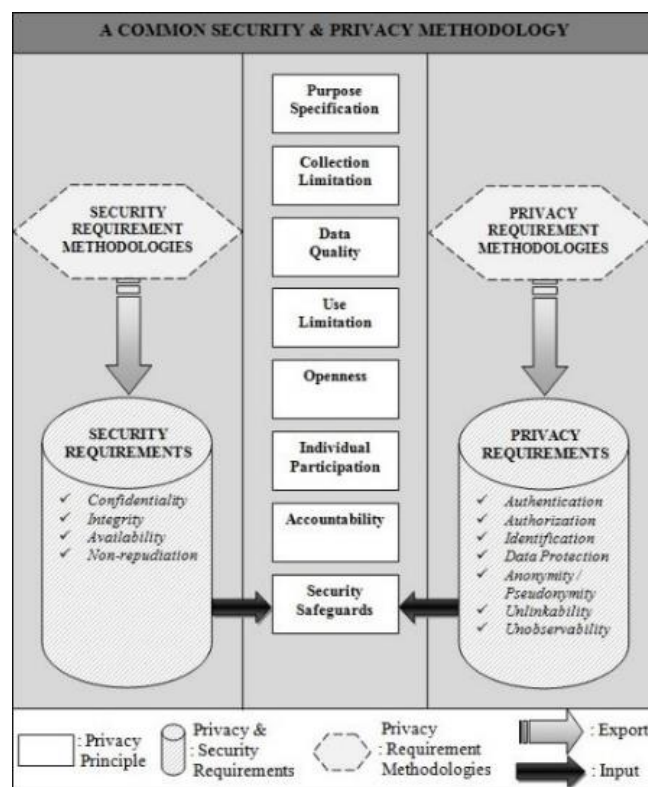


Figure 4: A Common Security and Privacy

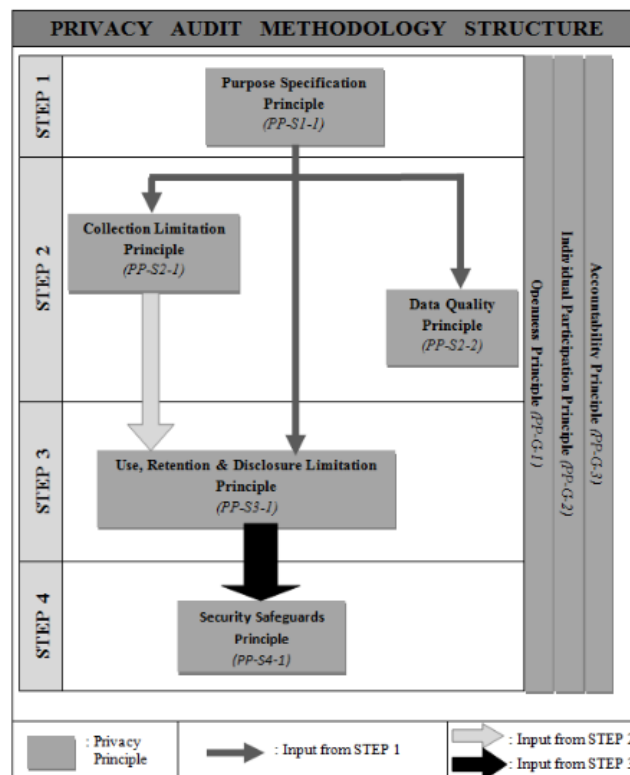


Figure 5: Privacy Audit Methodology Structure Methodology

Moreover, the collected data should be accurate and kept updated. If these privacy principles are not satisfied the upcoming privacy principles will not be applied in the right way, violating the data privacy. The third step includes the satisfaction of “Use, Retention and Disclosure Principle”. If the privacy principles from the step 2 have been satisfied, the data should be limited used, retained and disclosed according to organizations’ policies. If the privacy principle in the third step is not satisfied the upcoming privacy principles will not be applied in the right way, violating the data privacy. The fourth and last step includes the satisfaction of “Security Safeguards Principle”.

The other privacy principles include the satisfaction of “Openness Principle”, “Individual Participation Principle” and “Accountability Principle”. These privacy principles should be satisfied throughout the entire methodology.

Based on the hierarchy of the steps (as depicted in Figure 5), Step 1 is the most important one, Step 2 is more important than Step 3 and Step 3 is more important than Step 4. The other privacy principles should be applied throughout the entire process.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

6.3.3 Quantification of Security and Privacy Requirements

In order to facilitate auditors to “measure” the degree to which security and privacy requirements have been addressed by an organization, it is necessary to introduce metrics that will be utilized for the quantification of the requirements. The proposed method introduces metrics that have been based on the type and severity of the security and privacy requirements for the information system, the criticality of the data sets involved, the applicable privacy principles and the characteristics of the organization.

6.3.3.1 Security Requirements and Data Sets’ Sensitivity

The main criterion for determining the criticality of a security incident and thus the potential consequences for the organization, is the sensitivity of the data maintained and processed. Clearly, the weight of the security requirements depends on the sensitivity of the data sets; i.e. more sensitive data raise *harder* security requirements. On a second level, in order to judge the sensitivity of the data it is essential to identify all the different subsets (subcategory) of data and valueate independently each one of them. A description of the identified valuation metrics follows.

Metric 6.3.3.1.1 The sensitivity of each data subcategory

Description of Metric: The sensitivity of each data subset will be estimated through the use of a risk analysis method, like CRAMM [88] The outcome of the risk analysis will be a numeric value known as risk factor. The classification of data to different subcategories will be based on the fact that all data belonging to a specific subset should exhibit a similar sensitivity level for the organization. Some indicative data subcategories are:

- Personal Data (Data which uniquely identify a person using IDs, personal or marital status, business activities etc.)
- Sensitive Personal Data (Medical Data, convictions etc.)
- Financial Data (Data related to financial transactions, yearly tax etc.)
- Operational Data (Data generated during the execution of a service, i.e. cookies, private log files of the organization etc.)
- Other Data

As already mentioned, the estimation of the organization’s data sensitivity, through risk analysis, will be based on the impact that could be caused to the organization by a potential security incident on an independent data subcategory. The overall impact for the organization will depend on the partial impact caused by each data subcategory, adopting in all cases the worst-case scenario.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Input to Metric: The organization's Data Set, classified in data subcategories DS1, DS2 ... (DSn).

Formulation: Through Risk Analysis the risk factor for each data subcategory is calculated, depending

Level 1 – Very Low : Minimal impact (Risk Factor Value = 1)

Level 2 – Low : Small Impact (Risk Factor Value = 2)

Level 3 - Medium : Medium Impact (Risk Factor Value = 3)

Level 4– High : Significant Impact (Risk Factor Value = 4)

Level 5– Very High : Organization's viability in danger (Risk Factor Value = 5)

on the impact that a security incident could cause to the organization.

Final Output: A metric "SeveritySubCatDSx" for each data subcategory x (where $x=1,2,\dots,n$) is calculated, representing the impact that could be caused for the organization by a security incident that affects the data subcategory DSx.

Metric 6.3.3.1.2: The overall data set's sensitivity

Description of Metric: The overall sensitivity (risk factor) of the organization's data, calculated through the risk factors of each independent data subcategory (metric 6.3.3.1.1). The way to calculate the overall sensitivity is the following:

- If all organizational data have been classified in one category the overall sensitivity will be equal to the sensitivity of that specific data category.
- If the organizational data have been classified in several data subcategories, the overall sensitivity of organizations' data will be equal to the maximum sensitivity of the data subcategories. This is because the maximum sensitivity level covers all data subcategories.

The above calculation principle is depicted in Figure 6.

Input to Metric: The severity of each data subcategory (Metric 6.3.3.1.1)

Formulation:

$SeverityDS = \max (SeveritySubCatDS1, \dots , SeveritySubCatDn)$

Cases:

if (n=1) then $SeverityDS = SeveritySubCatDS$

if (n=2) then $SeverityDS = \max (SeveritySubCatDS1, SeveritySubCatDS2)$

if (n=n) then $SeverityDS = \max (SeveritySubCatDS1, \dots , SeveritySub-CatDn)$

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Final Output: A metric “Severity DS” is calculated, representing the overall severity of the organization’s data.

If the organization has several distinct data sets, each one divided in different data subcategories, the above Severity DS metric will be computed separately for each data set. The risk treatment process will start considering the data set that exhibits the biggest severity first, and then the data sets with smaller severities.

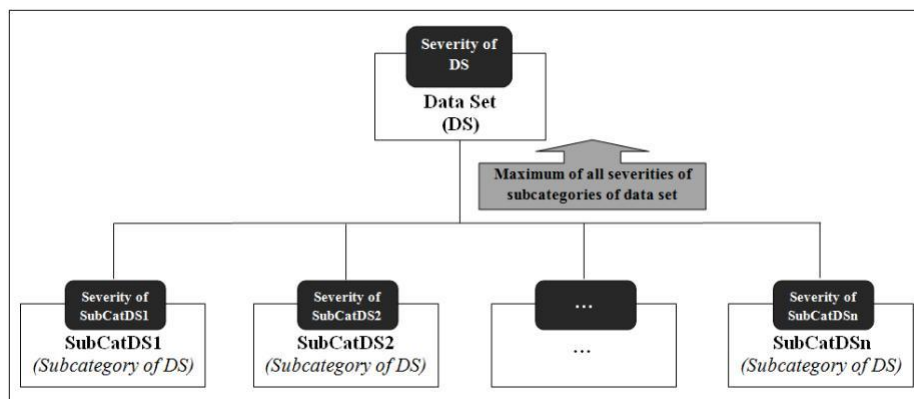


Figure 6: The overall Data Set Sensitivity

6.3.3.2 Privacy Requirements and Principles

In addition to the security requirements, it is important to consider and quantify the privacy requirements. For the purposes of this thesis, we assume that the privacy requirements have been considered together with the security requirements, thus covered by the already defined metrics, and thus here we simply evaluate the related privacy principles. As explained in [60], [61] the privacy principles are classified in a hierarchy of steps (Figure 4, Figure 5). Metrics, estimating the impact for the organization, in cases where one or more steps are not satisfied, will be defined.

The definition of these metrics is much more complex, as compared to the ones used for the data sets’ sensitivity. More specifically, the metrics for the privacy principles depend on the hierarchical level (step) of the principle, which is a constant value, and on the characteristics of the organization, which is a variable that depends on the organization type and activities.

Metric 6.3.3.2.1: Hierarchical Level of each Privacy Principle

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Description of Metric: The privacy audit method proposed in [61] has predefined steps. The specific metric reflects the criticality of the hierarchical level that a privacy principle belongs to, the most critical being Step 1.

Input to Metric: The hierarchical levels (steps) of the privacy audit method proposed in [61].

Formulation: According to the hierarchical level (step) that a privacy principle is associated with, a constant weighting factor “app” (where pp = privacy principle) is given to the principle. The weight reflects the importance of the specific step, and thus of the privacy principles associated with it, for the organization. The minimum weighting factor has been assumed to be 1. In addition, the weight associated with each step highlights the *criticality difference* among the various privacy principles. More specifically:

Step 1 – PP of very high importance (Weighting factor = 3)

Step 2 – PP of high importance (Weighting factor = 2)

Step 3 – PP of medium importance (Weighting factor = 1)

Step 4 – (Weighting factor = Severity DS)

The weighting factor for the Security Safeguards Principle (Step 4) is the only one that is not constant and thus not aligned with the hierarchical level that the principle is associated with. The reason is that the importance of the specific principle largely depends on the severity of the data set under consideration which is reflected by the Severity DS value (Metric 6.3.3.1.2) calculated through the risk analysis/PIA.

Horizontal Steps – PP of high Importance (Weighting factor = 2)

Final Output:

A metric “app - Weighting Factor” for each Privacy Principle, which is:

- ✓ Weighting Factor for the Purpose Specification Principle = 3
- ✓ Weighting Factor for the Collection Limitation Principle = 2
- ✓ Weighting Factor for the Data Quality Principle = 2
- ✓ Weighting Factor for the Use, Retention and Disclosure Principle = 1
- ✓ Weighting Factor for the Security Safeguards Principle = Severity DS
- ✓ Weighting Factor for the Openness Principle = 2
- ✓ Weighting Factor for the Individual Participation Principle = 2
- ✓ Weighting Factor for the Accountability Principle = 2

Metric 6.3.3.2.2: Organizational Characteristics

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Description of Metric: Each organization has its own type, activities, peculiarities etc. These characteristics may affect the potential impact / consequences for the organization in case of a privacy violation incident.

A vector “z1..N” is being used for modelling the organization’s characteristics. Each characteristic has its own scale, depending on how it affects the organization in case of a security or privacy violation incident. For instance, the characteristic “Data Volume” has importance α if the organization manages a very low volume of personal data, while its importance is β (where $\beta > \alpha$) if the organization maintains and processes a considerable amount of sensitive data.

Input to Metric: The characteristics of the organization.

Formulation: According to the organization’s characteristics a vector will be used to assess their impact on the security and privacy issues.

z1..N = [a numeric value for CH1 from the range: **Value1 Value2 ... ValueN**] [a numeric value for CH2 from the range: **Value1 Value2 ... ValueN**]

[...]

[a numeric value for CHN from the range: **Value1 Value2 ... ValueN**] where: indicative CHs and VALUES are presented in Table 33 next.

Table 35. Indicative Characteristics and Values of the Organization

No	CH1,2...N	RANGE OF VALUES
1	Data Volume	1: Few
		2: Many
2.	Data Life Time	1: No data is not kept at all
		2: Data are kept for specific period of time
		3: Data are kept forever
3.	Data Type	1: Public Data
		2: Private Data
		3: Sensitive Personal Data
4.	Way of Data Collection	1: With written consent of subject
		2: With electronic consent (e.g. accepting “terms and conditions”)

		3: Through another entity (legal or illegal)
5.	Organization Size	1: Small-Medium Company
		2: Large Company – nationwide
		3: Multinational company
6.	Number of Users	1: Under 100 users
		2: 100-1.000 users
		3: 1.000 users - ...
7.	Legal Framework of country the organization is established	1: Comply with the laws
		2: Deviations from Legal Framework exist
8.	Legal Framework of country the organization operates	1: Comply with the laws
		2: Deviations from Legal Framework exist
9.	Awareness / Culture of Employees	1: They are aware
		2: They are not aware
10.	Incident History	1: Maintained
		2: Not maintained

Final Output: A metric “Vector $z_{1..N}$ ”, providing the importance of each organizational characteristic.

Metric 6.3.3.2.3: Customization of Organizational Characteristics

Description of Metric: The Vector $z_{1..N}$ metric, defined above, provides a generic assessment of the way various organizational characteristics may influence the impact on the organization, in case of a privacy violation incident. However, each organization may, depending on the data that it processes and the type of its activities, judge the importance of each characteristic differently. To allow each organization to customize the importance of its characteristics, a *priority percentage* is given to each characteristic.

Input to Metric: Vector $z_{1..N}$ (Output of metric 6.3.3.2.2)

Formulation: Applying the *priority percentages* in Vector $z_{1..N}$ a new metric is derived:

$$k_i = \text{Priority percentages} * \text{Vector } z_{1..N}$$

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

Example:

$$ki = (20\% * CH1) + (18\% * CH2) + (15\% * CH3) + (12\% * CH4) + (10\% * CH5) + (8\% * CH6) + (6\% * CH7) + (5\% * CH8) + (4\% * CH9) + (2\% * CH10)$$

where: CH1,2,...,10: Characteristics 1,2,...,10 (e.g. Data Volume, Data Type, etc)

Final Output: *A metric “ki” is defined, representing the customized (specific to the organization) criticality of its characteristics on privacy issues.*

Metric 6.3.3.2.4: Severity of Privacy Principles

Description of Metric: The severity of each distinct Privacy Principle depends on two factors: the “*app - Weighting Factor*” for each Privacy Principle (section 6.3.3.2.1) and the criticality of the organizational characteristics (metric “ki” defined in section 6.3.3.2.3).

Input to Metric: The “app” weighting factor, the “ki” metric

Formulation: The value of “*Severity PP*” metric is calculated from the “app” weighting Factor and the “ki” metric.

$$Severity\ PP = app * ki$$

Final Output: *A metric “Severity PP”, representing the overall severity of each privacy principle.*

6.3.4 The Proposed PIA Method

Having defined the aforementioned metrics, it is now possible to use them in order to deduce the criticality of each privacy principle for every different data set of the organization. The value of each *Table Cell* in the following table is calculated in accordance to the following formula:

$$Table\ Cell = Severity\ DS + Severity\ PP$$

It should be stressed that the derived table cell value for a specific privacy principle and a specific data set, will not be necessarily the same for different organizations, since it depends on the calculated ki value which is related to specific organizational characteristics.

Table 36. The Proposed PIA Method

	Severity DS	[1...7]	[1...7]	...	[1...7]
Severity PP = $a_{pp} * k_i =$	Data Sets	DATA SET 1 <i>SeverityDS1</i>	DATA SET 2 <i>SeverityDS2</i>	...	DATA SET N <i>SeverityDSn</i>
	Privacy Principles	<p align="center"><u>LEVEL OF PRIVACY & SECURITY CRITICALITY</u></p> <p align="center">Range of values for each <i>Table Cell</i> = [(Severity DS_i) + ($a_{pp} * k_{i_{min}}$) ... (Severity DS_i) + ($a_{pp} * k_{i_{max}}$)]</p>			
[9] * k ₁	Purpose Specification Principle <i>SeverityPSP</i>				
[7] * k ₂	Collection Limitation Principle <i>SeverityCLP</i>				
[7] * k ₃	Data Quality Principle <i>SeverityDQP</i>				
[5] * k ₄	Use, Retention and Disclosure Limitation Principle <i>SeverityURDLP</i>				
[3] * k ₅	Security Safeguards Principle <i>SeveritySSP</i>				
[7] * k ₆	Openness Principle <i>SeverityOP</i>				
[7] * k ₇	Individual Participation Principle <i>SeverityIPP</i>				
[7] * k ₈	Accountability Principle <i>SeverityAP</i>				
<i>Where:</i>					
<ul style="list-style-type: none"> • Severity DS (risk factor for each data set) • Severity PP (privacy principles, privacy and security requirements, characteristics of the organization) • Severity PP = $a_{pp} * k_i$ • a_{pp} = weighting factor of each privacy principle • $k_i = 100\% * \text{Vector } z_i \text{ (Characteristics)}$ • z_i = characteristics of the organization 					

To summarize, the final value of each *Table Cell* highlights the criticality of each privacy principle for every data set maintained by the organization. The method employed for the calculation of that criticality level, as already explained in the previous sections, takes into account the consequences that the organization may experience in case of a security or privacy violation incident on a specific data set, the weighting of each privacy principle and the unique characteristics of each organization (Table 36).

The resulting table values offer a strong indication of the security measures and privacy enforcement mechanisms that the organization should adopt in order to effectively protect its data. More specifically the value of each table cell can be compared with the minimum or/and maximum value that the specific cell can take, depending on the characteristics of the organization (Table 1), and if it is found to be near to the maximum cell value the criticality of the privacy principle for the specific data set is considered to be very high.

Chapter 7 : Conclusions and Future Work

7.1 Conclusion

Within this thesis we defined specific goals regarding cloud computing security. Before starting any process, we studied contemporary literature, also giving a criticism on what are the advantages, disadvantages and deficiencies where applicable.

The trust model presented in this thesis and the relevant quantification of trust of cloud provider to cloud user can help to surpass several security risks that affect a cloud environment. Another important aspect of security in cloud computing environment is the protection of personal and even more of sensitive data. Within this thesis we proposed specific measures on how to protect these kind of data taking as guide the needs defined by the EU GDPR regulation. Finally we proposed a unique privacy impact assessment method to the proposed method if applied can protect the privacy of cloud users and the security of the data that they store and process.

Combination of proper trust management, personal data protection and privacy as presented in our thesis can lead to a very high level of security in cloud computing environment. Applying the guidelines, models and techniques on the standardized way of this thesis can encourage organizations to move their infrastructure to cloud.

7.2 Future Work

Within the last two years several malicious have presented techniques of bypassing two factor authentication. Our goal for future is to analyze all the available authentications methods and propose a novel one that will make sure that malicious actors will not be able to protect legitimate users taking into account the resources that the user has.

References

- [1] National Institute of Standards and Technology (NIST), "The NIST Definition of Cloud Computing." Sep-2011.
- [2] B. Sosinsky, *Cloud Computing Bible*, 1st ed. Wiley, 2011.
- [3] P. Kalagiakos and P. Karampelas, "Cloud Computing learning," in *2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, 2011, pp. 1–4.
- [4] W. Liu, "Research on cloud computing security problem and strategy," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, pp. 1216–1219.
- [4] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." Mar-2010.
- [5] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." Mar-2010.
- [6] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *2010 Proceedings of the 33rd International Convention MIPRO*, 2010, pp. 344–349.
- [7] Cloud Security Alliance, "Security as a Service: Defined Categories of Service." 2011.
- [8] Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing F. John Krauthem*, Dhananjay S. Phatak, and Alan T. Sherman* Cyber Defense Lab, Dept. of CSEE University of Maryland, Baltimore County (UMBC)
- [9] M. Ates, S. Ravet, A. M. Ahmat, and J. Fayolle, "An Identity Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights," in *2011 Sixth International Conference on Availability, Reliability and Security (ARES)*, 2011, pp. 555–560. Science (CloudCom), 2011, pp. 255–263.
- [10] H. Lee, I. Jeun, and H. Jung, "Criteria for Evaluating the Privacy Protection Level of Identity Management Services," in *Third International Conference on Emerging Security Information, Systems and Technologies*, 2009. SECURWARE '09, 2009, pp. 155–160.
- [11] Trusted Cloud Computing with Secure Resources and Data Coloring, Kai Hwang - University of Southern California, Deyi Li Tsinghua University, China, IEEE, 2010, online at <http://gridsec.usc.edu/hwang/papers/trusted-cloud-computing.pdf>
- [12] Privacy, Security and Trust in Cloud Computing, Siani Pearson <http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf>
- [13] Security and Privacy in Cloud Computing, Ramakrishnan Krishnan, 2017
- [14] Privacy, Security and Trust in Cloud Computing, Siani Pearson <http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf>
- [15] Wenjuan Li, Lingdi Ping, and Xuezheng Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in *International Conference on Electronics and Information Engineering (ICEIE)*, vol. 1, Kyoto, Japan, 2010, pp. 14–19.
- [16] Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, and Guangming Wan, "A Collaborative Trust Model of Firewall-through based on Computing" in *14th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Shanghai, China, 2010, pp. 329–334.
- [17] Yin Zhixi, Yin Zhixi, "A Secure Trust Model Based on Trusted Computing", Institute of Electrical and Electronics Engineers — Jan 23, 2009.
- [18] Paul D Manuel, Thamarai Selve, and Mostafa Ibrahim Abd-EI Barr, "Trust management system for grid and cloud resources" in *First International Conference on Advanced Computing (ICAC 2009)*, Chennai, India, 2009, pp. 176–181.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- [19] Mohammed Alhamad, Tharam Dillon, and Elizabeth Chang, "SLA-based Trust Model for Cloud Computing" in 13th International Conference on Network-Based Information Systems, Takayama, Japan, 2010, pp. 321 - 324.
- [20] Xiao Yong Li, Li Tao Zhou, Yong Shi, and Yu Guo, "A trusted computing environment model in cloud architecture" in Ninth International Conference on Machine Learning and Cybernetics (ICMLC), vol. 6, Qingdao, China, 2010, pp. 2843-2848.
- [21] Ch.Naveen Kumar Reddy, G.Vishnu Murthy , "Evaluation of Behavioral Security in Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012, 3328 – 3333.
- [22] Bo Tang , Ravi Sandhu, "Cross-Tenant Trust Models in Cloud Computing", Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on 14-16 Aug. 2013.
- [23] The Role of Trust Management in Distributed Systems Security, Matt Blaze, Joan Feigenbaum¹, John Ioannidis, and Angelos D. Keromytis Distributed Systems Lab 2011
- [24] An improved trusted cloud computing platform model based on DAA and privacy CA scheme, Wang Hanzhang, Hiang Liu-sheng, CCASM 2010
- [25] Application-Oriented Remote Verification Trust Model in Cloud Computing, Xiaofei Zhang ; Hui Liu ; Bin Li ; Xing Wang, 2nd IEEE International Conference on Cloud Computing Technology and Science
- [26] SLA-Aware Trust Model Cloud Service Deployment , Shyamlal Kumawat, Deepak Tomar, International Journal of Computer Applications (0975 – 8887) 2014
- [27] Liqin Tian, Anjuan Qiao, Lin Chuang, Ji Tieguo. Kind of Quantitative Evaluation of User Behaviour Trust Using AHP.Journal of Computational Information Systems, 2007, 3(4):1329-1334.
- [28] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.
- [29] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn. Design and implementation of a TCG-based integrity measurement architecture. In Proceedings of USENIX Security Symposium, pages 223–238, Aug. 2004
- [30] S. Ries, S. M. Habib, M. MuhlhLauser, and V. Varadharajan, Certainlogic: A logic for modeling trust and uncertainty,"Technische Universit at Darmstadt, Tech. Rep. TUD-CS-2011-0104, 2011.
- [31] S. Ries and E. Aitenbichler, Limiting sybil attacks on Bayesian trust models in open soa environments," in Proceedings of the The First International Symposium on Cyber-Physical Intelligence (CPI-09), 2009.
- [32] Fujitsu Research Institute,\Personal data in the cloud: A global survey of consumer attitudes," 2010
- [33] L. Wenjuan, P. Lingdi, and P. Xuezheng, "Use trust management module to achieve effective security mechanisms in cloud environment," in International Conference on Electronics and Information Engineering (ICEIE), vol. 1, Kyoto, Japan, 2010, pp. 14-19.
- [34] Z. Georgiopoulou, C. Lambrinoudakis,"Literature Review of Trust Models for Cloud Computing", International Conference On Cloud Computing And Big Data (CloudCom-Asia), Hong Kong, 2016.
- [35] P. D. Manuel, T. Selve, and M. I. Abd-EI Barr, "Trust management system for grid and cloud resources" in First International Conference on Advanced Computing (ICAC 2009), Chennai, India, 2009, pp. 176-181.
- [37] Geolocation: Risk, Issues and Strategies, ISACA, Geolocation: Risk, Issues and Strategies
- [38] B. Eriksson, P. Barford, J. Sommersy, and Robert Nowak, "A Learning-based Approach for IP Geolocation NIST Interagency Report 7904, December 2012

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- [39] E. K. Banks, M. Bartock, K. Fiftal, D. Lemon, K. Scarfone, U. Shetty et al., “Trusted Geolocation in the Cloud: Proof of Concept Implementation”, *International Journal of Computer Science and Information Technologies*, Vol. 3 (2) , 2012, 3328 – 3333.
- [40] B. K. Dewangan¹, P. Shende², “The Sliding Window Method: An Environment To Evaluate User Behavior Trust In Cloud Technology”, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 2, February 2013.
- [41] T. Li-qin, L. Chuang "Evaluation of User Behavior Trust in Cloud Computing" 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)
- [42] Bird & Bird, *Guide to the General Data Protection Regulation*, January 2017
- [43] Cloud Security Alliance, *CODE OF CONDUCT FOR GDPR COMPLIANCE*, November 2017, https://downloads.cloudsecurityalliance.org/assets/research/gdpr/CSA_Code_of_Conduct_for_GDPR_Compliance.pdf
- [44] European Parliament and of the Council , The European Parliament and the Council of the European Union, April 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1485368166820&from=en>
- [45] Microsoft, *Accelerate GDPR compliance with the Microsoft Cloud* , July 2017
- [46] Amazon Web Services, *Navigating GDPR Compliance on AWS*, 2018
- [47] Google Cloud Whitepaper, *General Data Protection Regulation (GDPR)*, May 2018
- [48] Deloitte, *Data Privacy in the cloud*, September 2015
- [49] LexisNexis, *GDPR and codes of conduct in SaaS*, January 2019
- [50] Oracle Cloud Infrastructure, *Oracle Cloud Infrastructure and the GDPR*, European Union General Data Protection Regulation, April 2018
- [51] Norm Barber , *The GDPR and Its Implications On Cloud Services*, September 2017
- [52] Microsoft, *Safeguard individual privacy with the Microsoft Cloud*, viewed August 2019, <https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview>
- [53] Information Commissioner’s Office, *Children and the GDPR* , 22 March 2018, <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>
- [54] Multistakeholder Expert Group , *Contribution from the multistakeholder expert group to the stock-taking exercise of June 2019 on one year of GDPR application*, 13 June 2019
- [55] Sohail Razi Khan, Luis Borges Gouvias, *The implication and challenges of GDPR’s on Cloud Computing Industry* , July 2019
- [56] Georgiopolou Z., Makri E.L., Lambrinoudakis C., “GDPR Compliance: Proposed Technical and Organizational measures for Cloud Providers”, *Proceedings of the 3rd International Workshop on SECURITY and Privacy Requirements Engineering (SECPRE 2019)*, in conjunction with ESORICS 2019, Luxembourg, September 2019
- [57] W Hong, JYL Thong, *Internet privacy concerns: An integrated conceptualization and four empirical studies*, *MIS Quarterly*, Vol. 37, No. 1 (2013) pp. 275-298, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229627.
- [58] Regulation (EU) 2016/679 of the European Parliament and of the Council, The European Parliament and the Council of the European Union, April 27, 2016, available at <http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1485368166820&from=en>.
- [59] OECD Privacy Principles, [OECDprivacy.org](http://oecdprivacy.org/), 1980, available at <http://oecdprivacy.org/>.
- [60]. Makri E. L., Lambrinoudakis C., “Towards a Common Security and Privacy Requirements Elicitation Methodology”, *Proceedings of the 10th International Conference Global Security, Safety and Sustainability (ICGS3 2015)*, 151-160, Springer CCIS 534, London, UK, September 2015.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- [61] Makri E. L., Lambrinouidakis C., “Privacy Principles: Towards a Common Privacy Audit Methodology”, Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus’15), pp. 219-234, Springer LNCS 9264, Valencia, Spain, September 2015.
- [62] F Bélanger, RE Crossler, Privacy in the digital age: a review of information privacy re-search in information systems, Journal MIS Quarterly, Volume 35 Issue 4, December 2011, Pages 1017-1042, available at <http://dl.acm.org/citation.cfm?id=2208951>.
- [63] David Wright, Paul De Hert, Chapter 1: Introduction to Privacy Impact Assessment, Book Title: Privacy Impact Assessment, 2012, pp 3-32, available at http://link.springer.com/chapter/10.1007/978-94-007-2543-0_1#page-1.
- [64] ISO/IEC FDIS 29134, Information technology — Security techniques — Privacy impact assessment — Guidelines, Target publication date: 2017-05-30, available at http://www.iso.org/iso/catalogue_detail.htm?csnumber=62289, <https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:dis:ed-1:v1:en>.
- [65] Information Commissioner’s Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, December 2007, Version 2.0, June 2009.
- [66] David Wright, Paul De Hert, Chapter 1: Introduction to Privacy Impact Assessment, Book Title: Privacy Impact Assessment, 2012, available at http://link.springer.com/chapter/10.1007/978-94-007-2543-0_1#page-1.
- [67] European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009H0387&from=EN>.
- [68] Yang Wang, Alfred Kobsa, Privacy-Enhancing Technologies, 2008, available at <http://www.cs.cmu.edu/afs/cs/Web/People/yangwan1/papers/2008-Handbook-LiabSec-AuthorCopy.pdf>.
- [69] Ann Cavoukian, Creation of a Global Privacy Standard, November, 2006, available at <http://www.ipc.on.ca/images/Resources/gps.pdf>.
- [70] Ann Cavoukian, Scott Taylor, Martin E. Abrams, Privacy by Design: essential for organizational accountability and strong business practices, Identity in the Information Society, Springer, 2010, available at <http://link.springer.com/article/10.1007/s12394-010-0053-z>.
- [71] Ann Cavoukian, Privacy by design – the 7 foundational principles, Technical report, Information and Privacy Commissioner of Ontario, January 2011. (revised version).
- [72] Oetzel, Marie Caroline and Spiekermann, Sarah, "PRIVACY-BY-DESIGN THROUGH SYSTEMATIC PRIVACY IMPACT ASSESSMENT - A DESIGN SCIENCE APPROACH" (2012), ECIS 2012 Proceedings, paper 160, available at <http://aisel.aisnet.org/ecis2012/160>.
- [73] Oetzel, Marie Caroline and Spiekermann, Sarah, A systematic method for privacy impact assessments: a design science approach, European Journal of Information Systems (2013), 1–25.
- [74] Information Commissioner’s Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 1.0, December 2007.
- [75] Information Commissioner’s Office (ICO), Privacy impact assessment and risk management, May 2013, available at <https://ico.org.uk/media/1042196/trilateral-full-report.pdf>.
- [76] Information Commissioner’s Office (ICO), Conducting privacy impact assessments code of practice, February 2014, available at <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>.
- [77] Information Commissioner’s Office (ICO), The Guide to Data Protection, January 2017, available at <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-7.pdf>.

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

- [78] European Commission, PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights, Duration: January 2011 - October 2012, available at <http://www.piafproject.eu/Index.html>.
- [79] David Wright, Kush Wadhwa, A step-by-step guide to privacy impact assessment, Second PIAF workshop, Sopot, Poland, 24 April 2012, available at http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf.
- [80] David Wright, Should Privacy Impact Assessments be Mandatory?, Communications of the ACM 54 (8), 2011, doi:10.1145/1978542.1978568, available at <http://cacm.acm.org/magazines/2011/8>.
- [81] Kush Wadhwa & Rowena Rodrigues (2013) Evaluating privacy impact assessments, Innovation: The European Journal of Social Science Research, 26:1-2, 161-180, DOI: 10.1080/13511610.2013.761748, available at <http://www.tandfonline.com/doi/abs/10.1080/13511610.2013.761748>, <http://www.tandfonline.com/doi/pdf/10.1080/13511610.2013.761748?needAccess=true>
- [82] Sean Brooks, Ellen Nadeau, Privacy Risk Management for Federal Information Systems, Information Technology Laboratory, NIST, Internal Report 8062, May 2015, available at http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.
- [83] John Martin Ferris, The ISO PIA Standard for Financial Services, Chapter 14: The ISO PIA Standard for Financial Services, Book Title: Privacy Impact Assessment, 2012, pp 307-321, available at http://link.springer.com/chapter/10.1007/978-94-007-2543-0_14.
- [84] David Wright, Should privacy impact assessments be mandatory?, Trilateral Research & Consulting, 17 Sept 2009, available at <http://www.ics.forth.gr/nis09/presentations/18-wright.pdf>.
- [85] Sushant Agarwal, Chapter: Developing a Structured Metric to Measure Privacy Risk in Privacy Impact Assessments, Book Title: Privacy and Identity Management. Time for a Revolution?, pp 141-155, 07 July 2016, available at: https://link.springer.com/chapter/10.1007%2F978-3-319-41763-9_10.
- [86] NIST (National Institute of Standards and Technology). (2002) Risk management guide for information technology systems, NIST Special Publication 800-30.
- [87] Data Protection Act 1998, available at <http://www.legislation.gov.uk/ukpga/1998/29/contents>, http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf
- [88] European Union Agency for Network and Information Security (ENISA), CRAMM (CCTA Risk Analysis and Management Method), available at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
- [89] Commission Nationale de l'Informatique et des Libertés (CNIL), Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA), June 2015 Edition, available at: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>.
- [90] Commission Nationale de l'Informatique et des Libertés (CNIL), The open source PIA software helps to carry out data protection impact assessment, January 2018, available at: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>.
- [91] Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Pierangela Samarati, Data Privacy: Definitions and Techniques, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20(6): 793-818 (2012).
- [92] Makri E.L., Georgiopoulou Z., Lambrinoudakis C., "A Proposed Privacy Impact Assessment Method using Metrics based on Organizational Characteristics", Proceedings of the 3rd

Trust Management, privacy, authorization, and authentication in Cloud Computing environments.

International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2019), in conjunction with ESORICS 2019, Luxembourg, September 2019.

[93] Zafeiroula Georgiopolou, Costas Lambrinouidakis, Trust Management Parameters in Cloud Computing Environments, Published in: CLOUD COMPUTING 2017 : The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization and at IARIA Journals

[94] Zafeiroula Georgiopolou, Eleni-Laskarina Makri, Costas Lambrinouidakis: GDPR Compliance: Proposed Technical and Organizational Measures for Cloud Providers. CyberICPS/SECPRE/SPOSE/ADIoT@ESORICS 2019: 181-194

[95] Zafeiroula Georgiopolou, Eleni-Laskarina Makri, Costas Lambrinouidakis: GDPR compliance: proposed technical and organizational measures for cloud provider. Inf. Comput. Secur. 28(5): 665-680 (2020)

[96] Eleni-Laskarina Makri, Zafeiroula Georgiopolou, Costas Lambrinouidakis: Utilizing a privacy impact assessment method using metrics in the healthcare sector. Inf. Comput. Secur. 28(4): 503-529 (2020)