University of Piraeus Department of Digital Systems
Post graduate program in Digital Systems Security

Supervisor: Dr. Konstantinos Labrinoudakis, Ass. Professor

Course Student: Nikolaos Yfantopoulos, MTE/0932

Thesis subject: Cloud Computing in Healthcare Systems

Piraeus, January 2012

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΠΙΒΛΕΠΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ, ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟΣ ΦΟΙΤΗΤΗΣ: ΥΦΑΝΤΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ, ΜΤΕ/0932

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ: ΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΥΓΕΙΑΣ

Πειραιάς, Φεβρουάριος 2012

ΠΕΡΙΛΗΨΗ

Η ηλεκτρονική υγεία, δηλαδή η εφαρμογή τεχνολογιών πληροφοριών και επικοινωνιών στον τομέα της υγείας, έχει ως στόχο τη συγκέντρωση, ανάλυση και αποθήκευση των κλινικών δεδομένων σε όλες τις μορφές καθώς και την ανταλλαγή αυτών των δεδομένων ανάμεσα στις μονάδες παροχής υγείας, και τους ασφαλιστικούς φορείς.

Η υπηρεσία της ηλεκτρονικής υγείας ενσωματώνει τις έννοιες τηλεϊατρική, τηλε-συμβουλευτική, φορητές ηλεκτρονικές συσκευές και ιατρικές δικτυακές πύλες, οι οποίες προϋποθέτουν την αποδοχή καινοτόμων τεχνολογιών για την συγκέντρωση και αξιοποίηση των ευαίσθητων ιατρικών δεδομένων.

Στην παρούσα εργασία θα μελετηθεί η χρήση τεχνολογίας υπολογιστικού νέφους σε συστήματα υγείας λόγω της μεγάλης ελαστικότητας, επεκτασιμότητας και οικονομίας κλίμακας (return of investment-ROI) που προσφέρει.

Επιπρόσθετα, οι δικτυακοί εξυπηρετητές, οι αποθηκευτικοί χώροι, οι βάσεις δεδομένων και γενικότερα οι υποδομές και οι υπηρεσίες ενός υπολογιστικού νέφους προσφέρουν μια ελκυστική πλατφόρμα για την συνεργασία όλων των μονάδων υγείας, αρχικά σε εθνικό και στη συνέχεια σε παγκόσμιο επίπεδο. Βέβαια, ένα σημαντικό μειονέκτημα που αναδύεται είναι ότι το υπολογιστικό νέφος έρχεται σε ρήξη με τους νόμους περί Ιδιωτικότητας και ασφάλειας των ευαίσθητων δεδομένων των ασθενών αφού σε περίπτωση παραβίασής του θα μπορούσε κάποιος κακόβουλος να έχει πρόσβαση σε όλους τους ιατρικούς φακέλους και γνωματεύσεις του ιατροφαρμακευτικού προσωπικού.

Αναλυτικότερα, η εργασία είναι δομημένη σε τέσσερα κύρια κεφάλαια που ενσωματώνουν τις έννοιες του υπολογιστικού νέφους και της χρησιμότητάς του στον τομέα της υγείας. Πιο συγκεκριμένα στο πρώτο κεφάλαιο αναλύεται η δομή, τα μοντέλα και τα χαρακτηριστικά του υπολογιστικού νέφους ενώ στο δεύτερο περιγράφονται οι απειλές, οι κίνδυνοι και η ασφάλεια σε αυτό. Στο τρίτο κεφάλαιο παρατίθενται οι προϋποθέσεις που ορίζονται από την HIPAA για εφαρμογή μοντέλου υπολογιστικού νέφους στην υγεία, καθώς και εφαρμογή της τηλεϊατρικής μέσω του μοντέλου νέφους. Τέλος, στο τέταρτο κεφάλαιο εφαρμόζεται ένα μοντέλο ιατρικής υγείας πάνω σε πλατφόρμα ως υπηρεσία λειτουργώντας ως ιδιωτικό σύννεφο και προσφέροντας υπηρεσίες υγείας εφαρμόζοντας παράλληλα μηχανισμούς για την εξασφάλιση της ασφάλειας και της ιδιωτικότητας των δεδομένων των ασθενών.

Λέξεις-κλειδιά: υπολογιστικό νέφος, απειλές, επιθέσεις, ασφάλεια, ηλεκτρονική υγεία

ABSTRACT

E-health, namely the application of ICT in health, is aimed at gathering, analyzing and storing clinical data in all formats and exchanges those data between health agents and insurers.

The service of e-health incorporates telemedicine concept, tele-counseling, portable electronic devices and medical portals, which involve the acceptance of innovative technologies for the collection and use of sensitive medical data.

This thesis studies the use of cloud computing technology in healthcare systems due to high flexibility, scalability and return of investment (ROI).

Additionally, network servers, storage facilities, databases and cloud's infrastructure and services offer an attractive platform for cooperation of all health facilities, first nationally and then globally. On the other hand, one major drawback is that cloud computing comes into conflict with privacy laws and security of sensitive patient data in case of security breach (impact: an opponent could gain access to all medical records).

The thesis is structured into four main chapters that incorporate the concept of cloud computing and its usefulness in healthcare systems. Precisely, the first chapter includes the concept of cloud computing, its models and its features, while the second analyzes the threats, the risks and the security on it. The third chapter analyzes the conditions defined by HIPAA for implementing cloud computing in healthcare systems and demonstrates the implementation of telemedicine through the use of cloud computing model. Finally, the fourth chapter applies a healthcare model on infrastructure as a service acting as a private cloud and providing healthcare services while ensuring mechanisms to meet security and privacy requirements on patient data.

Keywords: cloud computing, threats, common attacks, security, e-health

Πρόλογος

Η παρούσα εργασία με τίτλο «το υπολογιστικό νέφος σε συστήματα υγείας» εκπονήθηκε στα πλαίσια της διπλωματικής μου εργασίας στο τμήμα “ψηφιακών συστημάτων” υπό την επίβλεψη του καθηγητή κ. Λαμπρινουδάκη Κωνσταντίνου.

Τελειώνοντας το μεταπτυχιακό μου αποκόμισα βασικές γνώσεις και δεξιότητες πάνω σε θέματα ασφάλειας και ιδιωτικότητας δεδομένων και υπηρεσιών. Επιπλέον μέσα από το θερινό σχολείο ασφάλειας που διοργανώθηκε στην Σάμο υπό την αιγίδα του Πανεπιστημίου Αιγαίου και την συνεργασία του Πανεπιστημίου Πειραιώς, μου δόθηκε η δυνατότητα να γνωρίσω σπουδαίους διεθνείς καθηγητές, καθώς και συμφοιτητές από ξένα πανεπιστήμια με τους οποίους μοιράστηκα τις γνώσεις και τις ανησυχίες μου σε θέματα ασφάλειας.

Αρχικά θα ήθελα να ευχαριστήσω θερμά τον καθηγητή του τμήματος ψηφιακών συστημάτων και επιβλέπων της διπλωματικής μου, κ. Λαμπρινουδάκη Κωνσταντίνο για την συμβολή του στην παρούσα εργασία και την πολύτιμη βοήθεια και υποστήριξη που μου προσέφερε τόσο σε θεωρητικό όσο και σε τεχνικό επίπεδο.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για όλες τις θυσίες που έχουν κάνει για μένα και να τους αφιερώσω την διατριβή αυτή για όλα τα χρόνια που έχουν σταθεί δίπλα μου.

Περιεχόμενα

Εισαγωγή 6
Κεφάλαιο 1ο Βασικές έννοιες και χαρακτηριστικά του υπολογιστικού νέφους 7
1.1 Ορισμός Υπολογιστικού Νέφους 7
1.2 Συστατικά Υπολογιστικού Νέφους 7
1.3 Βασικά χαρακτηριστικά Υπολογιστικού Νέφους 9
1.4 Υπηρεσίες Υπολογιστικού Νέφους 10
1.5 Μοντέλα Ανάπτυξης στο Υπολογιστικό Νέφος 12
1.6 Το Υπολογιστικό Νέφος και ο νέος ρόλος του τμήματος πληροφορικής (IT) 14
Κεφάλαιο 2ο Κίνδυνοι Απειλές και Ασφάλεια στο Υπολογιστικό Νέφος 16
2.1 Κίνδυνοι που προκύπτουν από την επιλογή παρόχου 16
2.2 Τα οφέλη της ασφάλειας στο Υπολογιστικό Νέφος 17
2.3 Ευθυγράμμιση των προτύπων ασφάλειας στο Υπολογιστικό σύννεφο 19
2.3.1 Βασικές απαιτήσεις ασφάλειας του συστήματος διαχείρισης πληροφοριών του νέφους 20
2.3.2 Ευθυγράμμιση του NIST-FISMA με το μοντέλο του υπολογιστικού σύννεφου 21
2.4 Χρήση τεχνικής διαμοιρασμού μυστικού θέματος για ασφαλή αποθήκευση στο Υπολογιστικό νέφος 26
Κεφάλαιο 3ο Το Υπολογιστικό Σύννεφο στην υπηρεσία της υγείας 28
3.1 Όροι και προϋποθέσεις της HIPAA για εφαρμογή νέφους στον τομέα της Υγείας 28
3.2 Συνδυασμός Τηλεϊατρικής και χρήσης υπολογιστικού σύννεφου στον τομέα της υγείας 31
Κεφάλαιο 4ο Πρότυπο μοντέλο ηλεκτρονικής υγείας βασισμένο στο υπολογιστικό σύννεφο 36
4.1 Εισαγωγή για την ηλεκτρονική υγεία 36
4.2Μοντέλο συστήματος 37
4.3 Βασικές προϋποθέσεις ασφάλειας 38
4.4 Απειλές και επιθέσεις 38
4.5 Σχεδιασμός μοντέλου ηλεκτρονικής υγείας 40
4.7 Προδιαγραφές συστήματος ηλεκτρονικής υγείας 45
4.7.1 Υποδομή ως υπηρεσία 46
4.7.2 Πλατφόρμα ως υπηρεσία 48
4.7.3 Λογισμικό ως υπηρεσία 52
4.8 Έλεγχος ασφάλειας της πλατφόρμας ηλεκτρονικής υγείας με την χρήση του προτύπου NIST-FISMA για υπολογιστικά νέφη 54
Επίλογος 57
Παράρτημα 58
Βιβλιογραφία 59

Εισαγωγή

Σήμερα ο όρος υπολογιστικό σύννεφο (cloud computing) γίνεται ολοένα και πιο διαδεδομένος στον καθημερινό καταναλωτή λόγω της μεγάλης απήχησής του από εταιρίες πληροφορικής (HP, Microsoft) και επιχειρήσεις κατασκευής φορητών συσκευών (Apple, SE).

Αν κάνουμε όμως μια έρευνα στον καθημερινό καταναλωτή για το τι είναι το υπολογιστικό νέφος, πως μπορεί να χρησιμοποιηθεί, ποια προβλήματα και προκλήσεις εμφανίζονται με την χρήση του, θα πάρουμε σίγουρα διαφορετικές απαντήσεις που μπορεί να μην απεικονίζουν την πραγματική εικόνα του όρου και της σημασίας του. Τι είναι όμως στην πραγματικότητα το υπολογιστικό σύννεφο;

Αρχικά ο όρος «σύννεφο» χρησιμοποιήθηκε ως μεταφορά για τον όρο Διαδίκτυο και ήταν βασισμένος στο σχέδιο του σύννεφου που χρησιμοποιούνταν στο παρελθόν για να εκπροσωπήσει το τηλεφωνικό δίκτυο και στη συνέχεια το Διαδίκτυο στα διαγράμματα του δικτύου υπολογιστών ως μια αφαίρεση της υποκείμενης υποδομής που αντιπροσωπεύει. Συγκεκριμένα, το 1961 οι επιστήμονες του MIT είχαν οραματιστεί κάτι που ονόμασαν «the computer utility» (υπολογιστική χρησιμότητα). «Οι υπολογιστές μια μέρα μπορεί, σαν την τηλεφωνία, να αποτελέσουν μια υπηρεσία κοινής ωφέλειας» είχε πει ο καθηγητής Τζον Μακάρθι σε μια εκδήλωση του MIT. «Ο κάθε συνδρομητής θα πληρώνει ανάλογα με τη χρήση που κάνει, όμως θα έχει πρόσβαση σε όλες τις γλώσσες προγραμματισμού που χαρακτηρίζουν τα πολύ μεγάλα συστήματα.

Είναι όμως το υπολογιστικό σύννεφο επέκταση της υπολογιστικής χρησιμότητας ή ενσωματώνει τον ρόλο της υπολογιστικής χρησιμότητας στον ορισμό του;

Σύμφωνα με τους Foster et al [1] «*το υπολογιστικό σύννεφο όχι μόνο υπερέχει της υπολογιστικής χρησιμότητας, αλλά αποτελεί εξέλιξής της και στηρίζεται σε αυτό, καθώς αποτελεί την ραχοκοκαλιά του και την δομή υποστήριξης του. Η εξέλιξη αποτελεί ένα αποτέλεσμα αλλαγής της εστίασης από μια δομή που προσφέρει αποθήκευση και υπολογιστικούς πόρους (υπολογιστική χρησιμότητα) σε μια δομή που στηρίζεται στην οικονομία και στοχεύει στην παροχή αφηρημένων πόρων και υπηρεσιών (υπολογιστικό σύννεφο)*».

Ως αποτέλεσμα η υπολογιστική χρησιμότητα είναι η βάση για το υπολογιστικό σύννεφο και επίσης το δεύτερο (ΥΣ) αντιπροσωπεύει την ανάθεση και ενοικίαση των πόρων (αποθηκευτικός χώρος, μνήμη, ισχύς, υπηρεσίες και εφαρμογές) σε επιχειρήσεις-πελάτες ανάλογα με τις ανάγκες τους.

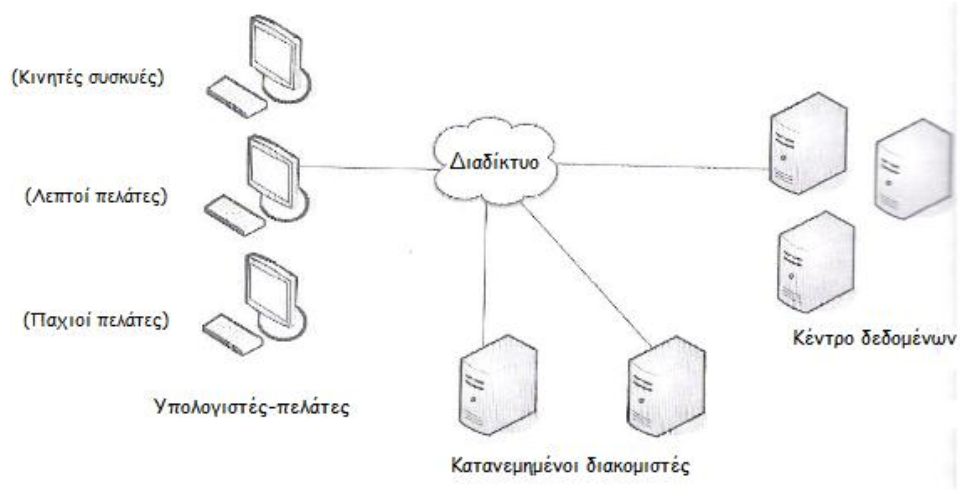
Κεφάλαιο 1ο Βασικές έννοιες και χαρακτηριστικά του υπολογιστικού νέφους

1.1 Ορισμός Υπολογιστικού Νέφους

Το υπολογιστικό νέφος είναι το τελευταίο κύμα εξέλιξης των συστημάτων αρχιτεκτονικής. Το σύννεφο χρησιμοποιεί τους υπολογισμούς ως μια χρησιμότητα, δηλαδή δίνει την δυνατότητα στους ‘’πελάτες’’ να υποβάλλουν τις διεργασίες που χρήζουν υπολογισμό στο σύννεφο, το οποίο παρέχει τους απαραίτητους πόρους για την εκτέλεση των διεργασιών αυτών. Σύμφωνα με το Αμερικανικό Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) [2], το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την κατόπιν ζήτησης (On-demand) πρόσβαση στο δίκτυο σε μια κοινόχρηστη πισίνα από διαμορφώσιμους υπολογιστικούς πόρους." Μεγαλύτερη σπουδαιότητα παρουσιάζει το γεγονός ότι οι ‘’πελάτες’’ μπορούν να εξοικονομήσουν χρηματικούς πόρους στην πάροδο του χρόνου αφού αντί να πληρώσουν για αγορά και συντήρηση άφθονων μηχανημάτων (π.χ εξυπηρετητών) μπορούν να συνδεθούν στο σύννεφο, πληρώνοντας μόνο για τους πόρους που αυτοί χρησιμοποιούν. Η λύση του υπολογιστικού νέφους είναι ιδιαίτερα ελκυστική για τους πελάτες των οποίων η χρήση των πόρων ποικίλλει σημαντικά, ή για εκείνους όπου το υλικό (αγορά μηχανημάτων) και το κόστος συντήρησης αποτελούν σημαντικό τμήμα του συνολικού προϋπολογισμού τους.

1.2 Συστατικά Υπολογιστικού Νέφους

Τα κύρια συστατικά που συνθέτουν μία λύση υπολογιστικού νέφους είναι 1)οι υπολογιστές-πελάτες, 2)το κέντρο δεδομένων και 3)οι κατανεμημένοι διακομιστές. Κάθε συστατικό, όπως φαίνεται και στο σχήμα 1.1, αποτελεί αναπόσπαστο κομμάτι μιας ολοκληρωμένης λύσης νέφους και διαδραματίζει ένα συγκεκριμένο ρόλο στην λειτουργική ομαλότητα κάθε εφαρμογής βασισμένης σε αυτό.



Σχήμα 1.1 Κύρια συστατικά Υπολογιστικού σύννεφου

Αναλυτικότερα οι *υπολογιστές πελάτες* είναι οι συσκευές με τις οποίες αλληλεπιδρούν οι τελικοί χρήστες για να διαχειρίζονται τις πληροφορίες τους στο νέφος. Οι υπολογιστές-πελάτες χωρίζονται σε 3 κατηγορίες:

- Κινητές συσκευές (mobile devices): είναι συσκευές όπως PDA's και Smartphones που επιτρέπουν την απομακρυσμένη πρόσβαση των πληροφοριών στον χρήστη, κατόπιν επεξεργασίας από τον κατανεμημένο διακομιστή.
- Λεπτοί πελάτες (thin clients)*:* είναι υπολογιστές που δεν έχουν ούτε μεγάλη υπολογιστική δύναμη, ούτε εσωτερικούς σκληρούς δίσκους, αφού εμφανίζουν όλες τις διαθέσιμες πληροφορίες κατόπιν επεξεργασίας αυτών από τον διακομιστή. Έτσι προσφέρεται συγχρόνως 1) μεγάλη ασφάλεια, αφού τα δεδομένα αποθηκεύονται στον κεντρικό διακομιστή και υπάρχει μικρότερη πιθανότητα να κλαπούν εάν ο υπολογιστής-πελάτης χαλάσει ή κλαπεί και 2)χαμηλό κόστος υλικού και μηχανογράφησης αφού η διαχείριση τους γίνεται στον διακομιστή και υπάρχουν λιγότερα σημεία αποτυχίας.
- Παχιοί πελάτες (thick clients): είναι υπολογιστές καθημερινής χρήσης που χρησιμοποιούν έναν φυλλομετρητή για να συνδεθούν στο νέφος.

Το *κέντρο δεδομένων* είναι το σύνολο των διακομιστών, στους οποίους φιλοξενείται κάθε εφαρμογή. Σε αυτήν την κατηγορία συμπεριλαμβάνονται και οι εικονικοί διακομιστές (δηλαδή σε έναν διακομιστή μπορεί να εγκατασταθεί λογισμικό που να επιτρέπει την ύπαρξη πολλαπλών στιγμιότυπων εικονικών διακομιστών), των οποίων ο αριθμός εξαρτάται από το μέγεθος και την ταχύτητα του φυσικού διακομιστή.

Οι *κατανεμημένοι διακομιστές* είναι διακομιστές που βρίσκονται σε γεωγραφικά διαφορετικές θέσεις. Έτσι δίνεται μεγαλύτερη ευελιξία και

ασφάλεια στον φορέα παροχής υπηρεσιών νέφους. Για παράδειγμα εάν εμφανιστεί μια παραβίαση ασφάλειας ή πρόβλημα διαθεσιμότητας πόρων σε μια τοποθεσία, τότε η υπηρεσία μπορεί να προσπελαστεί μέσω μιας άλλης τοποθεσίας, Επιπλέον εάν το νέφος χρήζει ανάγκης επιπρόσθετου υλικού (είτε αποθηκευτικού χώρου, είτε υπολογιστικής δύναμης), τότε μπορούν να προστεθούν περισσότεροι διακομιστές από μια τρίτη τοποθεσία και απλά να γίνουν μέρος του νέφους.

1.3 Βασικά χαρακτηριστικά Υπολογιστικού Νέφους

Τα βασικά χαρακτηριστικά του υπολογιστικού νέφους είναι:

- Η αυτό-εξυπηρέτηση κατόπιν ζήτησης (On-demand self-service): προσφέρει στην επιχείρηση/οργανισμό που υιοθετεί την λύση του νέφους, την δυνατότητα αξιοποίησης των υπολογιστικών πόρων (όπως η αποθήκευση στο σύννεφο) αυτόματα για όσο τους χρειάζεται και χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με τον πάροχο κάθε υπηρεσίας.
- *Ευρεία πρόσβαση στο δίκτυο (Broad network access)*: οι προσφερόμενες δυνατότητες από το νέφος είναι διαθέσιμες μέσω δικτύου και είναι προσβάσιμες μέσω τυποποιημένων μηχανισμών οι οποίοι προωθούν την χρήση ετερογενών πλατφόρμων λεπτού (thin client) ή παχύ πελάτη(thick client).
- Διάθεση των πόρων (Resource pooling): οι υπολογιστικοί πόροι των παρόχων νέφους συγκεντρώνονται με την χρήση ενός μοντέλου multi-tenant (κάθε οργανισμός εργάζεται με ένα προσαρμοσμένο εικονικό Instance της εφαρμογής και δεν δημιουργείται ανάγκη ξεχωριστής εγκατάστασης για κάθε οργανισμό που συνυπάρχει και λειτουργεί το ίδιο λογισμικό) ώστε να εξυπηρετήσουν πολλούς οργανισμούς υιοθέτησης νέφους, ανάλογα με την ζήτηση του καθενός. Οι παρεχόμενοι πόροι μπορεί να είναι επεξεργαστική ισχύς, μνήμη, εύρος δικτύου και εικονικές μηχανές.
- Μεγάλη ελαστικότητα (Rapid Elasticity): οι προσφερόμενες δυνατότητες του νέφους παρέχονται τόσο γρήγορα και με τόση μεγάλη προσαρμοστικότητα που κάποιες φορές φαίνονται να είναι απεριόριστες και σε οποιαδήποτε ποσότητα και χρονική στιγμή θελήσει ο οργανισμός-πελάτης.
- Μετρούμενη υπηρεσία (Measured Service): τα συστήματα νέφους αυτόματα ελέγχουν και βελτιστοποιούν την χρήση των πόρων χρησιμοποιώντας την δυνατότητα μέτρησης, σε κάποιο επίπεδο αφαίρεσης ανάλογα με το είδος της υπηρεσίας (μνήμη, επεξεργασία, εύρος και ενεργοί λογαριασμοί χρηστών). Η χρήση των πόρων μπορεί να παρακολουθηθεί, να ελεγχθεί και να

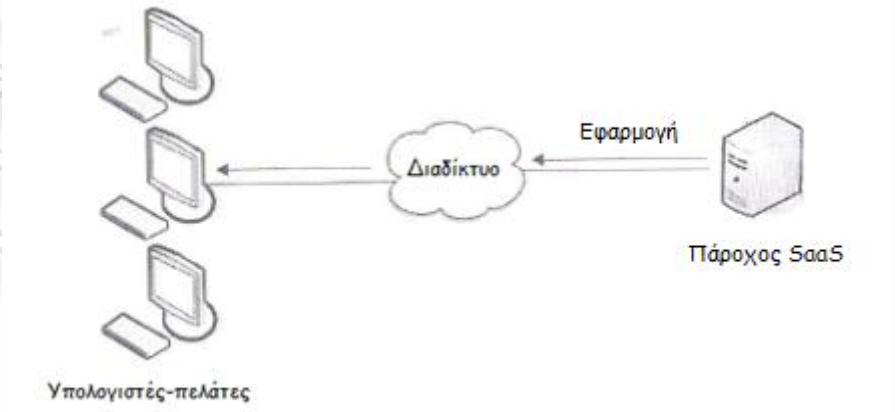
καταγραφεί παρέχοντας διαφάνεια στον οργανισμό-πελάτη και στον πάροχο του νέφους[3].

1.4 Υπηρεσίες Υπολογιστικού Νέφους

Το υπολογιστικό νέφος μπορεί να διαχωριστεί ως προς το είδος υπηρεσίας που προσφέρεται (service model) και ως προς το μοντέλο ανάπτυξής του (deployment model).

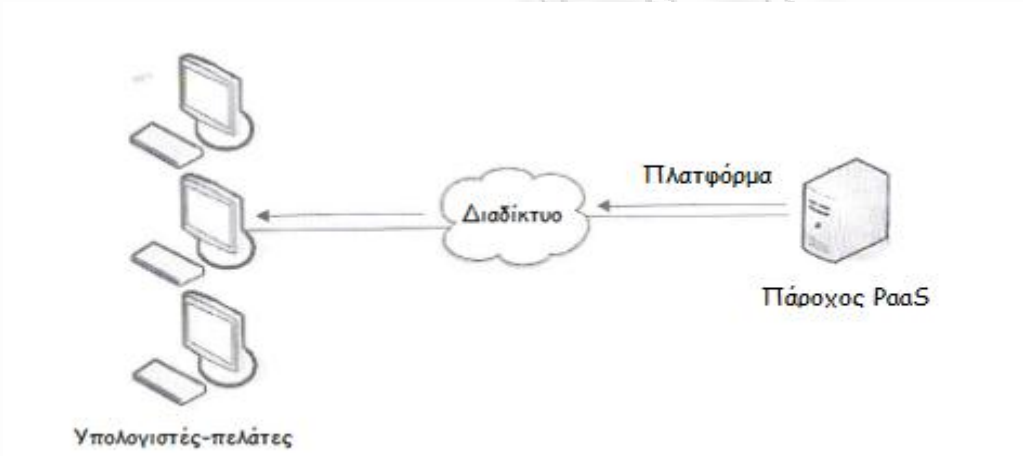
Ως προς το είδος υπηρεσίας που προσφέρεται, τα διαθέσιμα μοντέλα του υπολογιστικού νέφους είναι α) το λογισμικό ως μια υπηρεσία (Software as a Service-SaaS), β) η πλατφόρμα ως υπηρεσία (Platform as a Service-PaaS) και γ) το υλικό ως υπηρεσία (Hardware as a Service-HaaS).

Το λογισμικό ως υπηρεσία (Saas) είναι ένα μοντέλο ανάπτυξης λογισμικού σύμφωνα με το οποίο οι εφαρμογές και οι υπολογιστικοί πόροι παρέχονται για χρήση κατόπιν ζήτησης (use on demand). Λειτουργεί σε έναν κεντρικοποιημένο δίκτυο εξυπηρετητών προκειμένου να διατίθεται ως υπηρεσία στο διαδίκτυο (σχήμα 1.2) και είναι άκρως διαδεδομένο λόγω της ευελιξίας που προσφέρει, της ποιότητας υπηρεσιών, της υψηλής σταθερότητας και της ελάχιστης δυνατής συντήρησης που απαιτεί. Επίσης θεωρείται αξιόπιστη λύση ασφάλειας, αφού υιοθετεί SSL (Secure Socket Layer) στις υπηρεσίες του και έτσι τα δεδομένα μεταδίδονται ασφαλή από και προς τον χρήστη. Βασικό του μειονέκτημα είναι ότι παρέχει πρόσβαση βασισμένη σε δίκτυο εμπορικών λογισμικών και έτσι μια μικρομεσαία επιχείρηση με δικό της λογισμικό μπορεί να μην βρει συγκεκριμένη εφαρμογή διαθέσιμη μέσω του SaaS. Υπηρεσίες που ανήκουν σε αυτό το μοντέλο είναι το Google App Engine [http://code.google.com/appengine/], το Microsoft Azure [www.microsoft. com/windowsazure/], και το Heroku [http://heroku.com], οι οποίες εκτελούν εφαρμογές προγραμμάτων veamweare (όπως η εικονική μηχανή της Java).



Σχήμα 1.2 Ο πάροχος SaaS παρέχει μία εφαρμογή ή μέρος αυτής στον Υπολογιστή-πελάτη

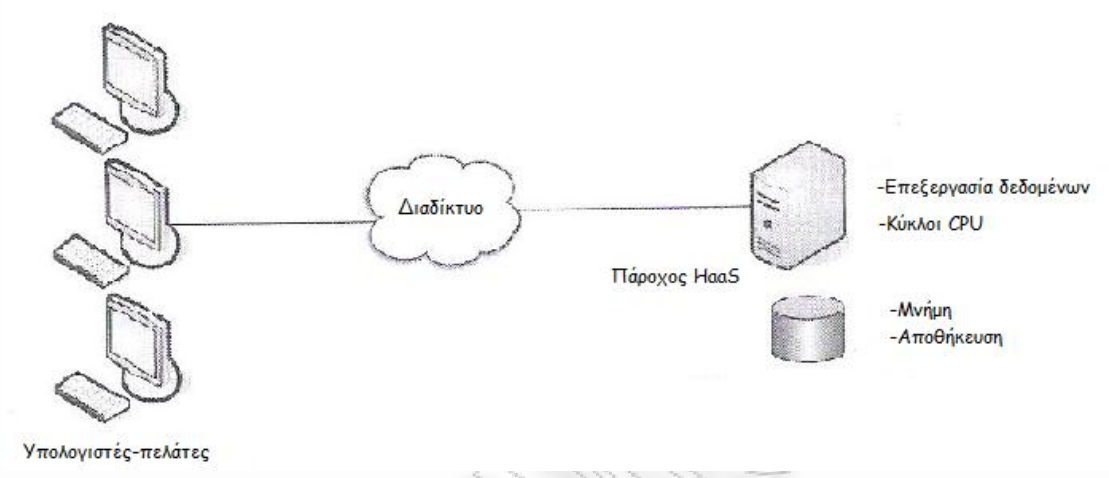
Η πλατφόρμα ως υπηρεσία (Platform as a Service-PaaS) είναι ένα μοντέλο παροχής εφαρμογών το οποίο ακολουθεί από κοντά το λογισμικό ως υπηρεσία(SaaS). Αναλυτικότερα, το μοντέλο PaaS παρέχει όλους τους πόρους που απαιτούνται για να δημιουργηθούν εφαρμογές και υπηρεσίες αποκλειστικά μέσω του διαδικτύου και χωρίς την ανάγκη εγκατάστασης κάποιου λογισμικού (σχήμα 1.3). Προσφέρει υποστήριξη δημιουργίας ενός περιβάλλοντος χρήστη και βασίζεται σε HTML ή Javascript. Βασικό του πλεονέκτημα είναι η υψηλή διαθεσιμότητα, η ελαστικότητα και η ευελιξία με δυνατότητες πλήρους αυτό-διαχείρισης, αυτό-συντήρησης και αυτό-κλιμάκωσης της υποδομής, του λειτουργικού συστήματος και της πλατφόρμας εφαρμογών. Από την άλλη πλευρά, ένα μειονέκτημα αυτού του μοντέλου είναι η έλλειψη δια-λειτουργικότητας και μεταφοράς μιας εφαρμογής από τον έναν πάροχο στον άλλο. Υπηρεσίες που ανήκουν αυτό το μοντέλο είναι το Salesforce [www.salesforce.com/platform/]και το NetSuite [www.netsuite.com /portal/platform/main.shtml].



Σχήμα 1.3 Ο πάροχος PaaS επιτρέπει στον Υπολογιστή-πελάτη την απομακρυσμένη πρόσβαση στην υπολογιστική πλατφόρμα

Το υλικό ως υπηρεσία (Hardware as a Service-HaaS) ή *αλλιώς υποδομή ως υπηρεσία (Infrastructure as a Service-IaaS)* είναι ένα μοντέλο παροχής υπολογιστικών και δικτυακών υποδομών, μέσα από το οποίο ο υπολογιστής-πελάτης μπορεί να υπερ-νοικιάσει υποδομή ανάλογα με τις απαιτήσεις που έχει σε μια t χρονική στιγμή. Αναλυτικότερα, ο πελάτης μπορεί να νοικιάσει πόρους όπως χώρο σε διακομιστή, εξοπλισμό δικτύου, μνήμη, κύκλους CPU και χώρο αποθήκευσης (σχήμα 1.4). Οι πόροι αυτοί τιμολογούνται βάση την χρήση τους και μπορούν να κλιμακωθούν δυναμικά προς τα πάνω ή προς τα κάτω ανάλογα κάθε φορά με τις ανάγκες σε πόρους της κάθε εφαρμογής. Βασικά πλεονεκτήματα του μοντέλου είναι α) η τιμολόγηση με βάση την υπολογιστική χρήση, αφού η χρέωση γίνεται βάση των πόρων του συστήματος που χρησιμοποιούνται και β) το περιβάλλον εικονικής πλατφόρμας, το οποίο επιτρέπει στους υπολογιστές πελάτες να τρέχουν στις

εικονικές μηχανές την εφαρμογή που θέλουν και γ) την δυνατότητα μεταφοράς των εικονικών μηχανών από το περιβάλλον του υπολογιστή-πελάτη στο υπολογιστικό νέφος. Υπηρεσίες που ανήκουν σε αυτό το μοντέλο είναι το Rackspace [www. Rackspacecloud.com], και το Nimbus [http://workspace.globus.org], οι οποίες τρέχουν hardware εικονικών μηχανών όπως ο Xen VM image.



Σχήμα 1.4 Ο πάροχος HaaS επιτρέπει στον Υπολογιστή-πελάτη την ενοικίαση πόρων υλικού

1.5 Μοντέλα Ανάπτυξης στο Υπολογιστικό Νέφος

Το δημόσιο υπολογιστικό νέφος (Public Cloud) είναι ένα μοντέλο το οποίο επιτρέπει την πρόσβαση των χρηστών στο σύννεφο μέσω διεπαφών που χρησιμοποιούν κύρια προγράμματα περιήγησης φυλλομετρητών. Συνήθως βασίζεται στο μοντέλο “pay-per-use” το οποίο είναι αρκετά ευέλικτο και παίρνει υπόψη κάθε φορά την ζήτηση της αγοράς για βελτιστοποίηση του νέφους. Αυτό βοηθά τις επιχειρήσεις/οργανισμούς που υιοθέτησαν το σύννεφο να εκμεταλλευτούν καλύτερα τις δαπάνες πληροφορικής τους σε επιχειρησιακό επίπεδο με τη μείωση των κεφαλαιουχικών δαπανών για την IT υποδομή τους. Τα πλεονεκτήματα του δημόσιου νέφους είναι η χρέωση της υπηρεσίας (χρέωση ανάλογα με την διάρκεια χρήσης της υπηρεσίας νέφους), η μεγάλη ευελιξία λόγω της άμεσης διάθεσης των υπηρεσιών, η άμεση κλιμάκωση σε μικρότερη ή μεγαλύτερη χωρητικότητα και η μεγάλη ελαστικότητα και διαχειρισιμότητα των υπηρεσιών που προσφέρει.

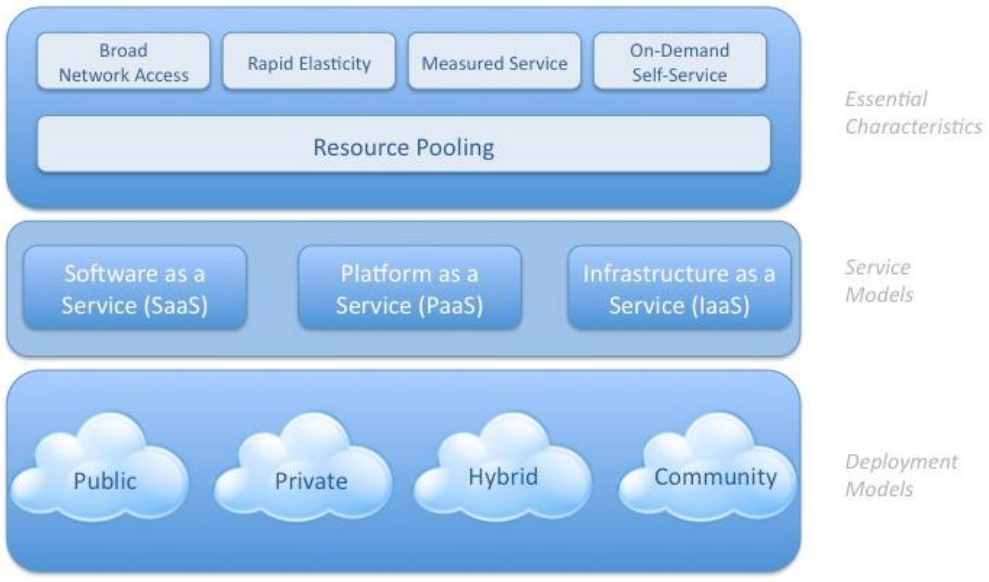
Το ιδιωτικό υπολογιστικό νέφος (Private Cloud) είναι ένα μοντέλο νέφους, το οποίο εγκαθίσταται μέσα στο κέντρο δεδομένων του οργανισμού. Υιοθετεί βασικές αρχές ασφάλειας, νομοθεσίας και κανονιστικών απαιτήσεων αφού προσφέρει μεγάλο έλεγχο εγκατάστασης και χρήσης στην επιχείρηση που το χρησιμοποιεί. Βασική του διαφορά με το δημόσιο νέφος είναι ότι όλοι οι διαθέσιμοι πόροι του νέφους και οι εφαρμογές διαχειρίζονται από τον ίδιο τον

οργανισμό, κερδίζοντας έτσι σε ευελιξία και παραμετροποίηση του συστήματος [4]. Βασικά του πλεονεκτήματα είναι:

- Όλοι οι πόροι του νέφους αποθηκεύονται σε μια κοινόχρηστη πισίνα μέσα στον οργανισμό/επιχείρηση και μπορούν να χρησιμοποιηθούν ανάλογα με τις ανάγκες του κάθε τμήματος,
- Όλες οι διαδικασίες μέσα στον οργανισμό μπορούν να αυτοματοποιηθούν,
- Τα τμήματα του οργανισμού/επιχείρησης μπορούν να αιτηθούν τις υπηρεσίες του νέφους όταν τις χρειάζονται (on-demand),
- Μπορεί να χρησιμοποιηθεί για απεριόριστο εύρος ζώνης.

Το υβριδικό υπολογιστικό νέφος (Hybrid Cloud) είναι ένα ιδιωτικό νέφος που συνδέεται με μία ή περισσότερες εξωτερικές υπηρεσίες νέφους. Η διαχείριση του είναι κεντρικοποιημένη, λειτουργεί ως ενιαία μονάδα και οριοθετείται από ένα ασφαλές δίκτυο. Παρέχει εικονικές λύσεις πληροφορικής μέσα από ένα συνδυασμό δημόσιου και ιδιωτικού νέφους. Τα υβριδικά νέφη παρέχουν ασφαλή έλεγχο των δεδομένων και των εφαρμογών και επιτρέπουν στις εμπλεκόμενες οντότητες να έχουν πρόσβαση σε πληροφορίες μέσω του διαδικτύου. Τέλος υιοθετεί μια ανοιχτή αρχιτεκτονική, η οποία επιτρέπει την διασύνδεση με άλλα συστήματα διαχείρισης [5].

Το κοινοτικό νέφος (Community Cloud) είναι ένα μοντέλο νέφους, το οποίο μοιράζεται σε διάφορους οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινά ενδιαφέροντα (απαιτήσεις ασφάλειας, θέματα συμμόρφωσης). Η διαχείριση του μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτες οντότητες και μπορεί να υλοποιηθεί εντός ή εκτός των συνόρων ενός οργανισμού.



Σχήμα 1.5 Αναπαράσταση υπολογιστικού νέφους, οριζόμενο από τα 5 χαρακτηριστικά του, τα 3 μοντέλα υπηρεσιών και τα 4 μοντέλα ανάπτυξής του [1]

1.6 Το Υπολογιστικό Νέφος και ο νέος ρόλος του τμήματος πληροφορικής (IT)

Για πολλούς, ο όλος θόρυβος περί Υπολογιστικού νέφους ίσως είναι υπερβολικός. Για άλλους πάλι, η ιδέα ότι «ο καλύτερος υπολογιστής είναι η απουσία υπολογιστή» ακούγεται πολύ ελκυστική. Το σίγουρο είναι ότι το Υπολογιστικό νέφος αποτελεί θεμελιώδη αλλαγή, αντίστοιχη της μετάβασης από custom λογισμικό σε standard πακέτα στον τομέα των εφαρμογών. Με τη SalesForce.com να προωθεί τις λύσεις της με σλόγκαν «no software» και το Amazon Elastic Computing Cloud να υπόσχεται «no hardware», θα μπορούσε κανείς να σκεφτεί ότι για τον μέσο IT Manager αυτό σημαίνει «no job!». Κάτι τέτοιο προφανώς δεν έχει βάση, αλλά το σίγουρο είναι ότι ο ρόλος του IT αλλάζει σημαντικά.

Η διαχείριση ενός περιβάλλοντος νέφους διαφέρει από αυτή του παραδοσιακού περιβάλλοντος. Τους εξυπηρετητές που χρησιμοποιεί το IT από το EC2 δεν μπορεί να τους διαχειριστεί το ίδιο, ούτε μπορεί την εφαρμογή CRM που χρησιμοποιείται ως υπηρεσία να την μετακινήσει σε άλλο εξυπηρετητή. Αυτό που μπορεί, είναι να μετακινήσει εργασίες μεταξύ παρόχων νέφους με βάση τη διαθεσιμότητα και το κόστος. Επίσης μπορεί και επιβάλλεται να απαιτεί από τον πάροχο, παροχή πληροφορίας για την online διαθεσιμότητα, ώστε τα συστήματά παρακολούθησης να μπορούν να ειδοποιούν για τυχόν θέματα, πριν αυτά προκύψουν.

Σε ένα όμως περιβάλλον νέφους, ο IT Operations Manager γίνεται πλέον IT Operations Planner και ο σωστός σχεδιασμός χωρίς σωστή πληροφόρηση είναι αδύνατος. Για να παρθούν αποφάσεις ως προς το ποιες εφαρμογές και ποιοι πόροι θα χρειαστούν, είναι απαραίτητη η ύπαρξη ενός Service Model, το οποίο αποτυπώνεται σε μια CMDB/CMS (Configuration Management Database/ System) λύση.

Κάτι που το IT μπορεί να παρακολουθήσει είναι το δίκτυο, αλλά στο προσεχές μέλλον, καθώς η πρόσβαση σε εφαρμογές δεν θα γίνεται αποκλειστικά μέσω του δικτύου της εταιρείας, αλλά θα υπάρχει απευθείας επικοινωνία μεταξύ εφαρμογών και virtual machines, το IT θα πρέπει να συμβιβαστεί με την ιδέα ότι χάνει μέρος του ελέγχου του, και το απλό «μπλοκάρισμα» μιας υπηρεσίας δεν θα είναι πια αποδεκτό.

Από την άλλη μεριά, το IT μπορεί να καθορίσει πολιτικές και διαδικασίες που θα πρέπει να ακολουθούν οι χρήστες. Επιπρόσθετα, μπορεί να συμφωνήσει με τους παρόχους νέφους να λαμβάνει πληροφορία πραγματικού χρόνου για τη χρήση, την απόδοση και τη διαθεσιμότητα, χρησιμοποιώντας standard APIs που θα τροφοδοτούν τα συστήματα παρακολούθησης και τα Service Level Agreement (SLA) του IT.

Παράλληλα όμως, μια πιο θετική προσέγγιση μπορεί να σημαίνει ένα νέο ρόλο του IT, ο οποίος αντί να επιδίδεται στο να απαγορεύει σχεδόν τα πάντα, να καταφέρνει την χρήση των εγκεκριμένων υπηρεσιών να είναι σημαντικά ευκολότερη από αυτή των μη εγκεκριμένων, με τη χρήση π.χ. ενός καταλόγου (Service Catalog) από προπληρωμένες υπηρεσίες, όλες διαθέσιμες με single sign-on, διαφανώς ολοκληρωμένες μεταξύ τους [6].

Νέες, λεπτές ισορροπίες

Η τελική επιτυχία ενός οποιουδήποτε οργανισμού, όσο αποδοτική και αν είναι η λειτουργία του, εξαρτάται από το χαρτοφυλάκιο των προϊόντων του και η Πληροφορική δεν αποτελεί εξαίρεση. Τα ερωτήματα όμως που γεννιούνται από αυτήν την προσδοκία είναι τα εξής

Πώς μπορεί το IT να εξασφαλίσει ότι το τελικό αποτέλεσμα θα είναι το βέλτιστο και ότι θα παρέχονται οι σωστές υπηρεσίες;

Το πρώτο πράγμα που πρέπει να γίνει είναι η διαχείριση του χαρτοφυλακίου των υπηρεσιών ή των εφαρμογών. Το IT πρέπει να εμπλακεί στην επιλογή των υπηρεσιών και εφαρμογών του οργανισμού, απλά επειδή το IT είναι αυτό που θα θεωρηθεί υπόλογο για τους όποιους σχετικούς κινδύνους.

Τι θα γίνει αν ο προμηθευτής παύσει τη λειτουργία του ή αν αυξήσει την ισχύ του στην αγορά πέραν των λογικών ορίων;

Το IT θα πρέπει να παρέχει μια στρατηγική disaster recovery και «εξόδου» για κάθε εφαρμογή και υπηρεσία. Η ευθύνη της εξασφάλισης μιας σωστής ισορροπίας μεταξύ επενδύσεων, κινδύνων και πόρων, επιβάλλουν το Project Portfolio Management (PPM), αλλά και ευρύτερα το ήδη προτεινόμενο και από το ITIL, Service Portfolio & Catalog Management, ως οι βασικές και απαραίτητες πλέον δεξιότητες του IT.

Η υποστήριξη είναι μια άλλη βασική ευθύνη του IT;

Εάν ο οργανισμός χρησιμοποιεί δέκα διαφορετικές SaaS εφαρμογές, το IT είτε θα αφήνει τους μεμονωμένους χρήστες να απευθύνονται απευθείας στους αντίστοιχους προμηθευτές για υποστήριξη και να ανοίγουν tickets σε πολλά διαφορετικά σημεία, είτε θα κρατήσει το πρώτο επίπεδο υποστήριξης εσωτερικά χρησιμοποιώντας μια υπηρεσία Service Desk.

Αλλά τα καθήκοντα του IT δεν σταματούν εκεί… Εάν ο οργανισμός χρησιμοποιεί CRM από έναν πάροχο και ERP από άλλον, το IT θα έχει την ευθύνη της σύνδεσης των δύο. Στην πραγματικότητα, η συνδεσιμότητα θα είναι το βασικότερο κριτήριο επιλογής των συγκεκριμένων παρόχων.

Κεφάλαιο 2ο Κίνδυνοι Απειλές και Ασφάλεια στο Υπολογιστικό Νέφος

2.1 Κίνδυνοι που προκύπτουν από την επιλογή παρόχου

Το υπολογιστικό νέφος παρέχει την δυνατότητα αποσύνδεσης μιας επιχείρησης από την υλοποίηση και συντήρηση των αναγκαίων IT υποδομών, αφού τις προσφέρει ως μορφή υπηρεσίας στον πελάτη. Ο πελάτης συνδέεται στην υποδομή του παρόχου και χρησιμοποιεί τις υπηρεσίες και τις εφαρμογές που πια υπάρχουν πάνω στο σύννεφο. Ένα όμως κρίσιμο ερώτημα που γεννιέται είναι η ανάγκη ασφάλειας των δεδομένων πάνω στο σύννεφο. Η εξασφάλιση της ασφάλειας των πληροφοριών και ιδιαίτερα της διαθεσιμότητας των δεδομένων απαιτούν την ύπαρξη δραστηριοτήτων διαχείρισης κινδύνου. Βέβαια, ένας σημαντικός παράγοντας είναι ότι αναπτύσσεται μια καινούργια σχέση μεταξύ της επιχείρησης και ενός τρίτου οργανισμού (πάροχος υπολογιστικού νέφους). Η διαμόρφωση της σχέσης αυτής επηρεάζεται από το επιχειρηματικό μοντέλο του παρόχου, από την οργάνωσή του και από την εταιρική του κουλτούρα, παράγοντες δηλαδή που επηρεάζουν άμεσα την ασφάλεια των δεδομένων της επιχείρησης που αποφασίζει να εναποθέσει τη διαχείριση τους στην υποδομή του παρόχου.

Κίνδυνοι που αφορούν την χρήση υπηρεσιών υπολογιστικού νέφους μέσα από την επιλογή παρόχου είναι οι ακόλουθοι:

- Η επιλογή του παρόχου αποτελεί έναν σημαντικό κίνδυνο, αφού η φήμη, το ιστορικό και η βιωσιμότητά του είναι στοιχεία βασικής επιλογής και πρέπει να εξεταστούν προκειμένου η επιλογή του παρόχου να είναι η βέλτιστη από άποψη διαθεσιμότητας και ασφάλειας των επιχειρηματικών δεδομένων. Συγκεκριμένα, η βιωσιμότητα του παρόχου αποτελεί ανασταλτικό παράγοντα διότι εξασφαλίζει ότι οι παρεχόμενες υπηρεσίες θα είναι διαθέσιμες και ως εκ τούτου τα δεδομένα μπορούν να υφίστανται πάνω στο σύννεφο και να εξασφαλίζεται η παρακολούθηση της διαχείρισης τους.

- Ένας δεύτερος κίνδυνος είναι η αδυναμία εκπλήρωσης των υποχρεωτικών υπηρεσιών του παρόχου η οποία μπορεί να έχει επιπτώσεις στην εμπιστευτικότητα και την διαθεσιμότητα των πληροφοριών, μιας και επηρεάζουν τις δραστηριότητες μιας επιχείρησης.

- Τρίτος και σημαντικός κίνδυνος που αναδύεται είναι η πρόσβαση τρίτων οντοτήτων σε κρίσιμες πληροφορίες η οποία μπορεί να οδηγήσει σε μη εξουσιοδοτημένη αποκάλυψη των πληροφοριών.

- Η έλλειψη κανονιστικής συμμόρφωσης αποτελεί έναν ακόμα κίνδυνο που προκύπτει από την ανάληψη ευθυνών σε περίπτωση παραβίασης των δεδομένων στο υπολογιστικό νέφος. Στην σύμβαση μεταξύ παρόχου και επιχείρησης/οργανισμού-πελάτη πρέπει να καταγράφεται ρητώς και αδιαμφισβήτητα η ευθύνη κάθε ενέργειας και οι τομείς στους οποίους ο πάροχος είναι υπεύθυνος και υπόλογος για τις επιπτώσεις που αφορούν την ασφάλεια των πληροφοριών.

- Πέμπτος και αδιαμφισβήτητα σοβαρός κίνδυνος είναι η μη διαθεσιμότητα των πληροφοριών σε περίπτωση καταστροφής λόγω του ότι δεν μπορεί να προσδιορισθεί που είναι ακριβώς αποθηκευμένα τα δεδομένα στο υπολογιστικό νέφος. Δεδομένου του κινδύνου αυτού, πρέπει να υπάρχει συνεχής έλεγχος των σχεδίων ανάκαμψης από καταστροφή και λήψη από τον πάροχο όλων των σχετικών μέτρων προστασίας που αφορούν την ύπαρξη αντιγράφων ασφαλείας για την ανάκτηση υπηρεσιών μετά από ενδεχόμενη καταστροφή.

2.2 Τα οφέλη της ασφάλειας στο Υπολογιστικό Νέφος

Παρόλο που το μεγαλύτερο εμπόδιο που αντιμετωπίζει το υπολογιστικό σύννεφο είναι η ασφάλεια, σε κάποιες περιπτώσεις μικρών οργανισμών μπορεί να παρέχει καινοτόμες παροχές ασφάλειας και βελτίωσης της συνολικής τους εικόνας. Πιο συγκεκριμένα, οι τομείς βελτίωσης που μπορούν οι μικρές επιχειρήσεις να αποκτήσουν οφέλη από την μετάβαση σε ένα δημόσιο υπολογιστικό νέφος είναι οι ακόλουθοι [3]:

- *Η Εξειδίκευση του προσωπικού*: Το διοικητικό προσωπικό και τα στελέχη του τμήματος πληροφορικής μπορούν να εκπαιδευτούν σε θέματα ασφάλειας εκμεταλλευόμενοι την αύξηση της υπολογιστικής δύναμης του νέφους. Επιπρόσθετα, εμφανίζεται η λήψη διορθωτικών μέτρων στον οργανισμό, με ένα σύνολο διαφορετικών καθηκόντων του προσωπικού.
- *Η "αντοχή" της πλατφόρμας*: Η δομή της πλατφόρμας του υπολογιστικού νέφους είναι πιο ομοιόμορφη από τις υπάρχουσες παραδοσιακές πλατφόρμες υπολογιστικής δύναμης. Η μεγαλύτερη ομοιομορφία και ομοιογένεια της, επιτρέπει την αποδοτικότερη αυτοματοποίηση της ασφάλειας όπως ο έλεγχος της διαμόρφωσης, οι έλεγχοι ευπάθειας, οι έλεγχοι ασφάλειας και η επιδιόρθωση των κύριων στοιχείων ασφαλείας της πλατφόρμας.

- *Η Διαθεσιμότητα των πόρων*: Η επεκτασιμότητα του Υπολογιστικού νέφους επιτρέπει μεγαλύτερη διαθεσιμότητα. Οι δυνατότητες του πλεονάζοντος προσωπικού και του σχεδίου αποκατάστασης καταστροφής είναι ενσωματωμένες στο νέφος και έτσι η κατόπιν ζήτησης (on demand) διάθεση των πόρων μπορεί να χρησιμοποιηθεί για μεγαλύτερη ανθεκτικότητα. Αυτό σημαίνει ότι ένας οργανισμός μπορεί να αντιμετωπίσει μια αυξημένη ζήτηση υπηρεσιών ή να ανακάμψει γρηγορότερα σε περίπτωση κατανεμημένης επίθεσης άρνησης εξυπηρέτησης (Distributed Denial of Service-DDoS Attack).
- *Η Δημιουργία αντιγράφων ασφαλείας και σημείου επαναφοράς*: Τα δεδομένα που διατηρούνται σε έναν πάροχο νέφους έχουν μεγαλύτερη διαθεσιμότητα και μικρότερο χρόνο αποκατάστασης σε περίπτωση καταστροφής σε σύγκριση με ένα παραδοσιακό "Data Center". Επίσης οι υπηρεσίες που προσφέρονται σε ένα υπολογιστικό νέφος μπορούν να χρησιμοποιηθούν από έναν οργανισμό ως μέσο αποθήκευσης των αντιγράφων ασφαλείας αντί της παραδοσιακής κασέτας αποθήκευσης δεδομένων.
- *Η Κινητικότητα τελικών σημείων*: Η αρχιτεκτονική του νέφους εκτείνεται στον οργανισμό-πελάτη με μορφή υπηρεσίας τελικού σημείου, έτσι ώστε να το χρησιμοποιήσει για τις φιλοξενούμενες εφαρμογές. Τα προγράμματα πελάτες του νέφους μπορεί να είναι βασισμένα είτε σε φυλλομετρητές περιήγησης είτε σε εφαρμογές. Δεδομένο ότι όλοι η υπολογιστική δύναμη είναι βασισμένη στον πάροχο του νέφους, τα προγράμματα πελάτες είναι υπολογιστικά ελαφριά και υποστηρίζονται εύκολα από φορητές συσκευές όπως Tablet PCs και Smart Phones.
- *Η Συγκέντρωση δεδομένων*: Όλα τα δεδομένα διατηρούνται και υποβάλλονται σε επεξεργασία στο σύννεφο και όχι σε κάποια φορητή συσκευή ή αφαιρούμενο αποθηκευτικό μέσο όπου η κλοπή και η απώλεια των δεδομένων είναι σύνηθες φαινόμενο.
- *Ο Προσανατολισμός του κέντρου δεδομένων*: Οι υπηρεσίες του νέφους μπορούν να χρησιμοποιηθούν για την βελτίωση της ασφάλειας του κέντρου δεδομένων (data center). Για παράδειγμα, το ηλεκτρονικό ταχυδρομείο μπορεί να ανακατευθυνθεί σε έναν πάροχο νέφους μέσω των αρχείων ανταλλαγής μηνυμάτων. Στη συνέχεια εξετάζει και αναλύει συλλογικά παρόμοιες πράξεις από άλλα κέντρα δεδομένων για να ανακαλύψει επιθέσεις spam, phishing, και malware, και έτσι να εκτελέσει διορθωτικά μέτρα (π.χ. καραντίνα ύποπτων μηνυμάτων βάση περιεχομένου).
- *Ο Προσανατολισμός του νέφους*: Οι υπηρεσίες του νέφους συσχετίζονται με προϊόντα νέφους όπως είναι ο αντίστροφος proxy, ο οποίος επιτρέπει την "αδέσμευτη" πρόσβαση σε SaaS περιβάλλον, αλλά συγχρόνως διατηρεί κρυπτογραφημένα τα δεδομένα που αποθηκεύονται σε αυτό. Επίσης, στις υπηρεσίες νέφους

συγκαταλέγονται και υπηρεσίες διαχείρισης ταυτοτήτων (identity management) οι οποίες χρησιμοποιούνται για αναγνώριση και αυθεντικοποίηση των χρηστών στο υπολογιστικό νέφος.

2.3 Ευθυγράμμιση των προτύπων ασφάλειας στο Υπολογιστικό σύννεφο

Το υπολογιστικό σύννεφο έχει σχεδιαστεί για να αποκομίσουν αμέτρητα οφέλη όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των παρόχων νέφους (Cloud Providers-CPs), των οργανισμών-πελατών νέφους (Cloud Consumers-CCs), και των παρόχων υπηρεσιών (Service Providers-SPs). Από την άλλη μεριά, το σύννεφο εξακολουθεί να έχει μια σειρά ανοιχτών θεμάτων που επηρεάζουν την αξιοπιστία του. Ένα από τα πιο σημαντικά είναι η ασφάλεια που παρέχεται στο νέφος, μιας και υπάρχει φόβος από την πλευρά του οργανισμού-πελάτη για μια πιθανή απώλεια των δεδομένων του και επιπλέον δεν υπάρχει κάποια εγγύηση ασφάλειας που να καταγράφεται στο συμφωνητικό μεταξύ του οργανισμού-πελάτη και του παρόχου νέφους για τα δεδομένα του πελάτη που αποθηκεύονται σε αυτό. Βάση των παραπάνω εμφανίζονται προκλήσεις και από πιθανούς ανταγωνιστές και από κακόβουλους χρήστες που θέλουν είτε για οικονομικούς είτε για λόγους εκφόβισης να αλλοιώσουν ή να καταστρέψουν τα δεδομένα ενός οργανισμού. Έμφαση δίνεται στα πρότυπα ασφαλείας του ISO 27000 και του NIST-FIMSA, τα οποία δεν καλύπτουν την περίπτωση του υπολογιστικού νέφους. Στις παραγράφους που ακολουθούν παρατίθεται συνοπτικά το πρότυπο του ISO 27000 και οι βελτιώσεις που δέχεται το πρότυπο του NIST-FISMA ώστε να καλύπτει το μοντέλο του υπολογιστικού νέφους.

Το σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) ορίζεται στο ISO27000 ως ένα σύστημα το οποίο παρέχει ένα μοντέλο για την θέσπιση, δημιουργία, παρακολούθηση, ανασκόπηση, διατήρηση και βελτίωση της προστασίας των ηλεκτρονικών αγαθών. Οι προαναφερθέντες λειτουργίες χωρίζονται στις εξής φάσεις:

- *Ορισμός των απαιτήσεων ασφαλείας*: η φάση περιλαμβάνει α) την αναγνώριση των στόχων/σκοπών ασφάλειας που το ISMS πρέπει να ικανοποιεί, β) τη διεξαγωγή ανάλυσης κινδύνου (risk analysis) και την αξιολόγηση για τον εντοπισμό των υφιστάμενων κινδύνων στο εσωτερικό του συστήματος και γ) την λεπτομερής καταγραφή των στόχων / κινδύνων σε απαιτήσεις ασφαλείας και πολιτικές ασφαλείας.
- *Επιβολή των απαιτήσεων ασφάλειας*: η φάση περιλαμβάνει α) την αναγνώριση των ελέγχων ασφάλειας που πρέπει να υλοποιηθούν και β) την εφαρμογή και διαμόρφωση των ελέγχων ασφάλειας βάση συγκεκριμένων απαιτήσεων ασφάλειας.
- *Παρακολούθηση και βελτίωση της ασφάλειας*: η φάση περιλαμβάνει α) την παρακολούθηση των υλοποιημένων ελέγχων ασφάλειας, β) την

ανάλυση της υπαρχούσης κατάστασης ασφάλειας ώστε να προσδιοριστούν τα υφιστάμενα ζητήματα ασφάλειας και γ) την διατήρηση και βελτίωση των υπαρχόντων ελέγχων ασφάλειας

Από την παραπάνω ανάλυση των απαιτήσεων ασφαλείας προκύπτουν ζητήματα όσον αφορά το μοντέλο ασφαλείας του υπολογιστικού νέφους. *Πρώτο ζήτημα* είναι ότι κάθε οντότητα στο νέφος έχει την δικιά της διαδικασία διαχείρισης ασφάλειας (Security Management Process- SMP) και θέλει να την διατηρήσει ή να την επεκτείνει βάση των δικών της αγαθών που φιλοξενούνται στο σύννεφο. *Δεύτερο ζήτημα* που προκύπτει είναι ότι καμία οντότητα (οργανισμός-πελάτης, πάροχος νέφους, πάροχος υπηρεσιών) δεν διατηρεί αυτόνομα ολόκληρη τη διαδικασία ασφάλειας των υπηρεσιών νέφους διότι καμία από αυτές δεν έχει διαθέσιμες όλες τις πληροφορίες που χρειάζονται για την διαχείριση της ασφάλειας ολόκληρου του μοντέλου νέφους. *Τρίτο ζήτημα* είναι η πολλαπλή μίσθωση (multi-tenancy) η οποία απαιτεί διατήρηση διαφορετικών προφίλ ασφάλειας για κάθε οργανισμό-πελάτη που ανήκει στο ίδιο instance. *Τέταρτο ζήτημα* είναι ότι καμία διαδικασία διαχείρισης ασφάλειας (SLA) δεν είναι διαθέσιμη , ώστε να μπορεί να χρησιμοποιηθεί για την διατήρηση συμφωνιών που έχει σχέση με την ασφάλεια των αγαθών στο νέφος. Το *Πέμπτο ζήτημα* αναφέρεται στα υπάρχοντα πρότυπα όπως το ISO27000 και το NIST-FISMA , τα οποία δεν υποστηρίζουν με επάρκεια το μοντέλο του νέφους, διότι τα προαναφερθέντα πρότυπα εξετάζουν την διαδικασία διαχείρισης ασφάλειας από την πλευρά του ιδιοκτήτη πλατφόρμας και όχι από την πλευρά του παρόχου υπηρεσιών (Service Provider-SP).

2.3.1 Βασικές απαιτήσεις ασφάλειας του συστήματος διαχείρισης πληροφοριών του νέφους

Κάθε προτεινόμενο πλαίσιο διαχείρισης ασφάλειας για το μοντέλο του νέφους πρέπει να καλύπτει τις παρακάτω βασικές προϋποθέσεις:

1. Ο οργανισμός-πελάτης υποχρεούται να καθορίσει τις απαιτήσεις ασφάλειας των αγαθών που φιλοξενούνται στο νέφος
2. Ο οργανισμός-πελάτης υποχρεούται να παρακολουθεί την ασφάλεια των αγαθών του
3. Ο πάροχος νέφους πρέπει να παρέχει υποστήριξη πολλαπλής μίσθωσης (multi-tenancy) όπου διαφορετικοί οργανισμοί-πελάτες μπορούν να διατηρούν την δικιά τους διαδικασία διαχείρισης ασφάλειας (SMP) με ισχυρή απομόνωση των δεδομένων.
4. Το σχέδιο διαχείρισης ασφάλειας πρέπει να βασίζεται σε υπάρχοντα πρότυπα διαχείρισης ασφάλειας, τα οποία ήδη τηρούνται απ' τους οργανισμούς-πελάτες και απ' τους παρόχους νέφους (CPs).

Η προσέγγιση των Mohemed Almorsy, John Grundy and Amani S. Ibrahim στο [7], βασίζεται στη βελτίωση και υποστήριξη της συνεργασίας μεταξύ των

οντοτήτων του νέφους, οι οποίες έχουν αναπτύξει μια προδιαγραφή ασφάλειας για το νέφος, την οποία και εκτελούν βάση των αναγκών τους.

2.3.2 Ευθυγράμμιση του NIST-FISMA με το μοντέλο του υπολογιστικού σύννεφου

Τα πρότυπα του NIST-FISMA καθορίζουν ένα πλαίσιο για την διαχείριση ασφάλειας των πληροφοριών και των πληροφοριακών συστημάτων. Το πλαίσιο έχει έξι βασικές φάσεις:

1) Κατηγοριοποίηση των υπηρεσιών ασφάλειας (Service security categorization)
2) Επιλογή των ελέγχων ασφάλειας (Security controls selection)
3) Εφαρμογή των ελέγχων ασφάλειας (Security controls implementation)
4) Αξιολόγηση των ελέγχων ασφάλειας (Security controls assessment)
5) Εξουσιοδότηση των υπηρεσιών (Service authorization)
6) Παρακολούθηση της αποτελεσματικότητας των ελέγχων ασφάλειας (Monitoring the effectiveness of security controls)

Ο πίνακας 1 αναπαριστά την ευθυγράμμιση των προτύπων του NIST-FISMA με το μοντέλο του υπολογιστικού νέφους.

ΦΑΣΗ	ΚΑΘΗΚΟΝΤΑ	ΠΑΡΟΧΟΣ ΝΕΦΟΥΣ	ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ	ΟΡΓΑΝΙΣΜΟΣ-ΠΕΛΑΤΗΣ	ΕΙΣΟΔΟΣ ΣΤΟΙΧΕΙΩΝ	ΕΞΟΔΟΣ ΑΠΟΤΕΛΕΣΜΑΤΩΝ
Κατηγοριοποίηση των υπηρεσιών ασφάλειας	Κατηγοριοποίηση των επιπτώσεων ασφαλείας	Ενημερωμένος	Ενημερωμένος	Υπεύθυνος	Επιχειρηματικοί στόχοι	Βαθμός επιπτώσεων
Επιλογή των ελέγχων ασφάλειας	Καταγραφή ελέγχων ασφάλειας	Υπεύθυνος			Λίστα ελέγχων	Καταγραφή ελέγχων ασφάλειας
	Δημιουργία ελέγχων ασφάλειας	Υπεύθυνος			Κατηγοριοποίηση ασφάλειας &εισαγωγή ελέγχων	Αρχικοί έλεγχοι & καταλληλότητα αυτών
	Αξιολόγηση των κινδύνων που διατρέχουν οι υπηρεσίες	Υπεύθυνος			αρχιτεκτονική πλατφόρμας, έκθεση ευπαθειών &καταμέτρηση γνωστών αδυναμιών	Αναγνώριση απειλών, ευπαθειών και κινδύνων
	Παραμετροποίηση των ελέγχων ασφάλειας	Υπεύθυνος			Αξιολόγηση κινδύνων	Σχέδιο διαχείρισης ασφάλειας
Εφαρμογή ελέγχων	Εφαρμογή ελέγχων ασφάλειας	Υπεύθυνος			Σχέδιο διαχείρισης ασφάλειας	Αναβάθμιση σχεδίου ασφάλειας
Αξιολόγηση των ελέγχων ασφάλειας	Ορισμός μετρικών ασφαλείας	Υπεύθυνος	Ενημερωμένος	Υπεύθυνος	Στόχος ασφάλειας	Σχέδιο αξιολόγησης ασφάλειας
	Αξιολόγηση της κατάστασης ασφάλειας	Υπεύθυνος			Σχέδιο αξιολόγησης ασφάλειας	Έκθεση αξιολόγησης
Εξουσιοδότηση των υπηρεσιών	Εξουσιοδότηση υπηρεσιών	Ενημερωμένος	Ενημερωμένος	Υπεύθυνος	Σχέδιο ασφάλειας & έκθεση αξιολόγησης	Εξουσιοδότηση υπηρεσιών
Παρακολούθηση της αποτελεσματικότητας των ελέγχων ασφάλειας	Παρακολούθηση της κατάστασης ασφάλειας	Υπεύθυνος			Σχέδιο αξιολόγησης ασφάλειας	Έκθεση της τελικής κατάστασης ασφαλείας

Πίνακας 1 Ευθυγράμμιση των προτύπων του NIST-FISMA με το μοντέλο του υπολογιστικού νέφους [2]

1) *Η κατηγοριοποίηση των υπηρεσιών ασφάλειας*: κάθε υπηρεσία (S_j) στην πλατφόρμα του νέφους μπορεί να χρησιμοποιηθεί για διαφορετικούς οργανισμούς-πελάτες. Κάθε οργανισμός πελάτης (T_i) που νοικιάζει την υπηρεσία κατέχει μόνο τις πληροφορίες του στα πλαίσια των διαμοιρασμένων υπηρεσιών (S_j). Ο οργανισμός-πελάτης είναι η μόνη οντότητα που μπορεί να αποφασίσει/αλλάξει τις επιπτώσεις απ' την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών βάση των επιχειρηματικών του στόχων. Επιπλέον, κάθε οργανισμός-πελάτης μπορεί να συμφωνήσει/δεχτεί διαφορετικά επίπεδα επιπτώσεων (χαμηλά, μεσαία, υψηλά), όσον αφορά τις παραβιάσεις ασφάλειας των πληροφοριών του. Η κατηγοριοποίηση των υπηρεσιών ασφάλειας μπορεί να γίνει ανά οργανισμό-πελάτη ή ανά υπηρεσία. Αναλυτικότερα, η κατηγοριοποίηση υπολογίζεται ως εξής:

SC (T_i) =[(εμπιστευτικότητα, επίπτωση), (ακεραιότητα, επίπτωση), (διαθεσιμότητα, επίπτωση)]
Η επίπτωση μπορεί να είναι [χαμηλή, μεσαία, υψηλή]

Εξίσωση (1)

SC (S_j) = [(εμπιστευτικότητα, μέγιστο για κάθε T_i (επίπτωση)]
[(ακεραιότητα, μέγιστο για κάθε T_i (επίπτωση)]
[(διαθεσιμότητα, μέγιστο για κάθε T_i (επίπτωση)]

SC=security categorization (κατηγοριοποίηση ασφάλειας)

Εξίσωση (2)

2) *Η επιλογή των ελέγχων ασφάλειας*: η επιλογή των ελέγχων ασφάλειας για την προστασία των αγαθών των οργανισμών-πελατών έχει δύο στάδια: α) Το πρώτο στάδιο είναι η αρχική επιλογή των ελέγχων ασφάλειας (τα πρότυπα του FISMA), οι οποίοι παρέχουν έναν κατάλογο από πρότυπους ελέγχους ασφάλειας κατηγοριοποιημένους σε τρία βασικά επίπεδα (χαμηλό, μεσαίο, υψηλό). Βασιζόμενη στην κατηγοριοποίηση ασφάλειας του οργανισμού-πελάτη ή της υπηρεσίας, επιλέγονται οι αρχικοί έλεγχοι, οι οποίοι προσδοκάται να παρέχουν το απαιτούμενο επίπεδο ασφάλειας που καθορίζεται απ' τον οργανισμό-πελάτη. β) δεύτερο στάδιο ορίζεται η παραμετροποίηση των ελέγχων ασφάλειας βάση των αναγνωρισμένων πιθανών ευπαθειών απειλών, κινδύνων και άλλων περιβαλλοντικών παραγόντων που είναι οι εξής:

   i. *Διαδικασία αξιολόγησης κινδύνων* (Risk assessment process)- Αρχική επιλογή ελέγχων ασφάλειας
      - Αναγνώριση ευπαθειών: σ' αυτό το βήμα, ο οργανισμός-πελάτης πρέπει να είναι γνώστης της υπηρεσίας και της αρχιτεκτονικής του λειτουργικού περιβάλλοντος. Ως αποτέλεσμα, εμπλέκεται και ο πάροχος υπηρεσιών

(SP), ο οποίος γνωρίζει την δομή της παρεχόμενης υπηρεσίας και ο πάροχος νέφους (CP) ο όποιος γνωρίζει την αρχιτεκτονική της πλατφόρμας του νέφους.

- Αναγνώριση απειλών: οι πιθανές απειλές και οι πηγές αυτών μπορούν να αναγνωριστούν απ' την συνεργασία του παρόχου υπηρεσιών, του παρόχου νέφους και του οργανισμού πελάτη. Ο τελευταίος εμπλέκεται περισσότερο σ' αυτή τη διαδικασία διότι γνωρίζει καλύτερο απ' τον καθένα την αξία αγαθών του και την πιθανή πηγή των παραβιάσεων ασφαλείας στον οργανισμό του.
- Πιθανότητα κινδύνου: υπολογίζεται με βάση: α) τις δυνατότητες των πηγών κινδύνου και β) τη φύση των υπαρχόντων ευπαθειών, η οποία βαθμολογείται ανάλογα ως χαμηλή, μεσαία ή υψηλή.
- Επίπεδο κινδύνου: υπολογίζεται ως η επίπτωση επί την πιθανότητα κινδύνου (επίπεδο κινδύνου= επίπτωση * πιθανότητα κινδύνου).

ii. *Παραμετροποίηση των ελέγχων ασφάλειας*: βασισμένη στην διαδικασία αξιολόγησης κινδύνου, η παρούσα διαδικασία μπορεί να σχεδιαστεί έτσι ώστε να περιορίσει νέους κινδύνους και να προσαρμοστεί με τις νέες συνθήκες περιβάλλοντος ως εξής:

- Σκοπός των ελέγχων ασφάλειας: α) αναγνώριση των υπαρχόντων ελέγχων ασφάλειας (στο περιβάλλον του οργανισμού-πελάτη) και αντικατάσταση μερικών εξ' αυτών είτε με καινούργιους, είτε με ελέγχους ασφάλειας που εφαρμόζει ο πάροχος νέφους. β) διαχωρισμός των στοιχείων του συστήματος σε κρίσιμα και μη. Συγκεκριμένα, ο πάροχος υπηρεσιών και ο οργανισμός-πελάτης πρέπει να ορίσουν ποια στοιχεία είναι κρίσιμα ώστε να ενδυναμώσουν την ασφάλεια σε αυτά, και ποια δεν είναι κρίσιμα οπότε δεν υπάρχει πιθανότητα παραβίασης ασφάλειας. γ) προσδιορισμός της τεχνολογίας και του περιβάλλοντος που σχετίζονται με τους ελέγχους ασφάλειας (π.χ όταν χρησιμοποιηθεί ασύρματο δίκτυο απαιτείται να χρησιμοποιηθούν έλεγχοι ασφαλείας γι αυτό).
- Αντιστάθμιση των ελέγχων ασφάλειας: όποτε οι εμπλεκόμενες οντότητες (CC,CP,SP) ανακαλύψουν ότι ένας ή περισσότεροι έλεγχοι ασφάλειας δεν ταιριάζουν με τις συνθήκες περιβάλλοντος, τότε πρέπει να

αντικαταστήσουν αυτούς τους ελέγχους με ελέγχους παραγωγικούς για το περιβάλλον τους.

- Οριοθέτηση παραμέτρων στους ελέγχους ασφάλειας: σ' αυτό το βήμα γίνεται η παραμετροποίηση των ελέγχων ασφάλειας, η οποία επιτυγχάνεται από την συνεργασία των παρόχων νέφους με τους οργανισμούς-πελάτες. Το αποτέλεσμα από το βήμα είναι ένα σχέδιο διαχείρισης ασφάλειας, το οποίο καταγράφει α) την κατηγοριοποίηση της ασφάλειας υπηρεσιών, β) τους κινδύνους, γ) τις ευπάθειες και δ) τους τελικούς (αναδιαμορφωμένους) ελέγχους ασφάλειας.

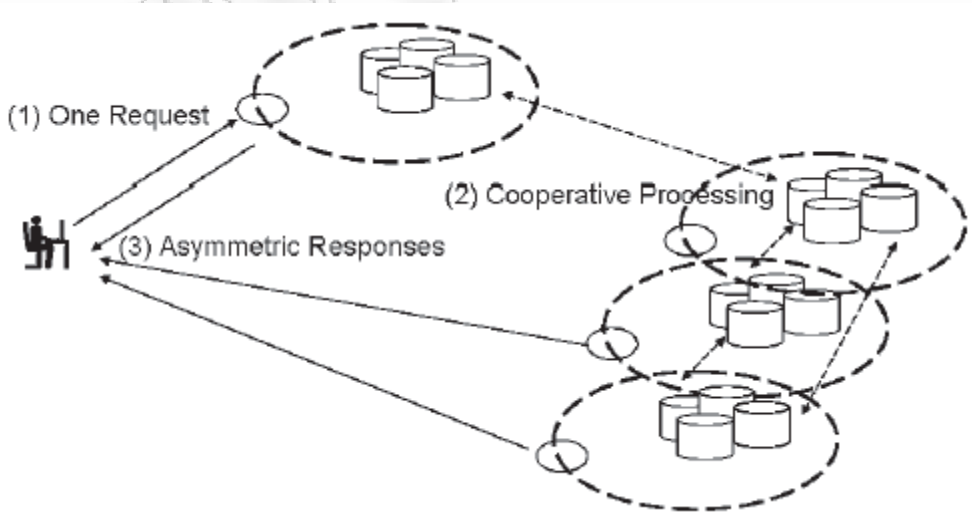
3) *Εφαρμογή των ελέγχων ασφάλειας*: το σχέδιο ασφάλειας για κάθε οργανισμό-πελάτη περιγράφει τους ελέγχους ασφάλειας που πρέπει να υλοποιηθούν από κάθε εμπλεκόμενη οντότητα βασισμένη στην κατηγορία των ελέγχων ασφάλειας. Η εφαρμογή των κοινών ελέγχων είναι υπευθυνότητα είτε του παρόχου νέφους (σε περίπτωση εσωτερικών ελέγχων ασφάλειας) είτε του οργανισμού-πελάτη (σε περίπτωση εξωτερικών ελέγχων). Η εφαρμογή των ελέγχων ασφάλειας συγκεκριμένων υπηρεσιών είναι υπευθυνότητα του παρόχου υπηρεσιών. Κάθε εμπλεκόμενη οντότητα πρέπει να καταγράφει τη διαδικασία υλοποίησης των ελέγχων ασφάλειας στο σχέδιο διαχείρισης ασφάλειας (Security Management Plan)
4) *Αξιολόγηση των ελέγχων ασφάλειας*: στην αξιολόγηση των ελέγχων απαιτείται να διασφαλιστεί ότι οι εφαρμοσμένοι έλεγχοι ασφάλειας λειτουργούν κανονικά και καλύπτουν τους καθορισμένους στόχους ασφάλειας. Συγκεκριμένα, η φάση αυτή περιλαμβάνει την δημιουργία ενός σχεδίου αξιολόγησης ασφάλειας που ορίζει ποιοι έλεγχοι πρέπει να αξιολογηθούν, ποια μέθοδος αξιολόγησης πρέπει να χρησιμοποιηθεί, και ποιες είναι οι μετρικές ασφάλειας για κάθε έλεγχο ασφάλειας. Τα αποτελέσματα από την διαδικασία αξιολόγησης καταγράφονται σε μία έκθεση αξιολόγησης ασφάλειας. Σ' αυτή τη φάση τα αποτελέσματα είτε μπορούν να οδηγήσουν σε προηγούμενες φάσεις (σε περίπτωση ελαττωματικών ελέγχων) είτε στις επόμενες (σε περίπτωση ορθών ελέγχων).
5) *Εξουσιοδότηση των υπηρεσιών*: Η φάση αυτή αναπαριστά την επίσημη αποδοχή όλων των οντοτήτων για τους αναγνωρισμένους κινδύνους που περιλαμβάνονται στην υιοθέτηση μιας υπηρεσίας και στην αποδοχή της μετρίασης των κινδύνων αυτών. Το σχέδιο ασφάλειας και το σχέδιο αξιολόγησης αποτελούν την διαδικασία διαχείρισης ασφάλειας γύρω από τις εμπλεκόμενες οντότητες.
6) *Παρακολούθηση της αποτελεσματικότητας των ελέγχων ασφάλειας*: στη φάση αυτή ορίζεται ότι ο πάροχος νέφους πρέπει να παρέχει εργαλεία παρακολούθησης ασφάλειας στον οργανισμό-πελάτη, ο οποίος στη

συνέχεια θα τα χρησιμοποιήσει για να παρακολουθήσει την ασφάλεια των αγαθών του. Τα εργαλεία παρακολούθησης πρέπει να έχουν την δυνατότητα λήψης των απαραίτητων μετρικών ασφαλείας και να βγάζουν ως έξοδο την αναφορά για τα συλλεγμένα μέτρα σε μία έκθεση ασφάλειας είτε βασισμένη στο γεγονός είτε στην περίοδο. Τέλος, τα αποτελέσματα της διαδικασίας παρακολούθησης θα δείξουν αν τα μέτρα που πήραμε είναι ορθά και σωστά υλοποιημένα. Αν όχι, τότε θα χρειαστεί να περάσουν ξανά όλες τις φάσεις (δηλαδή το SMP) ώστε να γίνει σωστή διαχείριση των νέων απροσδόκητων αλλαγών.

2.4 Χρήση τεχνικής διαμοιρασμού μυστικού θέματος για ασφαλή αποθήκευση στο Υπολογιστικό νέφος

Ο Yuji Suga στο [8] αναπτύσσει μια τεχνική διαμοιρασμού μυστικού θέματος (secret sharing schemes) ως προτεινόμενη λύση για την αποθήκευση των δεδομένων στο υπολογιστικό νέφος. Οι απαιτήσεις που χρειάζονται για την υλοποίηση της προτεινόμενης λύσης είναι: η διαφάνεια (transparency) στη ροή δεδομένων και το Lightweightness.

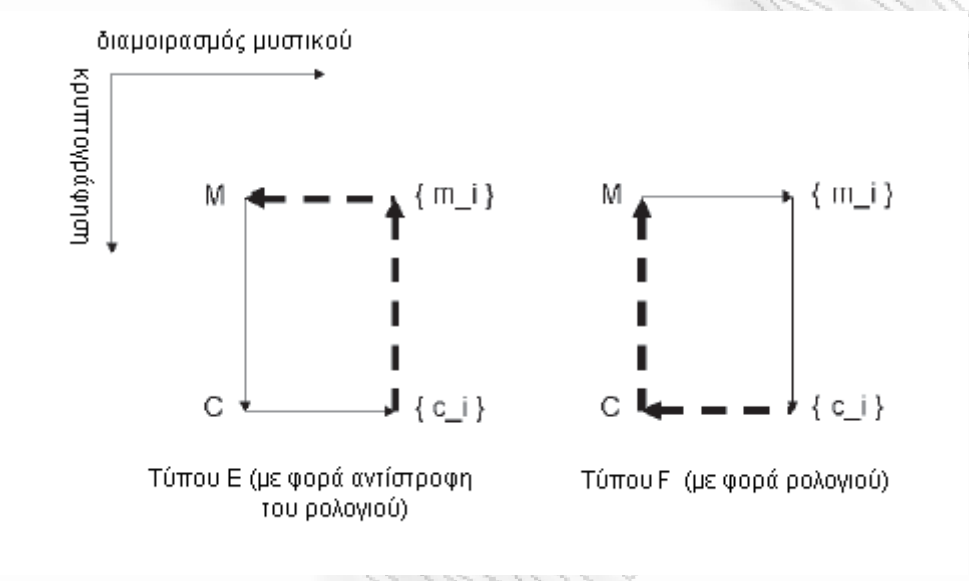
Όταν οι διαχειριστές του νέφους αναπαράγουν τα δεδομένα του πελάτη σε διαφορετικούς διαχειριστές του νέφους τότε ένας από αυτούς μπορεί να αποκτήσει ακούσια παραπάνω από τα θεμιτά προνόμια. Η λύση στο πρόβλημα αυτό είναι η διαφανής λειτουργικότητα της ροής δεδομένων (σχήμα 2.4.1).



Σχήμα 2.4.1 Ασύμμετρες υπηρεσίες υπολογιστικού νέφους [3]

Δεύτερη απαίτηση είναι η μείωση της κρυπτογραφικής επεξεργασίας των δεδομένων κατά την αποθήκευσή τους.

Στο σχήμα 2.4.2 αναπαρίσταται το μοντέλο της ροής δεδομένων. Η κρυπτογράφηση και ο διαμοιρασμός μυστικού είναι ευμετάβλητες, Μ είναι ένα απλό δεδομένο, C ένα κρυπτογραφημένο δεδομένο (με την χρήση συμμετρικού αλγορίθμου)που σχετίζεται με το Μ και Χ ->{xi} και σημαίνει ότι το {xi} είναι διαμοιρασμένο με το Χ εφαρμόζοντας μια τεχνική διαμοιρασμού μυστικού.



Σχήμα 2.4.2 Μοντέλο ροής δεδομένων [4]

Επίσης το μοντέλο του Yuji Suga περιλαμβάνει μια επέκταση του (2, n) VSS συστήματος, το οποίο ονομάζεται γράφημα με βάση τη δομή πρόσβασης. Το γράφημα είναι ένα ζεύγος G = (V,E) το οποίο αποτελείται από ένα σύνολο V το οποίο είναι η κορυφή του σύνολο G και ένα σύνολο Ε αποτελούμενο από 2 υποσύνολα του V και είναι το άκρο του G. Επίσης στο παραπάνω γράφημα γίνεται η υπόθεση ότι δεν περιέχονται βρόχοι, μη κατευθυνόμενες άκρες και πολλαπλές ακμές. Επιπλέον οι 2 κορυφές {vi, vj} μπορούν να έχουν κοινή ακμή αν και μόνο αν οι συμμετέχοντες μπορούν να ανακατασκευάσουν το μυστικό και από τις 2 πλευρές που σχετίζεται με τις {vi, vj}.

Η συγκεκριμένη δομή πρόσβασης έχει εστιάσει στο γεγονός ότι ένας γρήγορος αλγόριθμος ανταλλαγής μυστικού (που χρησιμοποιεί μόνο XoR) και ένας αλγόριθμος Block Cipher (ή Stream Cipher) είναι ευμετάβλητοι οπότε επιτυγχάνετε η απαίτηση Lightweightness.

Κεφάλαιο 3ο Το Υπολογιστικό Σύννεφο στην υπηρεσία της υγείας

3.1 Όροι και προϋποθέσεις της HIPAA για εφαρμογή νέφους στον τομέα της Υγείας

Η HIPAA ορίζει τα ελάχιστα εθνικά πρότυπα για την προστασία των πληροφοριών υγείας ενός ασθενή. Αρχικά δημιουργήθηκε για τον εξορθολογισμό των διαδικασιών της υγειονομικής περίθαλψης και τη μείωση του κόστους, με παράλληλη εξασφάλιση της ιδιωτικότητας των ασθενών.

Η HIPAA καλύπτει όλες τις προστατευόμενες πληροφορίες που έχουν σχέση με την υγεία του ασθενή (Protected Health Information-PHI), δηλαδή οποιαδήποτε πληροφορία σχετικά με την σωματική του ή πνευματική του υγεία, την παροχή υγειονομικής του περίθαλψης και την πληρωμή των συναφών υπηρεσιών υγείας. Επιπρόσθετα, οι προστατευόμενες πληροφορίες (PHI) περιλαμβάνουν και προσωπικές πληροφορίες του ασθενή, όπως το ονοματεπώνυμό του, ο αριθμός της κοινωνικής του ασφάλισης, ο φορέας ασφάλισής του, η ιατρική του κατάσταση και το είδος χρέωσης των υπηρεσιών υγείας. Για να είναι συμβατοί οι οργανισμοί/επιχειρήσεις με την HIPAA, πρέπει να σχεδιάσουν τα συστήματα και τις εφαρμογές τους έτσι ώστε να καλύπτουν τις απαιτήσεις ασφάλειας και ιδιωτικότητας που ορίζει αυτή.

Πιο συγκεκριμένα, οι απαιτήσεις ιδιωτικότητας απαιτούν τις πληροφορίες υγείας του ασθενή να είναι κανονικά προστατευμένες από όλες τις εμπλεκόμενες οντότητες. Επιπρόσθετα, οι κανόνες ιδιωτικότητας απαγορεύουν σε οποιαδήποτε οντότητα να μεταδίδει τις προστατευόμενες πληροφορίες μέσω ανοικτών δικτύων ή να τις κατεβάζει σε δημόσιους ή φορητούς υπολογιστές χωρίς την χρήση κρυπτογράφησης.

Από την άλλη μεριά οι απαιτήσεις ασφάλειας απαιτούν από όλες τις οντότητες να εφαρμόζουν διοικητικές, φυσικές και τεχνικές εγγυήσεις έτσι ώστε να προστατεύονται όλες οι ηλεκτρονικές πληροφορίες υγείας ενός ασθενή (PHI). Για να εφαρμοστεί η παραπάνω απαίτηση, πρέπει όλες οι εμπλεκόμενες οντότητες να εφαρμόζουν ελέγχους πρόσβασης, κρυπτογράφηση δεδομένων, δημιουργία αντιγράφων ασφαλείας και audit ελέγχους για τις ηλεκτρονικές πληροφορίες κατά τρόπο ανάλογο με τον σχετιζόμενο κίνδυνο.

Οι κανονισμοί προστασίας της ιδιωτικότητας στο υπολογιστικό νέφος ορίζουν την εφαρμογή κρυπτογράφησης όλων των προστατευόμενων πληροφοριών κατά την μετάδοση (“in-flight”) και αποθήκευσή τους (“at-rest”). Οι ίδιοι μηχανισμοί ασφάλειας που χρησιμοποιούνται στα παραδοσιακά υπολογιστικά περιβάλλοντα, πρέπει να εφαρμοστούν και στα εικονικά.

Για να διασφαλιστεί ή ασφάλεια των δεδομένων κατά την μετάδοση τους, αρχεία που περιέχουν προστατευμένες ηλεκτρονικές πληροφορίες υγείας, πρέπει να κρυπτογραφηθούν με αλγορίθμους 256 bit κλειδιών, όπως ο αλγόριθμος AES. Επιπρόσθετα, για να μειωθεί ο κίνδυνος έκθεσης των πληροφοριών, κάθε δεδομένο που δεν χρησιμοποιείται από τις εφαρμογές που τρέχουν στο σύννεφο, πρέπει να αφαιρεθεί πριν από την μετάδοση της πληροφορίας.

Μία επιπλέον απαίτηση ασφάλειας είναι η αυθεντικοποίηση στους εικονικούς εξυπηρετητές του υπολογιστικού νέφους που επιτυγχάνεται α) με την χρήση ζεύγος κλειδιού 2048 bit (RSA) και ένα μοναδικό αναγνωριστικό για ασφαλή πρόσβαση και β) με την χρήση διεπαφής (interface) της γραμμής εντολών Shell και κλειδιού Secure Shell (SSH).

Η τρίτη απαίτηση ασφάλειας αναφέρεται στην χρήση του τοίχου προστασίας στο νέφος, το όποιο πρέπει να έχει κλειδωμένο ως επιλογή το “deny-all” και αυτόματα να εμποδίζει όλη την εισερχόμενη κίνηση. Εξαίρεση αποτελεί η περίπτωση που ο ιατροφαρμακευτικός οργανισμός (κατόπιν εντολής της διοίκησης ή του διαχειριστή του συστήματος) επιτρέψει ρητώς να ανοιχτεί μια θύρα (port) για άμεση πρόσβαση. Στην παραπάνω απαίτηση πρέπει να προστεθεί η δημιουργία πολλών ομάδων ασφάλειας (security groups), έτσι ώστε να ενισχυθεί η διαφορετική πολιτική εισόδου-πρόσβασης στις πληροφορίες του ασθενή. Επιπρόσθετα, κάθε ομάδα ασφαλείας θα ελέγχεται μέσω κωδικοποιημένου X509 πιστοποιητικού και θα έχει περιορισμένη πρόσβαση στις υπηρεσίες θυρών, στις πηγαίες IP διευθύνσεις και στα πρωτόκολλα των Instances του υπολογιστικού νέφους.

Η τέταρτη απαίτηση εστιάζει στην δημιουργία και εφαρμογή πολιτικών ασφαλείας έτσι ώστε κάθε πάροχος υπολογιστικού νέφους να έχει περιορισμένη πρόσβαση (και μόνο όπου και αν απαιτείτε) στα δεδομένα του ιατροφαρμακευτικού οργανισμού, στα Instances και στα λειτουργικά συστήματα. Εξαίρεση στον κανόνα αποτελούν περιπτώσεις όπως εάν ο ιατροφαρμακευτικός οργανισμός για λόγους συντήρησης ή αναβάθμισης του συστήματος επιτρέψει στον πάροχο του νέφους να χρησιμοποιήσει τα κρυπτογραφημένα SSH κλειδιά ώστε να έχει πρόσβαση στο λειτουργικό σύστημα. Όταν ολοκληρωθεί η συντήρηση ή αναβάθμιση του συστήματος τότε τα κλειδιά ανακαλούνται και η πρόσβαση του παρόχου δεν είναι πια εφικτή. Όσον αφορά τις απαιτήσεις της πολιτική ασφαλείας από πλευράς ιατροφαρμακευτικού οργανισμού, αυτός οφείλει να κρυπτογραφεί κάθε ευαίσθητο και προστατευόμενο ιατρικό δεδομένο.

Πέμπτη απαίτηση ασφαλείας είναι η διεργασία ελέγχου πρόσβασης (Access Control Process) στα δεδομένα του ασθενή. Η απαίτηση αυτή εμπεριέχει την δημιουργία και εφαρμογή μιας πολιτικής ελέγχου πρόσβασης που βασίζεται

στην πολιτική ασφαλείας του ιατροφαρμακευτικού οργανισμού. Βάση της πολιτικής ελέγχου, ο διαχειριστής του συστήματος μπορεί να έχει πλήρη έλεγχο και εικόνα στο ποιος έχει πρόσβαση και σε ποια δεδομένα και στην συνέχεια να μοιράζει δικαιώματα “Read, Write, Delete, Full Permission” ή να τα αφαιρεί όπου δεν συμφωνούν με την πολιτική πρόσβασης. Επιπρόσθετα, η παραπάνω απαίτηση περιλαμβάνει την εφαρμογή πρωτοκόλλων δικτύου SSH, τα οποία χρησιμοποιούνται για αυθεντικοποίηση των απομακρυσμένων χρηστών μέσω κρυπτογραφίας δημοσίου κλειδιού (PKI). Η διαφύλαξη των κλειδιών και των λογαριασμών είναι σημαντικό ζήτημα για την θεμελίωση της ασφάλειας και ως προτεινόμενα μέτρα για την επίτευξη αυτού, αναφέρονται α) η αποθήκευση των κλειδιών σε μια πισίνα δεδομένων κρυπτογραφημένη από την πλευρά του ιατροφαρμακευτικού οργανισμού και β) η χρήση ασφαλής σύνδεσης (HTTPS) στις διαδικτυακές ιατρικές εφαρμογές από την πλευρά των χρηστών (ιατροφαρμακευτικού προσωπικού, ασθενών).

Η διαδικασία ελέγχου (auditing) είναι η έκτη απαίτηση ασφάλειας και είναι αυτή η οποία επιτρέπει στους αναλυτές ασφάλειας να ελέγξουν λεπτομερώς τα αρχεία καταγραφής δραστηριοτήτων και στην συνέχεια να δημιουργήσουν ένα αρχείο με το ποιος έχει πρόσβαση “που”, ποιες είναι οι είσοδοι των IP διευθύνσεων και ποια δεδομένα έχουν αναγνωστεί ή τροποποιηθεί πρόσφατα. Στην συνέχεια, το αρχείο αυτό πρέπει να αποθηκευτεί σε μια κεντρική τοποθεσία, για ένα μεγάλο χρονικό διάστημα έτσι ώστε ο επόμενος αναλυτής να συγκρίνει τα αποτελέσματα του προηγούμενου ελέγχου με τον τωρινό.
Η δημιουργία και υλοποίηση αντιγράφων ασφαλείας (Back-up) είναι ή έβδομη και πιο σημαντική απαίτηση για κάθε ιατροφαρμακευτικό οργανισμό και πρέπει να στηρίζεται στην πολιτική ασφαλείας του. Σε περίπτωση έκτακτης ανάγκης (πλημμύρα, πυρκαγιά) πρέπει να ανακτηθεί το ακριβές αντίγραφο των ηλεκτρονικών πληροφοριών υγείας και να επαναλειτουργήσει το ιατρικό σύστημα σε σύντομο χρονικό διάστημα. Σήμερα, αρκετοί πάροχοι νέφους (όπως η Amazon με το Elastic Cloud 2-EC2) προσφέρουν προσαρμόσιμη χωρητικότητα στο σύννεφο. Η χωρητικότητα αυτή μπορεί να χρησιμοποιηθεί ως “συσκευή πρότυπης αποθήκευσης μπλοκ” και να προσφέρει άμεση λειτουργικότητα και αποθήκευση που δεν στηρίζεται σε κάποιο Instance. Επιπλέον, κάθε οργανισμός μπορεί να δημιουργήσει snapshots χρονικών στιγμών, τα οποία αποθηκεύονται αυτόματα στο σύννεφο και αναπαράγονται σε πολλαπλές ζώνες διαθεσιμότητας (σε ξεχωριστά κέντρα δεδομένων). Τα snapshots μπορούν να χρησιμοποιηθούν κάθε στιγμή και να διαγραφούν μόνο σε περίπτωση που το ζητήσει ο διαχειριστής του ιατροφαρμακευτικού οργανισμού.

Τελευταία απαίτηση ασφάλειας είναι το σχέδιο αποκατάστασης καταστροφής (Disaster Recovery Plan), το οποίο ορίζεται ως βασική προϋπόθεση ασφάλειας από την HIPAA. Κάθε σχέδιο προϋποθέτει υψηλή διαθεσιμότητα

των συστημάτων και των δεδομένων και συνεχή πρόσβαση σε αυτά. Μέσα από ένα σύνολο μηχανισμών αποκατάστασης που προσφέρουν οι πάροχοι νέφους, ο διαχειριστής του συστήματος σε περίπτωση καταστροφής, πρέπει να ξεκινήσει τα Instances των εικονικών εξυπηρετητών και να χρησιμοποιήσει στατικές IP διευθύνσεις για την μετάβαση των δεδομένων από τον έναν εξυπηρετητή στο άλλον. Τέλος, ο διαχειριστής του συστήματος μπορεί να χρησιμοποιήσει τις πολλαπλές ζώνες διαθεσιμότητας, οι οποίες προσφέρουν μηδενική ανοχή λάθους, είναι ανεκτικές σε περιπτώσεις φυσικών καταστροφών και διασφαλίζουν 99,9% διαθεσιμότητα, για την αποκατάσταση του ιατρικού συστήματος.

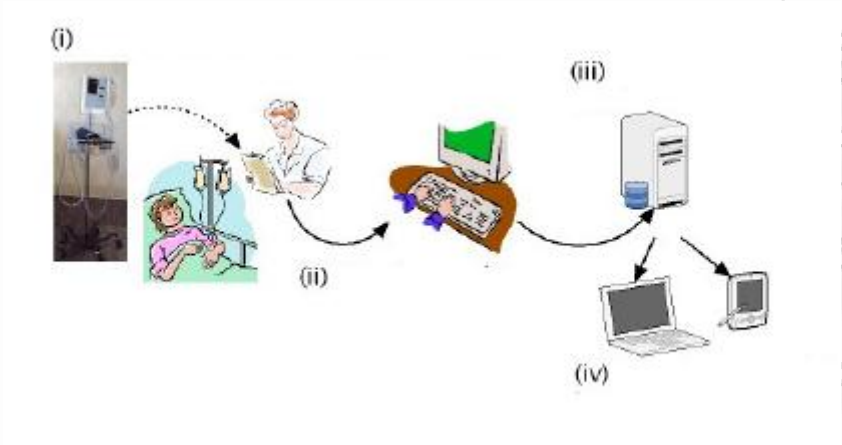
3.2 Συνδυασμός Τηλεϊατρικής και χρήσης υπολογιστικού σύννεφου στον τομέα της υγείας

Σήμερα η τηλεϊατρική επιτρέπει την απομακρυσμένη διάγνωση και παρακολούθηση των ασθενών και εγγυάται ασφάλεια και αξιοπιστία στην σύγχρονη υγειονομική περίθαλψη. Βέβαια υπάρχουν διάφορες προκλήσεις που συνδέονται με την αυτοματοποίηση αυτού του είδους του περιβάλλοντος όπως η ετερογένεια των συσκευών, τα πρωτόκολλα και ο προγραμματισμός των διασυνδέσεων, η απαίτηση για ευέλικτη και χωρίς επιπτώσεις εγκατάσταση, η απαίτηση για εύκολη ρύθμιση και διαχείριση των συστημάτων καθώς και η ύπαρξη αυτορυθμιζόμενων συστημάτων.

Η λύση στην παραπάνω πρόκληση στηρίζεται σε έννοιες αισθητήρων ασύρματων δικτύων και υπολογιστικής χρησιμότητας (utility computing). Αναλυτικότερα οι αισθητήρες είναι συνδεδεμένοι πάνω στον ιατρικό εξοπλισμό και στο δίκτυο υπολογιστών του οργανισμού και αλληλεπιδρούν μεταξύ τους για να ανταλλάσουν πληροφορίες. Οι πληροφορίες αυτές είναι διαθέσιμες στο υπολογιστικό νέφος , στο οποίο γίνεται η επεξεργασία από εξειδικευμένα συστήματα και τα οποία στην συνέχεια διανέμουν την πληροφορία στο ιατρικό προσωπικό για την πληρέστερη και πιο ακριβή ανάλυσή τους. Επίσης υποστηρίζεται ότι αυτές οι τεχνολογίες παρέχουν επιθυμητά χαρακτηριστικά για την αυτοματοποίηση του περιβάλλοντος της τηλεϊατρικής και την αντιμετώπιση των παραπάνω προκλήσεων. Η λύση των [Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker Westphall στο [9] συμβάλει: α)σε μια καινοτόμο και χαμηλού κόστους λύση για τη βελτίωση της ποιότητας της ιατρικής περίθαλψης και β) στην αντιμετώπιση των προκλήσεων της ενσωμάτωσης αισθητήρων σε ιατρικά μηχανήματα που χρησιμοποιούν τις υπηρεσίες του υπολογιστικού σύννεφου για συλλογή, επεξεργασία και διανομή των ζωτικής σημασία δεδομένων των ασθενών.

Το παρακάτω παράδειγμα αναπαριστά το κίνητρο για την ενσωμάτωση αισθητήρων και την χρήση των υπηρεσιών του υπολογιστικού νέφους στην υγειονομική περίθαλψη. Συγκεκριμένα διαδραματίζει το σενάριο χρήσης έγγραφων σημειώσεων που χρησιμοποιείται τώρα για την περίθαλψη του

ασθενή καθώς και τα προβλήματα που εμφανίζονται με την χρήση των σημειώσεων αυτών.



Εικόνα 3.2,1 Αναπαράσταση σεναρίου χειρόγραφης καταγραφής ιατρικών δεδομένων [5]

i. Το νοσηλευτικό προσωπικό συλλέγει τα δεδομένα του ασθενούς και τα καταγράφει σε ένα φύλλο ιατρικών σημειώσεων.

ii. Τα δεδομένα του ασθενή καταχωρούνται σε ένα τερματικό.

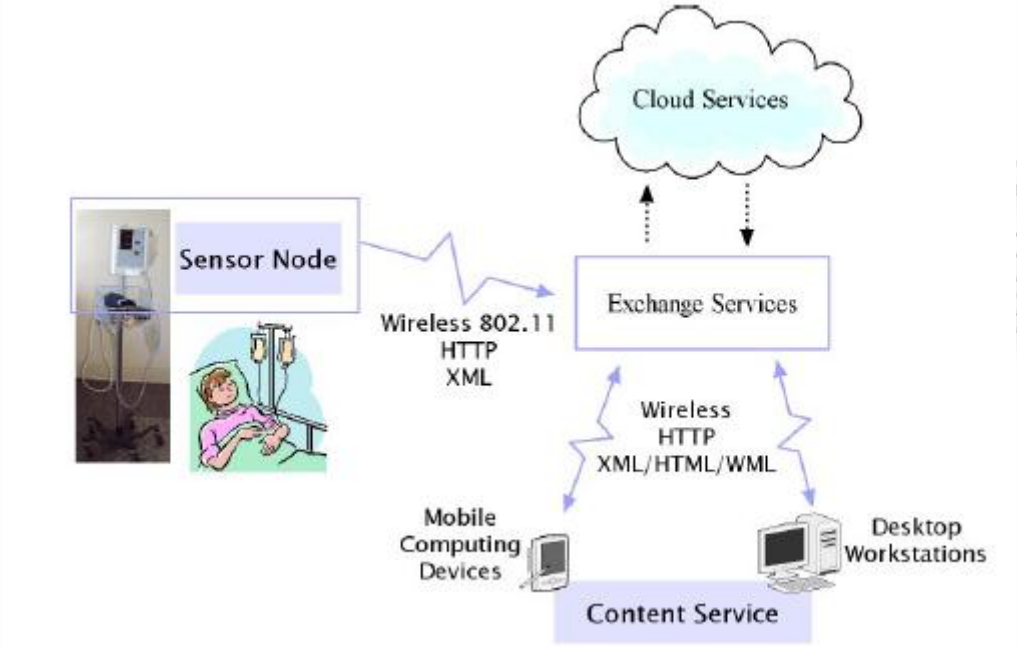
iii. Τα δεδομένα μεταδίδονται σε μια βάση δεδομένων ενός εξυπηρετητή ο οποίος τα οργανώνει, τα ταξινομεί και τα καταστεί προσβάσιμα μέσω μιας διεπαφής που χρησιμοποιεί η βάση δεδομένων.

iv. Το ιατροφαρμακευτικό προσωπικό μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα μέσω μιας ιατρικής εφαρμογής.

Είναι προφανές ότι από το παραπάνω σενάριο υπάρχει μία καθυστέρηση μεταξύ της συγκέντρωσης των δεδομένων και της πρόσβασης στις πληροφορίες. Αυτό είναι ανεπιθύμητο και αποτρέπει την παρακολούθηση σε πραγματικό χρόνο των ζωτικών δεδομένων των ασθενών και συγχρόνως περιορίζει τις δυνατότητες παρακολούθησης από το ιατρικό προσωπικό. Επιπλέον, η διαδικασία αυτή είναι επιρρεπής σε σφάλματα, δεδομένου ότι υπάρχει πιθανότητα εσφαλμένης εισόδου δεδομένων.

Από το παραπάνω σενάριο γεννιέται η ανάγκη αντικατάστασης της υπαρχούσης μεθόδου με την παροχή ολοκληρωμένων λύσεων τηλεϊατρικής που αυτοματοποιούν την διαδικασία συλλογής και επεξεργασίας των δεδομένων του ασθενή.

Η λύση στην παραπάνω ανάγκη είναι ένα σύστημα το οποίο αυτοματοποιεί την διαδικασία συλλογής των ζωτικής σημασίας δεδομένων των ασθενών μέσω ενός δικτύου αισθητήρων οι οποίοι είναι συνδεδεμένοι σε ιατρικές συσκευές και μεταδίδουν την πληροφορία στην υποδομή του νέφους το οποίο την αποθηκεύει, την επεξεργάζεται και την διανέμει.



Εικόνα 3.2.2 Αρχιτεκτονική του μοντέλου [6]

Η εικόνα 3.2.2 αναπαριστά την αρχιτεκτονική του μοντέλου τηλεϊατρικής με την χρήση νέφους. Όπως φαίνεται και παραπάνω, στην κλίνη του ασθενή υπάρχουν ασύρματοι αισθητήρες , στους οποίους έχει εγκατασταθεί λογισμικό υπεύθυνο για την συλλογή, κωδικοποίηση και μετάδοση των δεδομένων μέσω ενός ασύρματου καναλιού επικοινωνίας. Η υπηρεσία ανταλλαγής λειτουργεί ως μεσάζων μεταξύ των τοπικών και των απομακρυσμένων (remote) υπηρεσιών. Επίσης λαμβάνει αιτήσεις από τις τρέχουσες υπηρεσίες για ανάκτηση των δεδομένων από τις υπηρεσίες που παρέχονται στο υπολογιστικό νέφος. Οι υπηρεσίες νέφους είναι υπεύθυνες για την παροχή υπηρεσιών αποθήκευσης των συλλεγμένων δεδομένων ενώ παρέχουν μια πλατφόρμα για την σχεδίαση, τη δοκιμή και την ανάπτυξη ιατρικών εφαρμογών. Τέλος, οι σταθερές και κινητές συσκευές αλληλεπιδρούν με τις ιατρικές εφαρμογές έχοντας έτσι πρόσβαση σε όλες τις διαθέσιμες πληροφορίες του ασθενή.

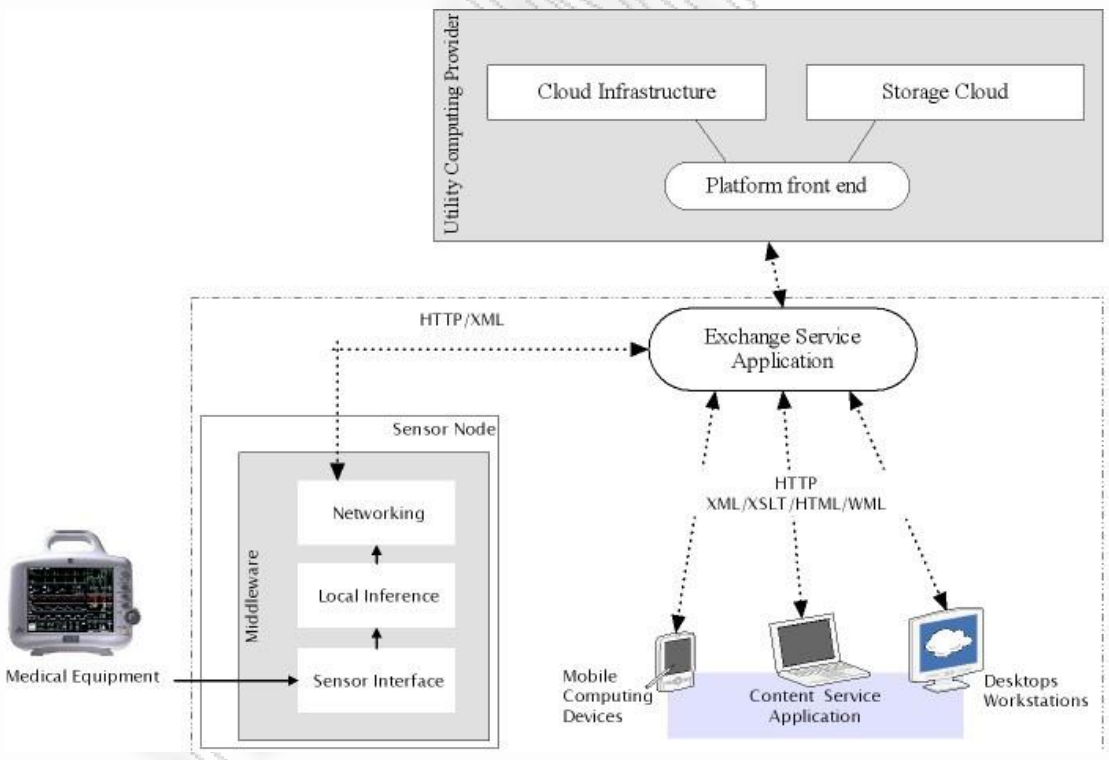
Τα πλεονεκτήματα της παραπάνω μεθόδου είναι ότι:

- ✓ Παρέχει σε πραγματικό χρόνο τα συλλεγμένα δεδομένα των ασθενών.
- ✓ Αντικαθιστά το έντυπο σημειωματάριο συλλογής δεδομένων και μηδενίζει την πιθανότητα λαθών.
- ✓ Διευκολύνει την διαδικασία ανάπτυξης της δικτύωσης (όλη η συνδεσμολογία είναι ασύρματη και δεν χρήζει ανάγκης καλωδίου ή φυσικής εγκατάστασης).

Τα βασικά στοιχεία που προκύπτουν από την αρχιτεκτονική είναι, (1) ότι οι αισθητήρες αντικαθιστούν την ανάγκη χειροκίνητης συλλογής δεδομένων και (στην συνέχεια) την εισαγωγή τους στο σύστημα υγείας. (2) Οι υπολογιστικοί πόροι που είναι διαθέσιμοι στο σύννεφο είναι υπεύθυνοι για την οργάνωση, εισαγωγή, διάθεση και διανομή των δεδομένων στο ιατροφαρμακευτικό προσωπικό. (3) Το υπολογιστικό νέφος παρέχει πρότυπες διεπαφές για την ολοκλήρωση των εφαρμογών του οργανισμού.

Παρακάτω αναλύεται και περιγράφεται λεπτομερώς η σχεδίαση και ανάπτυξη του μοντέλου τηλεϊατρικής με την χρήση νέφους.

Στο μοντέλο χρησιμοποιούνται ασύρματοι δρομολογητές που επιτρέπουν την αντικατάσταση του υπάρχοντος λειτουργικού συστήματος με λύση Linux. Επιπρόσθετα χρησιμοποιείται μια απλή εφαρμογή η οποία συλλέγει τα δεδομένα από μια σειριακή θύρα (συνδεδεμένη με την ιατρική συσκευή), τα μετασχηματίζει και τα φορτώνει στον Exchange εξυπηρετητή. Η λειτουργία που είναι υπεύθυνη για την αποθήκευση και την επεξεργασία των συλλεγμένων δεδομένων τρέχει σε εικονικά μηχανήματα με OPEN NEBULA λογισμικό. Τα στοιχεία και οι αλληλεπιδράσεις αναπαρίστανται στην εικόνα 3.2.3 και είναι τα εξής:



Εικόνα 3.2.3 Αναπαράσταση συσχετίσεων του μοντέλου [7]

Ο *αισθητήρας (Sensor Interface)* περιέχει τα στοιχεία για την εξαγωγή, μετατροπή και μεταφόρτωση των δεδομένων από το συνδεδεμένο ιατρικό εξοπλισμό. Στην συνέχεια το λογισμικό παρέχει ένα τυποποιημένο σύνολο

διεπαφών ελέγχου, εύκολα προγραμματιζόμενο για διαφορετικές ιατρικές συσκευές και τα δεδομένα μεταδίδονται μέσω του ασύρματου δικτύου στην υποδομή του υπολογιστικού νέφους.

Η *εφαρμογή υπηρεσιών του Exchange (Exchange Service Application)* περιλαμβάνει ένα μεγάλο αριθμό λειτουργικών υπηρεσιών που είναι υπεύθυνες για την οργάνωση των δεδομένων των ασθενών. Επιπρόσθετα, λειτουργεί ως διαμεσολαβητής μεταξύ των συνδεδεμένων συσκευών και των απομακρυσμένων υπηρεσιών. Έχει δύο βασικές λειτουργίες, λειτουργεί ως σημείο πρόσβασης και επιτρέπει στους αισθητήρες να αποθηκεύουν τα δεδομένα σε τοπικό επίπεδο για την προ-επεξεργασία τους (π.χ ανάλυση των δεδομένων πριν την μετάδοσή τους στο νέφος)

Τέλος ο *πάροχος υπολογιστικής χρησιμότητας (Utility Computing Provider)* παρέχει φυσική και λογική υποδομή για την αποθήκευση, επεξεργασία και υπηρεσία παράδοσης των δεδομένων.

Κεφάλαιο 4ο Πρότυπο μοντέλο ηλεκτρονικής υγείας βασισμένο στο υπολογιστικό σύννεφο

4.1 Εισαγωγή για την ηλεκτρονική υγεία

Ο όρος "ηλεκτρονική υγεία" (eHealth) καλύπτει ένα ευρύ φάσμα εργαλείων βασισμένων στις νέες πληροφοριακές υποδομές για την φαρμακευτική και ιατρική περίθαλψη που στοχεύουν στην καλύτερη πρόληψη, διάγνωση, θεραπεία, παρακολούθηση και διαχείριση της υγείας και του τρόπου ζωής.

Η ηλεκτρονική υγεία περιλαμβάνει τη συνεργασία μεταξύ ασθενών και φορέων ιατροφαρμακευτικής περίθαλψης, την ανταλλαγή δεδομένων μεταξύ διαφόρων ιδρυμάτων και την επικοινωνία μεταξύ ασθενών ή απασχολουμένων στον τομέα της υγείας. Επίσης περιλαμβάνει δίκτυα πληροφοριών για την υγεία, ηλεκτρονικά μητρώα υγείας, υπηρεσίες τηλεϊατρικής και φορητά επικοινωνούντα συστήματα για την παρακολούθηση και υποστήριξη των ασθενών. Τα εργαλεία ηλεκτρονικής υγείας παρέχουν πρόσβαση σε πληροφορίες για την υγεία που μπορούν να σώσουν ζωές, γεγονός ιδιαίτερα σημαντικό λόγω της ολοένα μεγαλύτερης διασυνοριακής κυκλοφορίας πολιτών και ασθενών. Αυτό που χρειάζεται είναι ένα σύνολο μεταρρυθμίσεων και ψηφιοποίησης του τομέα υγείας, συμπεριλαμβανομένης της παραγωγής, του εφοδιασμού και της διαχείρισής του. Τέτοιες τεχνικές καινοτομίες, αναμένεται να βελτιώσουν την ποιότητα των υπηρεσιών υγείας, μειώνοντας ταυτόχρονα τόσο το κεφάλαιο όσο και το λειτουργικό κόστος.

Βασική όμως πρόκληση στον τομέα της υγείας είναι η χρήση των συλλεγμένων δεδομένων των ασθενών με πολλούς τρόπους [τηλε-συμβουλευτική (teleconsultation), ηλεκτρονική συνταγογράφηση (ePrescribing), ηλεκτρονική παραπομπή (eReferral) ,ηλεκτρονική επιστροφή των ιατρικών εξόδων, διατηρώντας παράλληλα αυστηρούς μηχανισμούς πρόσβασης. Έχει παρατηρηθεί πολλές φορές ότι τα ιατροφαρμακευτικά δεδομένα υπόκεινται σε ένα σύνολο απειλών, κινδύνων και επιθέσεων, που η ασυνέπεια και η απώλεια των δεδομένων οδήγησαν σε σοβαρές συνέπειες. Γι’ αυτό το λόγο, μια πλατφόρμα e-health πρέπει να παρέχει μηχανισμούς για την ενίσχυση της ακεραιότητας, της ασφάλειας, της εμπιστευτικότητας και της δυνατότητας ελέγχου των ευαίσθητων ιατρικών δεδομένων σε όλο τον κύκλο ζωής τους.

4.2Μοντέλο συστήματος

Το μοντέλο του συστήματος αποτελείται από τις εξής έννοιες:

Τομέας: είναι μια επιχειρηματική περιοχή, η οποία διοικείται από τον διαχειριστή του συστήματος και προσφέρει είτε υπηρεσίες είτε αγαθά. Στο μοντέλο ηλεκτρονικής υγείας (e-health) οι επιχειρηματικές περιοχές είναι το νοσοκομείο, τα Περιφερειακά συστήματα υγείας (ΠεΣΥ) και οι ασφαλιστικές εταιρίες.

Χρήστης: είναι ένα άτομο ή μια υποδυόμενη υπηρεσία του μοντέλου ηλεκτρονικής υγείας (e-health). Ο χρήστης πρέπει να είναι μέλος ενός τουλάχιστον τομέα και πρέπει να είναι σε θέση να δηλώνει την ταυτότητά του για ένα συγκεκριμένο ρόλο.

Αντικείμενο: είναι μια οποιαδήποτε οντότητα που είναι διαχειριζόμενη από το σύστημα ηλεκτρονικής υγείας, όπως οι ασθενείς και οι ιατρικές συσκευές. Ένα αντικείμενο αναγνωρίζεται από ένα μοναδικό αναγνωριστικό (Unique ID) που αποδίδεται από τον διαχειριστή του τομέα. Πολλές φορές το μοναδικό χαρακτηριστικό αντικαθιστάται από ψευδώνυμο για λόγους ασφάλειας και μέτρο αντιστάθμισης στις επιθέσεις κατά της ιδιωτικότητας.

Ιδιότητα: είναι μια μονάδα πληροφοριών η οποία περιγράφει ένα αντικείμενο. Οι ιδιότητες είναι ατομικές μονάδες πληροφοριών από αρχικούς τύπους δεδομένων. Για παράδειγμα το αντικείμενο “ασθενής” αποτελείται από την ιδιότητα του “ονόματος” και από την ιδιότητα “καρδιο-αναπνευστικής πάθησης”. Τα πλεονεκτήματα που προκύπτουν από την εφαρμογή της ατομικής ιδιότητας είναι: 1)η δημιουργία σύνθετων ιατρικών εγγράφων (όπως τα ηλεκτρονικά μητρώα υγείας) και 2) η παροχή μεγάλης ευελιξίας στον διαμοιρασμό ατομικών ιδιοτήτων μεταξύ των τομέων.

Υπηρεσία: το πρότυπο μοντέλο υιοθετεί μια αρχιτεκτονική προσανατολισμένη στην υπηρεσία (Service Oriented Architecture-SOA) για την συλλογή και αποθήκευση των δεδομένων στο πλαίσιο των υπηρεσιών της ηλεκτρονικής υγείας. Τα πλεονεκτήματα αυτής της αρχιτεκτονικής είναι η αυτονομία, η δυνατότητα ελέγχου, η επαναχρησιμοποίηση και η εύκολη εφαρμογή και διαχείρισή της.

Υποδομή μοντέλου: όλη η υποδομή του πρότυπου μοντέλου θα βασίζεται στο υπολογιστικό νέφος. Συγκεκριμένα θα χρησιμοποιηθεί ένα υβριδικό υπολογιστικό νέφος για τα instances των υπηρεσιών και θα δουλεύει ως ιδιωτικό για την αποθήκευση των δεδομένων. Από τις τρεις υπηρεσίες που προσφέρονται στο υπολογιστικό σύννεφο, στο μοντέλο μας θα χρησιμοποιήσουμε την υποδομή ως υπηρεσία (PaaS), λόγω της μεγάλης

διαχειρισιμότητας που προσφέρει και γι αυτό το λόγο μπορεί να χρησιμοποιηθεί για την κάλυψη των απαιτήσεων των ιατρικών εφαρμογών.

4.3 Βασικές προϋποθέσεις ασφάλειας

Οι βασικές προϋποθέσεις ασφάλειας που πρέπει να πληρεί το πρότυπο μοντέλο ηλεκτρονικής υγείας είναι:

- Εμπιστευτικότητα δεδομένων: μηχανισμοί που διασφαλίζουν ότι μόνο εξουσιοδοτημένες οντότητες θα έχουν πρόσβαση στις υπηρεσίες και στα αποθηκευμένα δεδομένα.
- Ακεραιότητα δεδομένων: λειτουργίες που διασφαλίζουν την μη τροποποίηση ή αλλοίωση των ιατρικών δεδομένων.
- Διαθεσιμότητα δεδομένων: λειτουργίες που διασφαλίζουν ότι τα ιατρικά δεδομένα θα είναι πάντα διαθέσιμα όταν κάποια οντότητα τα αιτηθεί.
- Αυθεντικοποίηση: χρήση πρωτοκόλλων κρυπτογράφησης που επιτρέπουν σε μια οντότητα να αποδείξει την ταυτότητα της στο σύστημα ηλεκτρονικής υγείας.
- Εξουσιοδότηση: πολιτικές βασισμένες στους ρόλους (που βασίζονται στην πολιτική ασφαλείας του τομέα) προσδίδουν στις οντότητες δικαιώματα πρόσβασης σε πόρους.
- Ασφαλή αποθήκευση δεδομένων: αποθήκευση των ιατρικών ιδιοτήτων (ονοματεπώνυμο, ασθένεια) και των μετα-δεδομένων τους σε μια κρυπτογραφημένη βάση δεδομένων.
- Audit trail: μηχανισμοί που παρακολουθούν για μια συγκεκριμένη χρονολογική ακολουθία, τα εσωτερικά γεγονότα, τα εξωτερικά και τις επιπτώσεις τους.

4.4 Απειλές και επιθέσεις

Οι απειλές που πρέπει να ληφθούν υπόψη κατά την σχεδίαση και υλοποίηση του μοντέλου ηλεκτρονικής υγείας χωρίζονται σε δύο κατηγορίες: στις απειλές που απορρέουν από την χρήση υπολογιστικού νέφους και στις απειλές που έχουν σχέση με την ασφάλεια και την ιδιωτικότητα εκτός νέφους.

Οι απειλές που αφορούν το Υπολογιστικό νέφος είναι:

1. *Εξάντληση των πόρων*: επειδή το υπολογιστικό νέφος είναι on-demand υπηρεσία, η ανακριβής μοντελοποίηση και κατανομή των πόρων χρήσης μπορεί να οδηγήσει σε κίνδυνο της διαθεσιμότητας των υπηρεσιών και του ελέγχου πρόσβασης. Έτσι, ένας επιτιθέμενος μπορεί με επίθεση κατανεμημένης άρνησης εξυπηρέτησης (DDOS attack) να εκμεταλλευτεί την ανεπάρκεια των πόρων και να προκαλέσει ρήξη ασφαλείας στο ηλεκτρονικό σύστημα υγείας. Κατά συνέπεια χάνεται η εμπιστευτικότητα και η ακεραιότητα των ιατρικών δεδομένων.

2. *Αποτυχία δομής*: η πολυ-μίσθωση και οι κοινόχρηστοι πόροι (δηλαδή ο διαμοιρασμός της υπολογιστικής ισχύς και η αποθήκευση μεταξύ πολλών χρηστών) είναι δύο από τα χαρακτηριστικά του υπολογιστικού νέφους. Ο κίνδυνος που εμφανίζεται από την αποτυχία των μηχανισμών που χωρίζουν την αποθήκευση, τη μνήμη και τη δρομολόγηση μεταξύ των διαφόρων οργανισμών-πελατών της κοινής υποδομής μπορεί να οδηγήσει σε επιθέσεις SQL injection (σε βάσεις που μοιράζονται οι οργανισμοί πελάτες) και σε side channel επιθέσεις. Έτσι ο επιτιθέμενος μπορεί να προσποιηθεί τον πελάτη στον πάροχο του νέφους και να αποκτήσει πρόσβαση σε όλα τα ιατρικά δεδομένα ενός πελάτη-νοσοκομείου.
3. *Παρακολούθηση των δεδομένων κατά την μεταφορά*: Το υπολογιστικό νέφος είναι μια κατανεμημένη αρχιτεκτονική που επιτρέπει περισσότερα δεδομένα κατά τη μεταφορά σε σύγκριση με τις παραδοσιακές υποδομές. Για παράδειγμα, τα δεδομένα πρέπει να μεταφερθούν με τέτοιο τρόπο, ώστε να συγχρονιστούν πολλαπλές εικόνες μηχανών, οι εικόνες αυτές να διανεμηθούν σε πολλαπλές φυσικές μηχανές μεταξύ του νέφους και των απομακρυσμένων υπολογιστών-πελατών. Η μη ασφαλή μετάδοση των δεδομένων μπορεί να οδηγήσει σε επιθέσεις πλαστογράφησης δεδομένων (spoofing attack), σε επιθέσεις ενδιάμεσου στο κανάλι (man-in–the-middle attack), και σε επιθέσεις καταγραφής ανταλλαγής μηνυμάτων (replay attacks).
4. *Μη ασφαλής ή αναποτελεσματική διαγραφή δεδομένων*: Όταν γίνεται μια αίτηση για διαγραφή ενός πόρου στο σύννεφο, αυτό μπορεί να μην οδηγήσει σε πλήρη διαγραφή των δεδομένων διότι η πλήρης διαγραφή είναι δυνατή μόνο με την καταστροφή ενός δίσκου που αποθηκεύει και δεδομένα από άλλους οργανισμούς-πελάτες. Έτσι ένας κακόβουλος χρήστης (που μπορεί να είναι πελάτης του παρόχου υπολογιστικού νέφους) μπορεί να ελέγξει για δεδομένα που δεν έχουν διαγραφεί και να τα χρησιμοποιήσει είτε πουλώντας τα σε ασφαλιστικές εταιρίες είτε να αποκτήσει περαιτέρω πρόσβαση στα δεδομένα αυτά.
5. *Απώλεια των κλειδιών κρυπτογράφησης*: η κακή διαχείριση και διαφύλαξη των κλειδιών κρυπτογράφησης μπορεί να προκαλέσει αποκάλυψη των μυστικών κλειδιών ή των κωδικών πρόσβασης των οργανισμών-πελατών σε κακόβουλες οντότητες, οι οποίες με την σειρά τους να τα χρησιμοποιήσουν για μη εξουσιοδοτημένη χρήση ελέγχου ταυτότητας.
6. *Έκθεση σε κίνδυνο της μηχανής υπηρεσιών (service engine)*: Κάθε αρχιτεκτονική υπολογιστικού σύννεφου στηρίζεται σε μια μηχανή υπηρεσιών (service engine) που βρίσκεται πάνω από τους υλικούς πόρους των πελατών και τους διαχειρίζεται σε διαφορετικά επίπεδα αφαίρεσης. Για παράδειγμα, σε υπολογιστικά νέφη υποδομής ως υπηρεσία, η μηχανή υπηρεσιών μπορεί να είναι ο hypervisor. Ένας

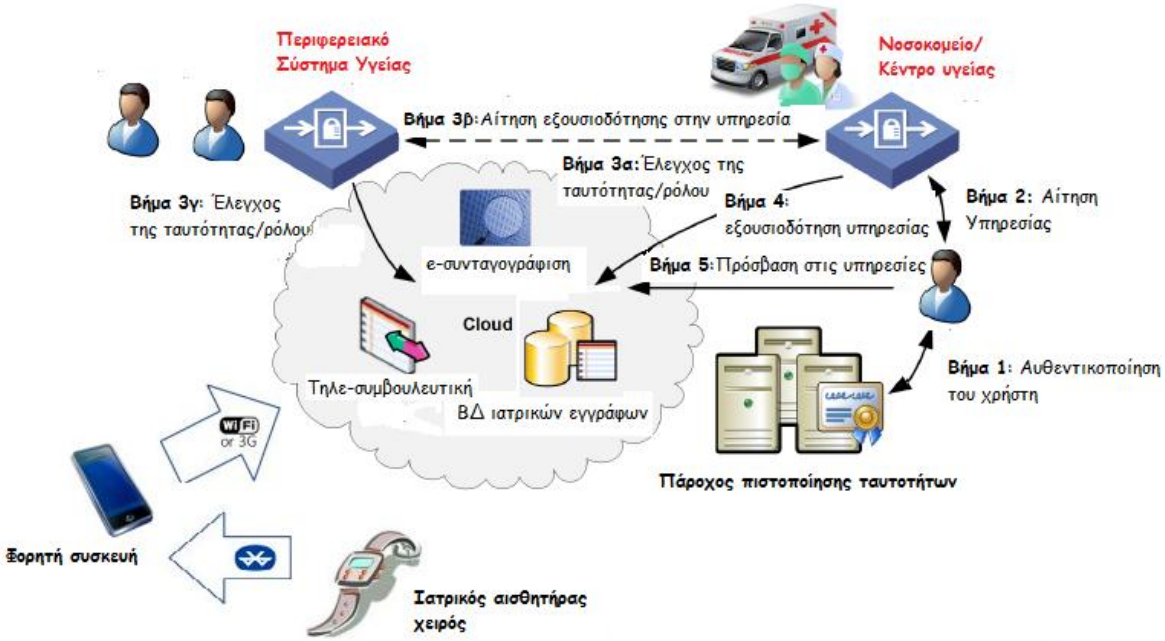
επιτιθέμενος μπορεί να θέσει σε κίνδυνο την μηχανή υπηρεσιών είτε μέσα από hacking των εικονικών μηχανών (σε νέφη υποδομής ως υπηρεσία), είτε επηρεάζοντας το runtime περιβάλλον (σε νέφη πλατφόρμας ως υπηρεσία), είτε τροποποιώντας το χώρο συγκέντρωσης των εφαρμογών (σε νέφη λογισμικού ως υπηρεσία). Ως αποτέλεσμα, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα δεδομένα των ασθενών, να τα παρακολουθήσει, να τροποποιήσει τις πληροφορίες τους με διαφανή τρόπο (χωρίς άμεση αλληλεπίδραση με την εφαρμογή μέσα στο περιβάλλον του νοσοκομείου) και να μειώσει τους εικονικούς πόρους του νοσοκομείου, με άμεση συνέπεια την άρνηση παροχής υπηρεσιών της ηλεκτρονικής υγείας.

Απειλές που έχουν σχέση με την ασφάλεια και την ιδιωτικότητα εκτός υπολογιστικού νέφους είναι:

1. *Έλλειψη εκπαίδευσης ιατρονοσηλευτικού προσωπικού στον τομέα της ασφάλειας*: η έλλειψη σωστής εκπαίδευσης και επαγρύπνησης του ιατρονοσηλευτικού προσωπικού πάνω σε θέματα ασφάλειας. Για παράδειγμα, 1) η δημιουργία και διαχείριση των πιστοποιητικών ταυτοποίησης (ασθενές όνομα χρήστη-κωδικού πρόσβασης, 2) η καταγραφή του πιστοποιητικού σε εμφανές σημεία όπως το πληκτρολόγιο του Η/Υ τους,3) η είσοδος σε μολυσμένες σελίδες ή σε σελίδες που οδηγούν σε παραπλανητικό ιστότοπο. Οι συνέπειες της ελλιπούς εκπαίδευσης μπορούν να αποβούν μοιραίες για το σύστημα ηλεκτρονικής υγείας και να βρεθεί σε κίνδυνο η εμπιστευτικότητα και η ακεραιότητα των ιατρικών δεδομένων.
2. *Έλλειψη ισχυρής αυθεντικοποίησης ασύρματου δικτύου*: η χρήση ασθενούς αυθεντικοποίησης στο ασύρματο κομμάτι δικτύου μπορεί να προκαλέσει ρήξη ασφάλειας, αφού κάποιος επιτιθέμενος μπορεί να εκμεταλλευτεί αυτήν την ευπάθεια, να εισβάλει στο δίκτυο και να εξαπολύσει επιθέσεις πλαστογράφησης δεδομένων (spoofing attack), επιθέσεις ενδιάμεσου στο κανάλι (man-in–the-middle attack), και επιθέσεις καταγραφής ανταλλαγής μηνυμάτων (replay attacks).

4.5 Σχεδιασμός μοντέλου ηλεκτρονικής υγείας

Ο σχεδιασμός του μοντέλου ηλεκτρονικής υγείας αναπαριστά σε πραγματικό χρόνο τα βήματα αυθεντικοποίησης ενός χρήστη που αιτείται κάποια υπηρεσία στο σύστημα υγείας. Αναλυτικότερα τα βήματα και οι ενέργειες είναι οι εξής:



Σχήμα 4.5.1 Αναπαράσταση αίτησης υπηρεσίας

Βήμα 1: Ο χρήστης συνδέεται σε έναν από τους παρόχους πιστοποίησης ταυτοτήτων λαμβάνοντας όνομα χρήστη και κωδικό πρόσβασης.

Βήμα 2: ο χρήστης χρησιμοποιώντας το πιστοποιητικό ταυτοποίησής του (όνομα χρήστη, κωδικό πρόσβασης) κάνει αίτηση για μία από τις υπηρεσίες της ηλεκτρονικής υγείας.

Βήμα 3: Το νοσοκομείο/κέντρο υγείας ελέγχει την ταυτότητα του χρήστη, την μετατρέπει σε ρόλο και ελέγχει το αίτημα της υπηρεσίας με τις εφαρμοσμένες πολιτικές ασφαλείας. Σε περίπτωση που η υπηρεσία παρέχεται από τοπικό τομέα, το νοσοκομείο είναι σε θέση να πιστοποιήσει εάν ο χρήστης έχει τη δυνατότητα να καταναλώσει αυτή την υπηρεσία και στη συνέχεια να τον συνδέσει στο νέφος που βρίσκεται η αιτούμενη υπηρεσία. Ωστόσο, εάν η υπηρεσία παρέχεται από ένα ξένο τομέα (βήμα 3γ), το νοσοκομείο θα δρομολογήσει την αίτηση υπηρεσίας στο Περιφερειακό σύστημα υγείας (ΠεΣΥ) χρησιμοποιώντας είτε ασφαλή σύνδεση μέσω VPN είτε πάνω από δίκτυο Peer to Peer. Για παράδειγμα, εάν πρέπει να ελεγχθεί η ασφάλιση ενός ασθενή ξένης εθνικότητας, τότε το νοσοκομείο θα δρομολογήσει την αίτηση στο ΠεΣΥ το οποίο με την σειρά του θα φροντίσει να επαληθεύσει μέσω της αντίστοιχης πρεσβείας (ξένος τομέας) την ασφάλιση του ασθενή.

Βήμα 4: εάν η αίτηση υπηρεσίας συμφωνεί με τις πολιτικές ασφάλειας, το νοσοκομείο δημιουργεί και υπογράφει ένα εισιτήριο υπηρεσιών (με χρήση SOAP). Αυτό το εισιτήριο περιέχει το ψευδώνυμο και το ρόλο του χρήστη, μια αναφορά στο τελικό σημείο της υπηρεσίας, την περίοδο ισχύος, και κλειδιά

συνεδρίας που επιτρέπουν στο λογισμικό του χρήστη και στο instance της υπηρεσίας τη δημιουργία μιας ασφαλούς συνεδρίας με χρήση πρωτοκόλλου SOAP (Simple Object Access Protocol). Σε περίπτωση όμως που η αίτηση απορριφθεί από το νοσοκομείο (λόγω μη συμφωνίας με την πολιτική ασφαλείας), τότε επιστρέφεται στο χρήστη ένα μήνυμα με το λόγο απόρριψης της αίτησής του.

Βήμα 5: Τέλος, το λογισμικό του χρήστη ξεκινά μια ασφαλή συνεδρία με χρήση των παρεχόμενων πληροφοριών από το εισιτήριο υπηρεσιών και αρχίζει να καταναλώνει την υπηρεσία. Σε περίπτωση όμως που έχουμε αναβάθμιση των ιδιοτήτων του χρήστη, τότε θα χρειαστεί να επαναληφθούν όλα τα βήματα από την αρχή.

4.6 Υλοποίηση μοντέλου ηλεκτρονικής υγείας

Ο κύριος στόχος του μοντέλου είναι να υποστηριχθεί η ανάπτυξη και η ενσωμάτωση των υπηρεσιών ηλεκτρονικής υγείας για την Α) συγκέντρωση, Β) αποθήκευση και Γ) διαμοιρασμό των ευαίσθητων ιατρικών δεδομένων.

Α. Συγκέντρωση ιατρικών δεδομένων

Η προσέγγιση του μοντέλου για την απλή, αποδοτική και ασφαλή λήψη των ιατρικών δεδομένων περιλαμβάνει τέσσερα βασικά στοιχεία:

- Το Αναγνωριστικό Ραδιοσυχνοτήτων (RFID),
- Τις φορητές συσκευές,
- Το υβριδικό υπολογιστικό νέφος
- Τις ασφαλείς υπηρεσίες πρωτόκολλου SOAP

Το Αναγνωριστικό Ραδιοσυχνοτήτων (RFID) είναι μια τεχνολογία που μπορεί να χρησιμοποιηθεί για την αναγνώριση, την αυθεντικοποίηση, την παρακολούθηση και τον εντοπισμό των ιατρικών αντικειμένων, καθώς και για την συλλογή πληροφοριών για τα ιατρικά αντικείμενα και το περιβάλλον τους. Υπάρχουν 2 τύποι RFID, χωριζόμενοι σε ενεργητικούς και παθητικούς ανάλογα με τον αναμεταδότη τους. Στο πρότυπο μοντέλο θα χρησιμοποιηθούν ενεργά RFID για τη συλλογή των ιατρικών δεδομένων των ασθενών σε πραγματικό χρόνο.

Οι φορητές συσκευές, όπως κινητά τηλέφωνα, PDAs και tablet PCs χρησιμοποιούνται ως αναγνώστες RFID , οι οποίες συλλέγουν τιμές από τους ενεργούς αναμεταδότες RFID, και στη συνέχεια τα διαβιβάζουν στις αντίστοιχες βάσεις δεδομένων στο υπολογιστικό νέφος. Οι φορητές συσκευές βασίζονται σε περιβάλλοντα ανοιχτού κώδικα και συγκεκριμένα σε ANDROID OS συστήματα τα οποία προσφέρουν εύκολο προγραμματισμό βασισμένο στις ανάγκες της ηλεκτρονικής υγείας , αναγνώστη Bar code, αναγνώστη RFID, Bluetooth ,WiFi λειτουργία και έλεγχο πρόσβασης με χρήση

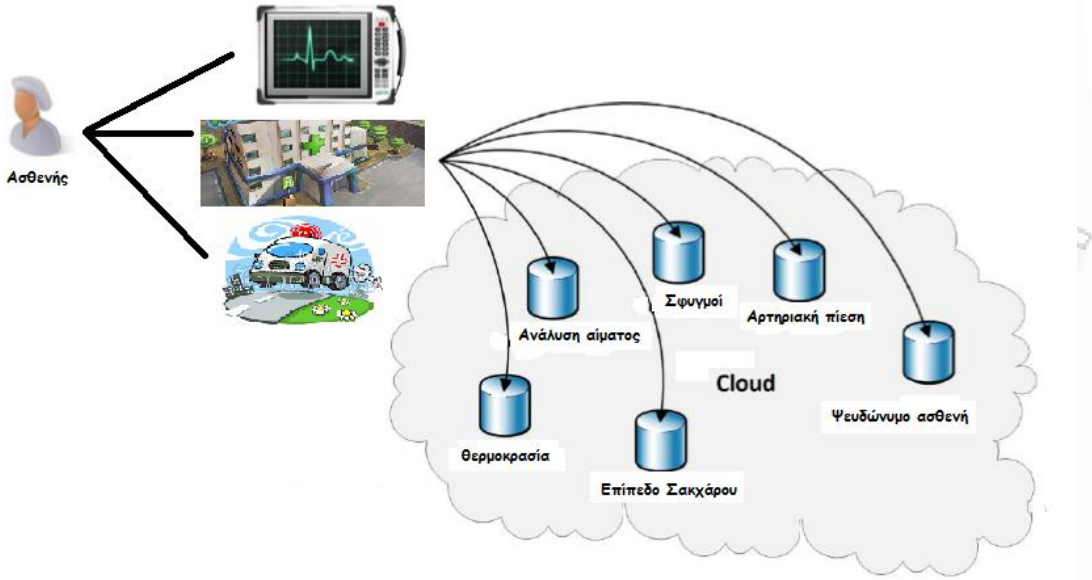
βιομετρικών στοιχείων (δαχτυλικά αποτυπώματα) που διασφαλίζουν ότι μόνο το εξουσιοδοτημένο ιατρικό προσωπικό μπορεί να χρησιμοποιήσει τις συσκευές αυτές.

Το υβριδικό υπολογιστικό νέφος χρησιμοποιείται ως σύνδεσμος με το δίκτυο (ενσύρματο, ασύρματο) του νοσοκομείου και ενσωματώνει τη ραχοκοκαλιά του εσωτερικού δικτύου του νοσοκομείου, τα ασύρματα σημεία πρόσβασης, τους δρομολογητές περιαγωγής και το δίκτυο κινητής τηλεφωνίας. Το ενσύρματο εσωτερικό δίκτυο συνδέει τους σταθμούς εργασίας (ιατρονοσηλευτικού προσωπικού) με τις πτέρυγες των ασθενών και στη συνέχεια τους πρώτους με τους διαδικτυακούς εξυπηρετητές και τους εξυπηρετητές αποθήκευσης δεδομένων (database servers). Τα ασύρματα σημεία πρόσβασης μπορούν να εξυπηρετήσουν όλες τις φορητές συσκευές (κατόπιν αυθεντικοποίησης του χρήστη) και οι δρομολογητές περιαγωγής μπορούν να χρησιμοποιηθούν όταν ένα ad-hoc δίκτυο είναι απαραίτητο να συνδεθεί στο δίκτυο του νοσοκομείου σε περίπτωση έκτακτης ανάγκης. Τέλος, το δίκτυο κινητής τηλεφωνίας (3G/4G) είναι ιδιαίτερα χρήσιμο για το ιατρικό προσωπικό σε κίνηση, αφού επιτρέπει την αποστολή δεδομένων των ασθενών από ένα ασθενοφόρο στο νοσοκομείο για την ταχεία διάγνωση του ασθενή.

Οι υπηρεσίες του πρωτόκολλου SOAP διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των ευαίσθητων ιατρικών δεδομένων κατά την μετάδοσή τους. Συγκεκριμένα όταν το νοσοκομείο χρησιμοποιεί την έκδοση εισιτηρίων για την αίτηση μια υπηρεσίας, πρέπει και οι χρήστες να χρησιμοποιήσουν το ίδιο πρωτόκολλο (SOAP) για την κρυπτογράφηση και αποκρυπτογράφηση των συναλλαγών τους.

Β. Αποθήκευση ιατρικών δεδομένων

Η πλατφόρμα του μοντέλου διατηρεί τις ιδιότητες σε μια ατομική μορφή για να ενισχύσει την επαναχρησιμοποίηση και την διαχειρισιμότητά τους. Ένα σημαντικό πλεονέκτημα είναι ότι ένα ατομικό χαρακτηριστικό μπορεί να αποθηκεύεται σε μία μόνο βάση δεδομένων, η οποία είναι κατάλληλη για την ανάπτυξη, την μετανάστευση, την αναδιάταξη και την δημιουργία σημείου επαναφοράς των ιδιοτήτων/ δεδομένων μέσα στο σύννεφο (όλες οι βάσεις δεδομένων είναι βασισμένες σε ένα και μόνο ξεχωριστό χαρακτηριστικό). Για παράδειγμα, όλα τα δεδομένα αρτηριακής πίεσης των ασθενών αποθηκεύονται και διατηρούνται στην ίδια βάση δεδομένων που είναι αποκλειστικά και μόνο για χαρακτηριστικά αρτηριακής πίεσης.
Η ασφάλεια που εφαρμόζεται είναι βασισμένη σε κρυπτογράφηση επιπέδου βάσης δεδομένων, διότι τα ευαίσθητα ιατρικά δεδομένα αποθηκεύονται σε ιδιωτικό νέφος και πλήρη πρόσβαση σε αυτά έχει μόνο ο διαχειριστής του συστήματος (νοσοκομείο/ΠεΣΥ).



Σχήμα 4.6.1 Αναπαράσταση αποθήκευσης ιδιοτήτων/δεδομένων ασθενή

Γ. Διαμοιρασμός ιατρικών δεδομένων

Ο πιο σημαντικός στόχος της πλατφόρμας του μοντέλου είναι να επιτρέπει σε αξιόπιστες οντότητες, σε ρόλους και σε υπηρεσίες εφαρμογών να έχουν πρόσβαση στα ευαίσθητα ιατρικά δεδομένα με πολλούς διαφορετικούς τρόπους, διατηρώντας παράλληλα αυστηρά δικαιώματα πρόσβασης. Για να επιτευχθεί ο στόχος απαραίτητο είναι να θεσπιστεί και να εφαρμοστεί μια πολιτική διαμοιρασμού πληροφοριών. Η πολιτική πρέπει να περιλαμβάνει τις έννοιες: 1) άδεια, 2) αιτών της υπηρεσίας, 3) λειτουργίες, 4) ιδιότητες των αντικειμένων, 5) πλαίσιο, 6) ιδιοκτήτης, 7) πολλαπλότητα εγγραφών, 8) χρονικό περιθώριο και 9) συμμόρφωση με τους κανόνες.

1) Άδεια: εμφανίζει την δράση των κανόνων και ορίζει εάν ένα αίτημα πληρεί τα κριτήρια των κανόνων ή όχι.
2) Αιτών: προσδιορίζει την πηγή της αίτησης από ένα συγκεκριμένο άτομο ή την συμμετοχή του σε κάποιο ρόλο.
3) Λειτουργία: αναφέρεται στο δικαίωμα δημιουργίας, ανάγνωσης, αναβάθμισης και διαγραφής.
4) Ιδιότητα: είναι μια μονάδα πληροφοριών που περιγράφει ένα αντικείμενο.
5) Πλαίσιο: προσδιορίζει το λόγο για τον οποίο οι πληροφορίες διαμοιράζονται. Επιπρόσθετα, διέπει το επίπεδο πρόσβασης και τα δικαιώματα που συνδέονται με την ανταλλαγή πληροφοριών, δημιουργώντας προτεραιότητα σύμφωνα με την αιτούμενη πληροφορία.
6) Ιδιοκτήτης: ορίζει ένα ρόλο με επαρκή δικαιώματα για την διαχείριση όλων των πτυχών μιας πληροφορίας, και επιτρέπει ή απαγορεύει την

πρόσβαση σε αυτή (όπως απαιτείται από τη νομοθεσία και καθορίζεται από τις αρμοδιότητές).

7) Πολλαπλότητα εγγραφών: ορίζει το μέγιστο αριθμό των εγγραφών που μπορούν να μοιραστούν κατά τη διάρκεια μιας χρονικής περιόδου.
8) Χρονικό περιθώριο: καθορίζει την διάρκεια ισχύος ενός κανόνα
9) Συμμόρφωση με τους κανόνες: αναφέρεται στις νομοθετικές απαιτήσεις που καθορίζουν την ανταλλαγή πληροφοριών(π.χ ανωνυμία ευαίσθητων δεδομένων).

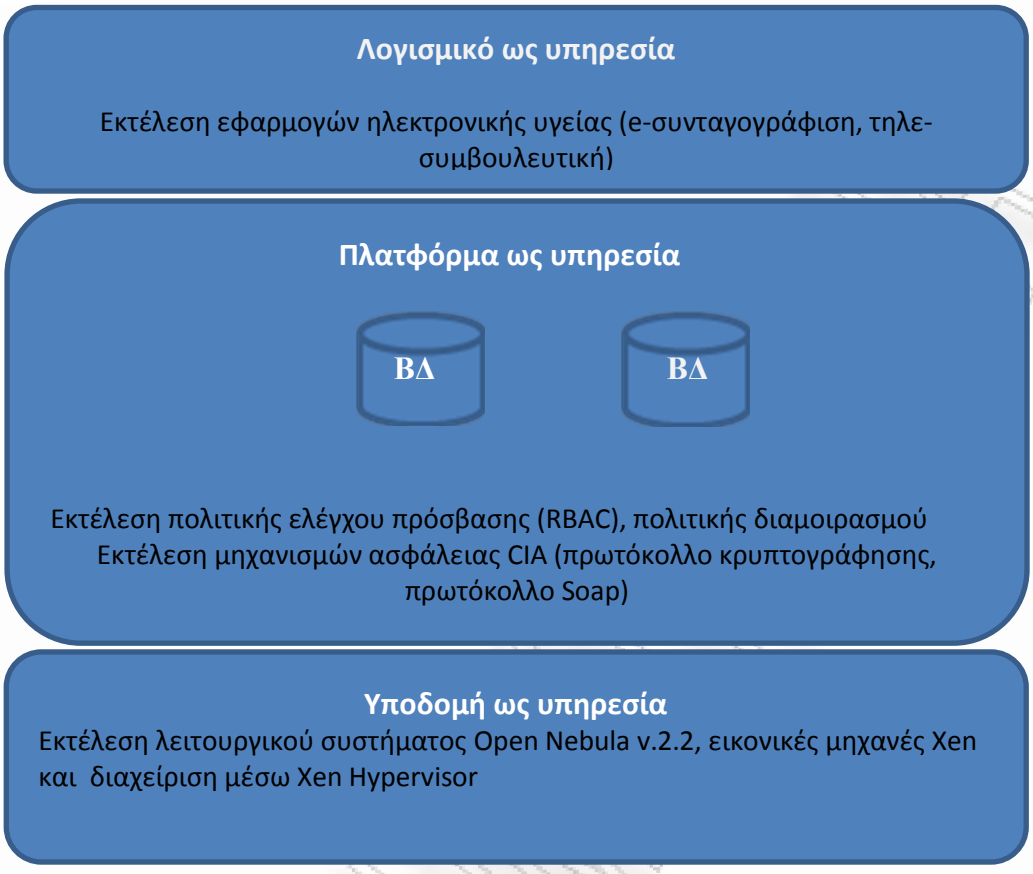
Οι κανόνες ασφάλειας που πρέπει να περιέχει η πολιτική διαμοιρασμού είναι:

- Υπηρεσία εξουσιοδότησης: Μια υπηρεσία εξουσιοδότησης επιτρέπει ή αρνείται σε άτομα ή ρόλους να έχουν πρόσβαση σε μια υπηρεσία εφαρμογής.
- Υπηρεσία εγγραφής: αντιπροσωπεύει την εγγραφή ενός ασθενούς σε μια συγκεκριμένη υπηρεσία της ηλεκτρονικής υγείας, ώστε αυτόματα να επιτρέπεται η δημιουργία και η ανάγνωση του ηλεκτρονικού του φακέλου (όπως απαιτείται από την υπηρεσία για να είναι λειτουργική).
- Ρητή συγκατάθεση: η πολιτική διαμοιρασμού πρέπει να επιτρέπει σε έναν ασθενή να παραχωρεί δικαιώματα πρόσβασης για τις δικές του ιδιότητες σε αξιόπιστες οντότητες και ρόλους.
- Συναίνεση: Μερικές φορές είναι δύσκολο για έναν ασθενή να ονομάσει μια οντότητα για μια συγκεκριμένη συναίνεση, γιατί είναι ασαφή, άγνωστο ή δύσκολο να περιγραφεί. Μια γενική συναίνεση είναι χρήσιμη σε αυτή την κατάσταση για να διευκολύνει την ανταλλαγή πληροφοριών μέσα στα πλαίσια της πολιτικής διαμοιρασμού.
- Έρευνα: χρησιμοποιείται μόνο σε εξαιρετικές καταστάσεις-περιπτώσεις, όπως για παράδειγμα μια ιατρική έρευνα σε ένα περιστατικό, ώστε να υποχρεώσει την άνευ όρων ανταλλαγή πληροφοριών.

Όταν ολοκληρωθεί η πολιτική διαμοιρασμού των ιατρικών δεδομένων , ο πάροχος πιστοποίησης ταυτοτήτων χρησιμοποιεί το πρωτόκολλο Κέρβερος (βασισμένο στην πολιτική διαμοιρασμού) για την αυθεντικοποίηση των χρηστών. Η χρήση του πρωτοκόλλου εμφανίζεται στα βήματα 1 έως 5 στην ενότητα 4.5.

4.7 Προδιαγραφές συστήματος ηλεκτρονικής υγείας

Το μοντέλο της ηλεκτρονικής υγείας θα υλοποιηθεί σε ιδιωτικό υπολογιστικό νέφος πλατφόρμας ως υπηρεσία. Στο σχήμα 4.7.1 φαίνεται ο διαχωρισμός των επιπέδων σε λογισμικό, πλατφόρμα και υποδομή ως υπηρεσία.



Σχήμα 4.7.1 Διαχωρισμός επιπέδων μοντέλου ηλεκτρονικής υγείας βασισμένο σε υπολογιστικό νέφος

Αναλυτικότερα το μοντέλο στηρίζεται στην υλοποίηση πλατφόρμας ως υπηρεσία με την χρήση Eucalyptus Enterprise Edition σε συνεργασία με την Amazon (EC2) για την προσφορά λογισμικού ως υπηρεσία.

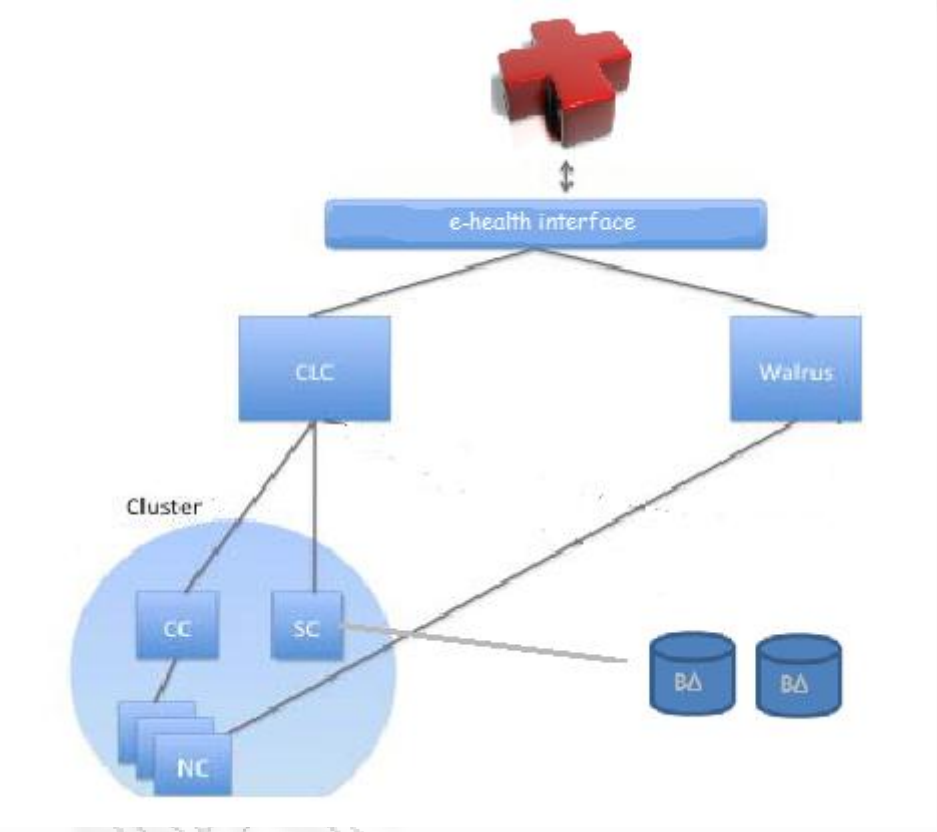
4.7.1 Υποδομή ως υπηρεσία

Το hardware που θα χρησιμοποιηθεί για την ανάπτυξη του μοντέλου νέφους είναι τέσσερις φυσικοί εξυπηρετητές. Ο ένας θα εκτελεί καθήκοντα Cloud Controller, ο δεύτερος Cluster controller ,ο τρίτος Storage controller και ο τέταρτος Node controller. Οι τεχνικές προδιαγραφές τους περιγράφονται στον πίνακα 3.

	Cloud controller	**Cluster controller**	**Storage controller**	**Node controller**
Επεξεργαστής	Intel Xeon E5620, 2,4GHz	Intel Xeon E5502, 1,86GHz	Intel Xeon E5502, 1,86GHz	Intel Xeon E3-1230, 3.20 GHz
Μνήμη	12 GB DDR3/1333	12 GB DDR3/1333	8 GB DDR3/1333	12 GB DDR3/1333
Αποθηκευτικός χώρος	2TB (2x1TB) SATA2/7200rpm	1TB SATA2/7200rpm	1TB SATA2/7200rpm	2TB (2x1TB) SATA2/7200rpm
Δικτύωση	Gigabit Lan	Gigabit Lan	Gigabit Lan	Gigabit Lan

Πίνακας 3 Τεχνικές προδιαγραφές εξυπηρετητών

Τα λειτουργικά σύστημα των τεσσάρων εξυπηρετητών είναι το Open Nebula v.2.2 για τον Cloud Controller και Ubuntu Enterprise Edition για τους Cluster controller, Storage controller και Node controller. Πάνω στον cluster controller και στο Node controller θα τρέχει ο Xen Hypervisor για την διαχείριση των εικονικών μηχανών. Οι εικονικές μηχανές που θα στηθούν είναι 4: μία για τον εξυπηρετητή πιστοποίησης ταυτοτήτων του νοσοκομείου, μία για την αποθήκευση των δεδομένων σε βάσεις (Data Base server) και δύο εικονικές μηχανές για την εξυπηρέτηση των ιατρικών εφαρμογών και υπηρεσιών. Στο σχήμα 4.1.4 αναπαρίστανται η διασυνδεσιμότητα των εξυπηρετητών [10].



Σχήμα 4.7.2 Σχηματική αναπαράσταση επιπέδου υποδομής

Ο *Cloud Controller (CLC)* είναι το σημείο εισόδου στο σύννεφο για τους διαχειριστές, τους προγραμματιστές εφαρμογών υγείας και τους τελικούς χρήστες. Είναι επίσης υπεύθυνος για την υποβολή ερωτημάτων στον διαχειριστή των κόμβων (node manager) που αφορούν τους πόρους και την υλοποίηση αυτών κάνοντας αιτήσεις στον Cluster Controller.Τέλος, αποτελεί την διασύνδεση με την πλατφόρμα διαχείρισης και αναλαμβάνει τον ρόλο της διαχείρισης των εικονικών πόρων (δίκτυο, αποθήκευση) μέσω διεπαφής εφαρμογών ή μέσω διεπαφής με φυλλομετρητή.

Ο *Cluster controller (CC)* τρέχει σε ένα μηχάνημα με Cluster ή σε οποιοδήποτε μηχάνημα που έχει δυνατότητα σύνδεσης δικτύου με τον Node

controller και τον Cloud Controller. Συγκεκριμένα, συλλέγει πληροφορίες από τα εγκατεστημένα εικονικά μηχανήματα και προγραμματίζει το χρονοδιάγραμμα εκτέλεσης των εικονικών μηχανών σε συγκεκριμένους κόμβους. Επίσης, διαχειρίζεται τα εικονικά Instances και συμμετέχει στην εκτέλεση των SLAs (Service Level Agreements) με τις οδηγίες που έχει δώσει ο Cloud Controller. Απαραίτητη προϋπόθεση των παραπάνω είναι ότι όλοι οι κόμβοι που συνδέονται με τον Cluster controller πρέπει να βρίσκονται στο ίδιο Ethernet δίκτυο.

Ο *storage controller (SC)* είναι υπεύθυνος για την διασύνδεση των συστημάτων αποθήκευσης.

Ο *Node controller (NC)* εκτελείται σε κάθε μηχάνημα που φιλοξενεί εικονικά instances. Κύριος σκοπός του, είναι να ελέγχει τα εικονικά μηχανήματα όπως την εκτέλεση, την επιθεώρηση και τον τερματισμό τους. Επίσης ελέγχει και διενεργεί αιτήματα στο λογισμικό του συστήματος (δηλαδή στα Ubuntu Enterprise Edition και στον Xen Hypervisor) σύμφωνα με τα ερωτήματα και τα αιτήματα ελέγχου του Cluster controller.

Ο *Walrus* επιτρέπει στους χρήστες να αποθηκεύουν τα δεδομένα οργανωμένα το καθένα σε ξεχωριστή βάση δεδομένων (κατόπιν αυθεντικοποίησης από τον έλεγχο πρόσβασης του νοσοκομείου).

Το e-health interface εξασφαλίζει την πρόσβαση σε υπηρεσίες ηλεκτρονικής υγείας είτε απομακρυσμένα μέσω χρήσης φιλομετρητή (Web Interface), είτε μέσω διεπαφής εφαρμογής (API) σε συγκεκριμένη υπηρεσία.

4.7.2 Πλατφόρμα ως υπηρεσία

Στο επίπεδο πλατφόρμα ως υπηρεσία, εφαρμόζονται η πολιτική ελέγχου πρόσβασης, η πολιτική διαμοιρασμού στην οποία αναφερθήκαμε στην προηγούμενη ενότητα και οι μηχανισμοί ασφαλείας με κρυπτογράφηση επιπέδου ΒΔ.
Η <u>πολιτική ελέγχου πρόσβασης</u> εφαρμόζεται στο μοντέλο μας με την χρήση RBAC (Role based Access Control). Το RBAC τάσσεται υπέρ της προσέγγισης στην διάκριση των διαφόρων τύπων χρηστών και των προνομίων τους, που βασίζεται σε μια συλλογή πόρων. Πιο συγκεκριμένα, ομαδοποιεί τους χρήστες σε ρόλους, και κάθε ομάδα συνδέεται με έναν αριθμό προνομίων. Κάθε λειτουργία από αυτές που ορίζονται στο σύστημα (ανάγνωση, γραφή, δημιουργία, διαγραφή,) μπορεί να συνδέεται με ένα προνόμιο που έχει ανατεθεί σε ένα ρόλο. Στους χρήστες έχουν ανατεθεί ρόλοι με βάση τις ευθύνες και τα προσόντα τους. Κάθε χρήστης μπορεί να είναι εκ νέου από ένα ρόλο και να ανατίθενται σε άλλο. Οι ρόλοι είναι δυναμικοί, έτσι ώστε σε ένα ρόλο που του έχουν αποδοθεί κάποια δικαιώματα, να μπορούν

να αλλάξουνε άμεσα. Επίσης νέα δικαιώματα μπορούν να προστίθενται στο ρόλο και τα υπάρχοντα δικαιώματα μπορούν να διαγράφονται από αυτό.

Ο πυρήνας του μοντέλου RBAC περιλαμβάνει πέντε βασικά στοιχεία:

- χρήστες
- ρόλους
- αντικείμενα
- διαδικασίες
- δικαιώματα

Η προσέγγιση με το σχήμα RBAC εφαρμόζεται ευρέως στον τομέα της υγειονομικής περίθαλψης επειδή οι κλασσικοί ρόλοι υγείας (ιατρός, νοσηλεύτρια) είναι απλοί.
Αργότερα, οι ερευνητές συνειδητοποίησαν ότι οι ρόλοι έχουν μια δυναμική πτυχή εκτός από την αρχική διαρθρωτική πτυχή που τους αποδόθηκε. Κατά συνέπεια, οι υφιστάμενες έννοιες δικαιωμάτων έπρεπε να επεκταθούν προκειμένου να υποστηριχθούν επιπρόσθετες απαιτήσεις δικαιωμάτων στην υγειονομική περίθαλψη. Για παράδειγμα, ένας γιατρός επιτρέπεται να διαθέτει πρόσβαση σε πληροφορίες σχετικά με την υγεία ενός κοινού ασθενή μόνο σε περίπτωση που ασχολείται με την επεξεργασία του εν λόγω ασθενούς. Επίσης παρατηρήθηκε ότι οι ρόλοι έχουν περισσότερες και πιο σύνθετες μεταβλητές (όπως ο χρόνος, ο τόπος, το μέσο και το σύστημα που τους πιστοποίησε), οι οποίες επηρεάζουν τη συμπεριφορά τους.
Οι Motta και Furuie [11] πρότειναν ένα σύνθετο ρόλο πρόσβασης βάσει του μοντέλου ελέγχου έγκρισης, με στόχο την αύξηση της προστασίας της ιδιωτικότητας και του απορρήτου των δεδομένων των ασθενών, ενώ είναι αρκετά ευέλικτο ώστε να επιτρέπει και την εξέταση ειδικών περιπτώσεων. Πρότειναν ακόμα, τον καθορισμό ενός ιεραρχικού ρόλου με την κληρονομιά αδειών και δικαιωμάτων, ενώ μοντελοποίησαν τους τύπους των δεδομένων που βρέθηκαν σε ένα Ηλεκτρονικό Ιατρικό Φάκελο (EHR) σύμφωνα με τα κλινικά περιεχόμενα (δημογραφία, συνταγές).

Οι άδειες εξουσιοδοτήσεις ορίζονται ως εξής:

- R: ο ρόλος
- PT: ο τύπος του δικαιώματος ο οποίος μπορεί να είναι θετικός όταν μια διαδικασία-ενέργεια επιτρέπεται στο σύστημα και αρνητική όταν δεν επιτρέπεται
- Opr: η διαδικασία (ή ο τρόπος πρόσβασης)
- Obj: το αντικείμενο (ή η πηγή πληροφοριών) που πρέπει να προστατευθεί
- At: ο τύπος εξουσιοδότησης ο οποίος μπορεί να είναι ισχυρός ή αδύναμος

Ένα παράδειγμα κρυπτογράφησης ιατρικού φακέλου με την χρήση RBAC εμφανίζεται στην προσέγγιση των Molva kai Bagga [12]. Συγκεκριμένα, αναπαρίσταται ένας ιατρικός φάκελος ενός ασθενή που κρυπτογραφείται με πολιτικές που καθορίζουν ποιοι μπορούνε να διαβάσουνε το συγκεκριμένο αρχείο.

```
pol = <Doctor, role> OR <Nurse, role>,…
act = read only
doc = document
```

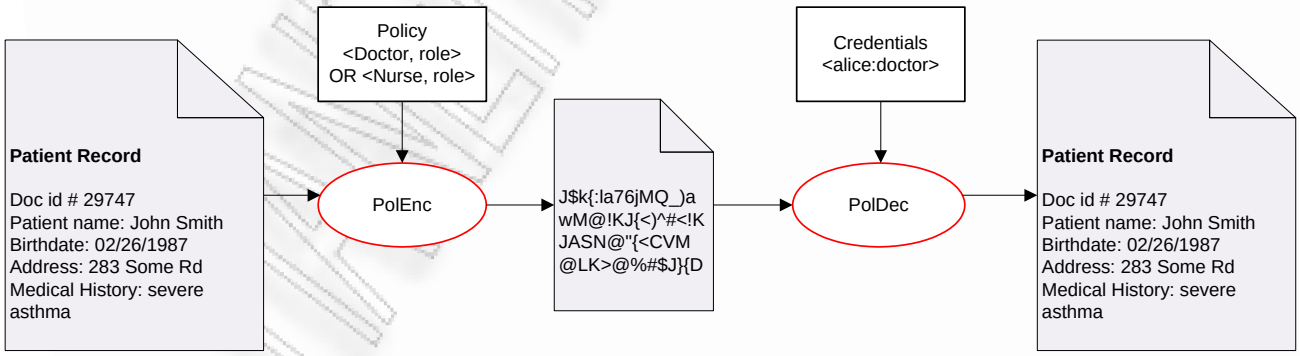
Ο φάκελος κρυπτογραφείται με την πολιτική που εφαρμόστηκε:

```
temp = PolEnc(doc, pol)
```

και φαίνεται ότι στην περίπτωση που κάποιος θελήσει να έχει πρόσβαση στον φάκελο, η πρόσβαση θα του επιτραπεί μόνο εάν έχει τα δικαιώματα (credentials) που ικανοποιούνε την πολιτική.

```
cred = (alice:doctor)
doc = PolDec(temp, pol, cred)
```

Στην συγκεκριμένη περίπτωση η Alice που είναι η προσωπικός γιατρός του John Smith βλέπουμε ότι είναι γιατρός και μάλιστα η προσωπική του γιατρός. Αυτό της δίνει το δικαίωμα πρόσβασης και ανάγνωσης σε όλα τα στοιχεία που αφορούν το φάκελο του ασθενή. Εάν για παράδειγμα μια στατιστική υπηρεσία εκπονούσε έρευνα για το πόσοι ασθενείς πάσχουν από δισκοπάθεια, από τα αντίστοιχα δικαιώματα που θα είχε, θα της επιτρεπόταν πρόσβαση μόνο σε αριθμητικά δεδομένα ασθενών που πάσχουν από δισκοπάθεια χωρίς όμως να της επιτραπεί από το σύστημα να συλλέξει οποιοδήποτε άλλο δεδομένο όπως όνομα, ηλικία και άλλα χαρακτηριστικά του ιατρικού φακέλου.



4.7.3 Σχηματική αναπαράσταση κρυπτογράφησης ιατρικού φακέλου [8]

Τι γίνεται όμως στην περίπτωση που κάποιος ασθενής πχ εισαχθεί σε ένα νοσοκομείο στο τμήμα επειγόντων περιστατικών; Με κάποιο τρόπο θα πρέπει το τμήμα επειγόντων περιστατικών να προσπελάσει τον ιατρικό του φάκελο

και να επέμβει σύμφωνα με τις πληροφορίες που βρίσκονται σ' αυτόν (πχ αν παρουσιάζει ανωμαλίες στην χορήγηση κάποιου φαρμάκου) και στην νοσηλεία του. Εδώ υπεισέρχεται το μοντέλο Break the glass.

Η προσέγγιση ''Break the glass'' [13] βασίζεται στην γρήγορη διαχείριση και διανομή των λογαριασμών ενός ασθενή σε μια κατάσταση εκτάκτου ανάγκης (π.χ ο ασθενής είναι σε κόμμα, οπότε δεν μπορεί να δώσει username/ password για να πιστοποιηθεί στο σύστημα. Σε τέτοιο σενάριο επεμβαίνει η λύση του ''Break the glass'' δίνοντας στο διαχειριστή του συστήματος πρόσβαση ώστε να ελέγξει το ιστορικό και γενικότερα τον φάκελο του ασθενή.

Σκοπός αυτής της προσέγγισης, είναι να επιτρέπει στους διαχειριστές ''επείγουσας ανάγκης'', να έχουν πρόσβαση στο σύστημα σε περιπτώσεις όπου η κανονική πιστοποίηση της ταυτότητας του ασθενή δεν μπορεί να ολοκληρωθεί με επιτυχία.
Η λύση της έκτακτης πρόσβασης θα πρέπει να χρησιμοποιείται μόνο όταν κανονικές διαδικασίες ταυτοποίησης είναι ανεπαρκείς. Περιπτώσεις όπου η πρόσβαση έκτακτης ανάγκης είναι απαραίτητη είναι οι ακόλουθες:

1. Προβλήματα πρόσβασης στον λογαριασμό του χρήστη:
    - κάποιος χρήστης ξέχασε το username/password μετά από ένα παρατεταμένο διάστημα αποχής από το νοσοκομείο.
    - Κλείδωμα λογαριασμού μετά από επανειλημμένες προσπάθειες ενός χρήστη για log-in στο σύστημα.

2. Προβλήματα στην αυθεντικοποίηση του χρήστη λόγω σοβαρής ασθένειας
    - Όταν ένας ασθενής πάσχει από νόσο Alzheimer ή βρίσκεται σε κώμα

Λογαριασμοί για περιπτώσεις εκτάκτου ανάγκης πρέπει να δημιουργούνται εκ των προτέρων έτσι ώστε να επιτρέπουν τον έλεγχο πρόσβασης στον φάκελο ενός ασθενή σε περίπτωση ανάγκης. Επίσης κατά την δημιουργία και εφαρμογή τέτοιων λογαριασμών πρέπει να λαμβάνεται πάντα υπόψη η πολιτική ασφαλείας που ορίζει το κάθε νοσοκομείο. Μερικοί παράγοντες που καθορίζουν λογαριασμούς επείγουσας ανάγκης είναι οι ακόλουθοι:

- Το όνομα χρήστη σε ένα λογαριασμό επείγουσας ανάγκης πρέπει να είναι προφανές (π.χ emergency001 ο λογαριασμός αυτός θα χρησιμοποιείται για πιστοποίηση του ασθενή μόνο σε καταστάσεις έκτακτης ανάγκης).
- Τέτοιοι λογαριασμοί πρέπει να επιτρέπουν την πρόσβαση μόνο σε απαραίτητα στοιχεία για την διάγνωση του ασθενή και να καθορίζονται

από τα αποτελέσματα της αποτίμησης κινδύνου (π.χ πρόσβαση η οποία θα υποστηρίζει μόνο την ανάγνωση (read-only) των απαιτούμενων δεδομένων που είναι απαραίτητα για την εκτέλεση της θεραπείας καθώς θα εμποδίζει και την πρόσβαση σε δεδομένα που έχουν αποκτηθεί στο παρελθόν).

Τα δεδομένα ενός λογαριασμού για επείγοντα περιστατικά πρέπει να είναι διαθέσιμα με κατάλληλο και εύλογο τρόπο. Αυτά τα δεδομένα μπορεί να παρέχονται ως τυπωμένη σελίδα ή εισιτήριο υπηρεσιών.

Σε αυτό το σημείο πρέπει να συσταθεί μια διαδικασία για τον καθαρισμό των λογαριασμών έκτακτης ανάγκης που έχουν χρησιμοποιηθεί. Τέτοιες διαδικασίες είναι οι εξής:

- Απενεργοποίηση ή διαγραφή του λογαριασμού έκτακτης ανάγκης αφού ο κωδικός έχει ήδη χρησιμοποιηθεί για μια τέτοια περίπτωση. Η πολιτική ασφαλείας πρέπει να ορίζει την αυτόματη απενεργοποίηση του λογαριασμού έκτακτης ανάγκης μετά την πρώτη χρήση ή διέλευση μιας χρονικής περιόδου που αντιστοιχεί από 8 ώρες έως μία ημέρα.
- Επανεξέταση των δραστηριοτήτων που εκτελούνται, συμπεριλαμβανομένων των στοιχείων που αποκτήθηκαν κατά την πρόσβαση του φακέλου σύμφωνα με την πολιτική του νοσοκομείου.
- Δημιουργία και διανομή νέων λογαριασμών για μελλοντική χρήση του ‘’Break-the-glass’’. Εκχώρηση νέων κωδικών πρόσβασης σε έναν λογαριασμό έκτακτης ανάγκης, βάσει της πολιτικής ασφαλείας.

Οι μηχανισμοί ασφαλείας που εφαρμόζονται στην βάση δεδομένων είναι η χρήση κρυπτογράφησης με αλγόριθμο RSA (2048bit) και τα κλειδιά κρυπτογράφησης είναι βασισμένα σε ένα γεννήτορα ψευδοτυχαίων αριθμών.

4.7.3 Λογισμικό ως υπηρεσία

Στο επίπεδο λογισμικού ως υπηρεσία τρέχουν οι εφαρμογές της e-συνταγογράφισης και της τηλε-συμβουλευτικής.

Η *e-συνταγογράφηση* είναι μια ιατροφαρμακευτική εφαρμογή της Γενικής Γραμματείας Κοινωνικών Ασφαλίσεων (ΓΓΚΑ), η οποία εξυπηρετεί την παραγωγή, την διακίνηση και τον έλεγχο των ιατρικών συνταγών και των παραπεμπτικών με τη χρήση τεχνολογίας ΤΠΕ, διασφαλίζοντας παράλληλα την ασφάλεια και την ιδιωτικότητα των ευαίσθητων ιατρικών δεδομένων των ασθενών.

Στο πλήρες εύρος της, υποστηρίζει το σύνολο των διαδικασιών δημιουργίας, εκτέλεσης, διαχείρισης, ελέγχου, εκκαθάρισης και πληρωμής συνταγών

φαρμάκων και ιατρικών πράξεων σε όλα τα σημεία ενδιαφέροντος (ιατρείο, κέντρο υγείας, κλινική, νοσοκομείο, φαρμακείο, διαγνωστικό εργαστήριο) και παρέχει σημαντικές δυνατότητες παρακολούθησης, έρευνας και ανάλυσης για όλους τους ενδιαφερόμενους.

Για να πραγματοποιηθεί είσοδος στο σύστημα, ο ιατρός/φαρμακοποιός πρέπει να πραγματοποιήσει αρχικά συναλλαγή με το σύστημα πιστοποίησης ταυτοτήτων και να παραλάβει μοναδικό όνομα χρήστη και κωδικό πρόσβασης. Η εμφάνιση των στοιχείων του ασθενή θα διαφέρει από οντότητα σε οντότητα, δηλαδή ο ιατρός ενός νοσοκομείου που παρακολουθεί τον ασθενή θα έχει πρόσβαση σε περισσότερα δεδομένα από έναν φαρμακοποιό. Σημαντικό είναι να τονιστεί ότι μόνο με τη συγκατάθεση του ασθενή οι οντότητες έχουν πρόσβαση στις πληροφορίες τους (σύμφωνα με πολιτική διαμοιρασμού ιατρικών δεδομένων).

Η *τηλε-συμβουλευτική* (τηλε-διάσκεψη) είναι μια ιατρική εφαρμογή του Εθνικού Συστήματος Υγείας (ΕΣΥ) η οποία επιτρέπει την διασύνδεση των μονάδων υγείας και εξυπηρετεί την ανταλλαγή ιατρικών διαγνώσεων σε πραγματικό χρόνο. Οι βασικές λειτουργίες που υποστηρίζει είναι:

- Ανταλλαγή και μετάδοση ακτινογραφιών, καρδιογραφημάτων σε πραγματικό και ετεροχρονισμένο χρόνο. Συγκεκριμένα, το σύστημα επιτρέπει την μετάδοση ακτινογραφιών και καρδιογραφημάτων σε ψηφιακή μορφή μέσω χρήσης ΤΠΕ από τον “μη εξειδικευμένο” ιατρό σε κάποιο “εξειδικευμένο ιατρό” ο οποίος θα μπορεί να πραγματοποιεί τη διάγνωση της εξέτασης την οποία μπορεί να επιστρέψει στην συνέχεια στο “μη ειδικευμένο ιατρό” μαζί με τις οδηγίες. Η ψηφιοποίηση των ιατρικών δεδομένων (σε περίπτωση που τα ιατρικά δεδομένα συλλέγονται σε αναλογική μορφή από τις κατάλληλες ιατρικές συσκευές) επιτυγχάνεται με χρήση ειδικών συσκευών όπως οι ψηφιοποιητές ακτινογραφιών (x-ray scanners, camera/frame grabber), ψηφιακοί καρδιογράφοι.
- Ανταλλαγή γραπτών μηνυμάτων μεταξύ των εμπλεκόμενων ιατρών. Με αυτό τον τρόπο κάθε χρήστης θα μπορεί να στέλνει μηνύματα σε οποιονδήποτε χρήστη του προτεινόμενου δικτύου.
- Πρόσβαση σε πηγές πληροφοριών και βάσεις δεδομένων ανάλογα με τον ρόλο και την ταυτότητα του χρήστη

Η πρόσβαση στο σύστημα θα επιτυγχάνεται με χρήση όνομα χρήστη και κωδικού πρόσβασης και η ανταλλαγή των δεδομένων θα γίνεται μετά από εξουσιοδότηση του ασθενή σε κάθε οντότητα που εξετάζει τα δεδομένα.

4.8 Έλεγχος ασφάλειας της πλατφόρμας ηλεκτρονικής υγείας με την χρήση του προτύπου NIST-FISMA για υπολογιστικά νέφη

Μετά την σχεδίαση, υλοποίηση και ανάλυση των προδιαγραφών του συστήματος ηλεκτρονικής υγείας πρέπει να γίνει η αξιολόγηση του μοντέλου με κάποιο πρότυπο ασφαλείας. Στο πρότυπο μοντέλο θα εφαρμοστεί το NIST-FISMA για υπολογιστικά σύννεφα. Όπως αναπαρίσταται και στον πίνακα 4 η αξιολόγηση γίνεται σε 6 φάσεις και οι εμπλεκόμενες οντότητες είναι το νοσοκομείο (ο οργανισμός-πελάτης), το Υπουργείο Απασχόλησης και Κοινωνικής Προστασίας (πάροχος υπηρεσιών και προγραμμάτων υγείας) και η Amazon (πάροχος υπολογιστικού σύννεφου).

Στην 1^{η} φάση (κατηγοριοποίηση των υπηρεσιών ασφαλείας), το νοσοκομείο έχει συμφωνήσει (με την AMAZON) το SC (Νοσοκομείου)= χαμηλή και το SC (e-health)= χαμηλή. Δηλαδή οι επιπτώσεις απ' την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών βάση των στόχων του νοσοκομείου να είναι χαμηλές. Επιπλέον, όσον αφορά τις παραβιάσεις ασφάλειας των πληροφοριών της ηλεκτρονικής υγείας είναι συμφωνημένο να είναι χαμηλό το επίπεδο επιπτώσεων, δηλαδή μία παραβίαση να έχει χαμηλή επίπτωση στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των υπηρεσιών ηλεκτρονικής υγείας. Βέβαια η διασφάλιση των SC (Νοσοκομείου) και SC (e-health) σε χαμηλό επίπεδο σημαίνει μεγαλύτερο κόστος από πλευράς Νοσοκομείου αφού ο πάροχος νέφους πρέπει να εφαρμόσει όλους τους μηχανισμούς και ελέγχους ασφαλείας για την διατήρηση των επιπέδων σε χαμηλό επίπεδο.

Στην 2η φάση επιλέγονται οι αρχικοί έλεγχοι, οι οποίοι προσδοκάται να παρέχουν το απαιτούμενο επίπεδο ασφάλειας που καθορίζεται από το νοσοκομείο. Οι αρχικοί έλεγχοι είναι η πιστοποίηση του χρήστη (user name και password ή βιομετρικά στοιχεία), η εφαρμογή πρωτοκόλλου SOAP (Simple Object Access Protocol), η χρήση VPN και η εφαρμογή κρυπταλγορίθμου RSA (2048 bit) για κρυπτογράφηση των βάσεων δεδομένων. Εφόσον έγινε η καταγραφή, το επόμενο βήμα είναι η δημιουργία των παραπάνω ελέγχων και η αξιολόγηση των κινδύνων που διατρέχουν οι υπηρεσίες από απειλές εντός και εκτός υπολογιστικού νέφους (κεφ. 4.4). Σημειωτέο είναι ότι για τους ελέγχους ασφάλειας υπεύθυνες είναι και οι τρεις οντότητες.

Στην 3^{η} φάση πραγματοποιείται η εφαρμογή των ελέγχων ασφαλείας, δηλαδή έλεγχος της κρυπτογράφησης των Β.Δ, έλεγχος των πιστοποιητικών και έλεγχος της απομακρυσμένης σύνδεσης μέσω VPN.

Στην 4 φάση πραγματοποιείται η αξιολόγηση των ελέγχων ασφάλειας με εφαρμογή μετρικών ασφαλείας (η αξιολόγηση γίνεται και ποιοτικά και ποσοτικά). Όπως φαίνεται και από τον πίνακα 4 υπεύθυνοι για την αξιολόγηση είναι το νοσοκομείο και ο πάροχος υπολογιστικού σύννεφου (AMAZON). Το Υπουργείο Απασχόλησης και Κοινωνικής Προστασίας (πάροχος υπηρεσιών και προγραμμάτων υγείας) πρέπει απλά να είναι ενημερωμένο.

Στην 5η φάση έχουμε την επίσημη αποδοχή και των 3 οντοτήτων (νοσοκομείο, ΥΑΚΠ, AMAZON) για τους αναγνωρισμένους κινδύνους που περιλαμβάνονται στην υιοθέτηση μιας υπηρεσίας και στην αποδοχή της μετρίασης των κινδύνων αυτών.

Τέλος στην 6η φάση πραγματοποιείται η παροχή εργαλείων ελέγχου ασφάλειας από την AMAZON στο νοσοκομείο/ΠεΣΥ με υποχρεωτική συλλογή μετρικών και δημιουργία αναφοράς βασισμένη σε γεγονός ή περίοδο (IDS, IPS).

ΦΑΣΗ	ΚΑΘΗΚΟΝΤΑ	ΠΑΡΟΧΟΣ ΝΕΦΟΥΣ:AMAZON	ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ: Υ.Α.Κ.Π.	ΟΡΓΑΝΙΣΜΟΣ-ΠΕΛΑΤΗΣ: Νοσοκομείο- ΠεΣΥ	ΕΙΣΟΔΟΣ ΣΤΟΙΧΕΙΩΝ	ΕΞΟΔΟΣ ΑΠΟΤΕΛΕΣΜΑΤΩΝ
Κατηγοριοποίηση των υπηρεσιών ασφάλειας:	SC (Νοσοκομείου)= χαμηλή SC (e-health)= χαμηλή	Ενημερωμένος	Ενημερωμένος	Υπεύθυνος	Α) συγκέντρωση Β) αποθήκευση Γ) διαμοιρασμός ευαίσθητων ιατρικών δεδομένων.	Αποδοχή από Νοσοκομείο-ΠεΣΥ επίπεδα επιπτώσεων από παραβιάσεις των Α), Β) κ Γ)
Επιλογή των ελέγχων ασφάλειας:	Καταγραφή: Πιστοποιητικό χρήστη (username και password ή βιομετρικά) SOAP (Simple Object Access Protocol) VPN RSA 2048 bit κρυπτογράφηση (για βάσεις δεδομένων)	Υπεύθυνος			Λίστα ελέγχων: Πιστοποιητικό χρήστη (username και password ή βιομετρικά) SOAP (Simple Object Access Protocol) VPN RSA 2048 bit κρυπτογράφηση (για βάσεις δεδομένων)	Καταγραφή ελέγχων ασφάλειας: Πιστοποιητικό χρήστη (username και password ή βιομετρικά) SOAP (Simple Object Access Protocol) VPN RSA 2048 bit κρυπτογράφηση (για βάσεις δεδομένων)
	Δημιουργία: Πιστοποιητικό χρήστη (username και password ή βιομετρικά) SOAP (Simple Object Access Protocol) VPN RSA 2048 bit κρυπτογράφηση (για βάσεις δεδομένων)	Υπεύθυνος			Εισαγωγή ελέγχων λαμβάνοντας υπόψη τα επίπεδα επιπτώσεων (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα)	Αρχικοί έλεγχοι & καταλληλότητα αυτών
	Αξιολόγηση των κινδύνων που διατρέχουν οι υπηρεσίες: Απειλές εντός και εκτός υπολογιστικού νέφους (κεφ. 4.4).	Υπεύθυνος			αρχιτεκτονική πλατφόρμας AMAZON (πλατφόρμα ως υπηρεσία), έκθεση ευπαθειών &καταμέτρηση γνωστών αδυναμιών	Αναγνώριση απειλών, ευπαθειών και κινδύνων που προκύπτουν από κεφ. 4.4.
	Παραμετροποίηση των ελέγχων ασφάλειας	Υπεύθυνος			Αξιολόγηση κινδύνων	Σχέδιο διαχείρισης ασφάλειας
Εφαρμογή ελέγχων:	Έλεγχος πιστοποιητικού του χρήστη Έλεγχος κρυπτογράφησης ΒΔ Έλεγχος VPN απομακρυσμένης σύνδεσης	Υπεύθυνος			Σχέδιο διαχείρισης ασφάλειας (καταγραφή υλοποίησης ελέγχου ασφάλειας από AMAZON, Υ.Α.Κ.Π. και Νοσοκομείο - ΠεΣΥ)	Αναβάθμιση σχεδίου ασφάλειας
Αξιολόγηση των ελέγχων ασφάλειας	Ορισμός μετρικών ασφαλείας	Υπεύθυνος	Ενημερωμένος	Υπεύθυνος	Στόχοι ασφάλειας του Νοσοκομείου – ΠεΣΥ (κεφ. 4.3.)	Σχέδιο αξιολόγησης ασφάλειας
	Αξιολόγηση της κατάστασης ασφάλειας	Υπεύθυνος			Σχέδιο αξιολόγησης ασφάλειας	Έκθεση αξιολόγησης
Εξουσιοδότηση των υπηρεσιών	Αναγνώριση κινδύνων από Υ.Α.Κ.Π. , νοσοκομείο και AMAZON.	Ενημερωμένος	Ενημερωμένος	Υπεύθυνος	Σχέδιο ασφάλειας & έκθεση αξιολόγησης	Εξουσιοδότηση υπηρεσιών (RBAC)
Παρακολούθηση της αποτελεσματικότητας των ελέγχων ασφάλειας	Παροχή εργαλείων ελέγχου ασφάλειας από AMAZON σε νοσοκομεια/ΠεΣΥ με υποχρεωτική συλλογή μετρικών και δημιουργία αναφοράς βασισμένη σε γεγονός ή περίοδο (IDS, IPS,)	Υπεύθυνος			Σχέδιο αξιολόγησης ασφάλειας από εργαλεία που παρέχεται από το AMAZON	Έκθεση της τελικής κατάστασης ασφαλείας

Πίνακας 4 Έλεγχος ασφάλειας ηλεκτρονικής υγείας με χρήση του προτύπου NIST-FISMA για μοντέλα υπολογιστικού νέφους

Επίλογος

Στις μέρες μας, το υπολογιστικό σύννεφο αποτελεί μια νέα τεχνολογία με πολλές υποσχέσεις και σταδιακή εξέλιξη. Από τη μία μεριά προσφέρει μειωμένο κόστος λειτουργίας και συντήρησης υλικού (δηλαδή δυνατότητα Return of Investment-ROI, με την πάροδο των 2 με 3 χρόνων το ποσό που έχει αναλωθεί για υιοθέτηση υπολογιστικού νέφους να έχει αποσβεστεί από την διαφορά του κόστους υλικού και λογισμικού εάν χρησιμοποιήσουμε δικούς μας πόρους και υποδομές) και από την άλλη μεριά, γεννιούνται νέοι κίνδυνοι ασφαλείας των πληροφοριών με την χρήση τεχνολογικών υποδομών υπολογιστικού σύννεφου.

Ο τομέας της υγείας στην Ελλάδα χρήζει ανάγκης υιοθέτησης σύγχρονων μορφών ΤΠΕ όπως είναι το υπολογιστικό σύννεφο, εφαρμόζοντας παράλληλα αυστηρούς μηχανισμούς ασφάλειας και διαφύλαξης της ιδιωτικότητας. Για να εφαρμοστεί στην Ελλάδα το υπολογιστικό σύννεφο στον τομέα της υγείας πρέπει πρώτα να τηρηθούν τρεις βασικές προϋποθέσεις.
Η πρώτη προϋπόθεση, είναι η θέσπιση νόμου ή κανονιστικού πλαισίου που να ενσωματώνει την έννοια του υπολογιστικού σύννεφου και να διασφαλίζει την ιδιωτικότητα των ευαίσθητων δεδομένων (όπως ο φάκελος ενός ασθενή) σε αυτό.

Δεύτερη προϋπόθεση για εφαρμογή υπολογιστικού νέφους στην υγεία, είναι η εύρεση παρόχου που να μπορεί να πληρεί τα κριτήρια ασφάλειας που ορίζει το νοσοκομείο-πελάτης προκειμένου ο δεύτερος να τον εμπιστευτεί για την διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα των ευαίσθητων δεδομένων των ασθενών του . Βέβαια σύμφωνα με μελέτη που έγινε στην Ευρώπη ένα μεγάλο ποσοστό παρόχων σύννεφου δεν θέλει να φιλοξενήσει στις υποδομές του δεδομένα ασθενών, αφού πρέπει να λάβει πρόσθετα μέτρα ασφάλειας και συχνά δεδομένα ασθενών γίνονται στόχος επιθέσεων λόγω της μεγάλης εμπορικής και σημασιολογικής αξίας που έχουν.

Τρίτη προϋπόθεση είναι η ψηφιοποίηση όλων των εγγράφων και των χειρόγραφων φακέλων των ασθενών από όλες τις υπηρεσίες του νοσοκομείου, ώστε να καταστεί λειτουργικό το σύστημα ηλεκτρονικής υγείας με χρήση υπολογιστικού νέφους.

Μόλις ολοκληρωθούν και οι τρεις προϋποθέσεις, τότε το σύστημα υγείας στην Ελλάδα θα είναι σε θέση να υιοθετήσει την υποδομή του υπολογιστικού σύννεφου και να προσφέρει ποιοτικότερες υπηρεσίες ηλεκτρονικής υγείας σε αισθητά πολύ μικρότερο χρονικό διάστημα. Τέλος, θα μειωθεί και το λειτουργικό κόστος, αφού η ανάγκη αναβάθμισης και συντήρησης του υλικού θα είναι, σε μεγάλο επίπεδο, μειωμένη.

Παράρτημα

Γλωσσάριο

Διεπαφή εφαρμογής (Application Programming Interface-API): είναι ένα σύνολο προγραμματισμένων οδηγιών που χρησιμοποιούν οι πάροχοι υπολογιστικού σύννεφου μέσω των προγραμματιστών τους, προκειμένου να καταστεί δυνατή η δημιουργία και η ανάπτυξη εφαρμογών για τις υπηρεσίες τους.

Εικονική μηχανή (Virtual Machine): είναι ένας διακομιστής που προσομοιάζει ένα πραγματικό ή πλασματικό υλικό για ένα μη τροποποιούμενο/ φιλοξενούμενο λειτουργικό σύστημα.

Πάροχος σύννεφου/νέφους (Cloud Provider): είναι ο πάροχος ο οποίος διαθέτει χώρο αποθήκευσης, λογισμικό ή λειτουργικό σύστημα σε τρίτους (οργανισμούς-πελάτες) μέσω ενός ιδιωτικού ή δημόσιου δικτύου.

Συμφωνία επιπέδου υπηρεσιών (Service Level Agreement-SLA): είναι η σύμβαση παροχής υπηρεσιών μεταξύ του παρόχου υπολογιστικού νέφους και του οργανισμού-πελάτη. Υπάρχουν δύο τύποι συμφωνιών επιπέδου υπηρεσιών, η προκαθορισμένη αδιαπραγμάτευτη συμφωνία και η συμφωνία κατόπιν διαπραγματεύσεων. Επίσης οι SLAs μπορούν να χρησιμοποιηθούν ως μέσο αντιμετώπισης των “ανησυχιών” ενός οργανισμού για θέματα ασφάλειας, προστασίας των προσωπικών δεδομένων, διαδικασιών, και τεχνικών ελέγχων, όπως η εξουσιοδότηση των εργαζομένων, η εξασφάλιση της ιδιωτικότητας, η κρυπτογράφηση των δεδομένων, η παρακολούθηση και αναφορά της αποτελεσματικότητας των υπηρεσιών, καθώς και η συμμόρφωση με τους νόμους και τους κανονισμούς.

Υπολογιστική χρησιμότητα (Utility Computing): είναι μια μετρούμενη υπηρεσία η οποία επιτρέπει την ενοποίηση του συνόλου των τερματικών, των αποθηκευτικών συστημάτων και των δικτύων σε ένα μεγάλο σύστημα που ευνοεί τη διανομή δύναμης ενός πολλαπλού συστήματος πόρων σε έναν μόνο χρήστη για ένα συγκεκριμένο σκοπό.

Hypervisor: είναι το λογισμικό που ελέγχει το επίπεδο μεταξύ των λειτουργικών συστημάτων υλικού και επιτρέπει σε πολλαπλά λειτουργικά συστήματα να τρέχουν στο ίδιο φυσικό υλικό.

Paravirtyalization: είναι μια τεχνική εικονικού διακομιστή που προσομοιάζει το υλικό για ένα λειτουργικό σύστημα (ΛΣ) φιλοξενίας. Οι Paravirtyalized διακομιστές είναι τροποποιημένα/φιλοξενούμενα λειτουργικά συστήματα που υπάρχουν πάνω από τον Hypervisor. Η κύρια διαφορά τους με μια εικονική μηχανή είναι ότι το ΛΣ σε ένα περιβάλλον paravirtualized τροποποιείται για να λειτουργήσει κατευθείαν με τον Hypervisor ενώ στις εικονικές μηχανές δεν τροποποιείται.

Βιβλιογραφία

[1] Foster I, Zhao Y, Raicu I, Lu S, “Cloud Computing and Grid Computing 360-Degree Compared”. November 2008, In: Grid Computing Environments Workshop (GCE’08), διαθέσιμο στην ιστοσελίδα: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=4729055

[2] Wayne Jansen, Timothy Grance, “Guidelines on Security and Privacy in Public Cloud Computing”, January 2011, National Institute of Standards and Technology, διαθέσιμο στην ιστοσελίδα: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[3] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, January 2011, National Institute of Standards and Technology, διαθέσιμο στην ιστοσελίδα: http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

[4] Dooley B, 2010, ‘Architectural Requirements of the Hybrid Cloud’, *Information Management Online*, 10 February 2010,[On-line Άρθρο], διαθέσιμο στην ιστοσελίδα: http://www.informationmanagement.com/news/hybrid-cloudarchitectural requirements-10017152-1.html

[5] Global Netoptex Incorporated, 2009, “Demystifying the cloud. Important Opportunities, crucial choices”, 13 December 2009, [On-lineΆρθρο], διαθέσιμο στην ιστοσελίδα: http://www.gni.com

[6] Κυριάκος Αποστολίδης, CA Ελλάδας, Κύπρου και Μάλτας, “Το Cloud Computing και ο νέος ρόλος του IT”, 8 Ιουνίου 2010, [On-line Άρθρο], διαθέσιμο στην ιστοσελίδα: http://www.netweek.gr/default.asp?pid=9&la=1&arId=19654&pg=1&ss=

[7] Mohemed Almorsy, John Grundy and Amani S. Ibrahim, 2011 IEEE 4th International Conference on Cloud Computing, “Collaboration-Based Cloud Computing Security Management Framework”, Computer Science & Software Engineering, Faculty of Information & Communication Technologies

[8] Yuji Suga suga, “Business Requirements for Applying Secret Sharing Schemes to Cloud Computing”, [On-line Άρθρο], διαθέσιμο στην ιστοσελίδα:http://www.imi.kyushu-u.ac.jp/PDF/SSCC2011-proceedings.pdf

[9] Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker Westphall, Jorge Werner, Armando Fracalossi, Giovanni Schmitt Salvador, “A Cloud Computing Solution for Patient’s Data Collection in Health Care Institutions”, Network and Management Laboratory – LRG, Federal University of Santa Catarina

[10] Eucalyptus Cloud Computing Platform, Administrator's Guide, Enterprise Edition 2.0, Eucalyptus Systems, Inc.© 2010

[11] Motta, Furuie, "A contextual role based access control authorization model for electronic patient record", IEEE Trans Inform Technol Biomed, September 2003, διαθέσιμο στην ιστοσελίδα:: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1229859

[12] Walid Bagga, Refic Molva, "Collusion-Free Policy-Based Encryption Collusion-Free Policy-Based Encryption", ISC'06 Proceedings of the 9th international conference on Information Security, διαθέσιμο στην ιστοσελίδα: http://www.eurecom.fr/util/publidownload.fr.htm?id=1958

[13] "Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems", NEMA/COCIR/JIRA Security and Privacy Committee (SPC) – December 2004, διαθέσιμο στην ιστοσελίδα: http://hipaa.yale.edu/security/breakglass.html

[14] L. Fan, W. Buchanan, C. Th¨ummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, D. Bell, "DACAR Platform for e-Health Services Cloud", Faculty of Engineering, Computing & Creative Industries, Edinburgh Napier University, Edinburgh, UK, Faculty of Medicine, Imperial College London

[15] Daniele Catteddu and Giles Hogben, "Benefits, Risks and Recommendations for information security", November 2009, [On-line περιοδικό], διαθέσιμο στην ιστοσελίδα:http://www.enisa.europa.eu/

[16] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a Chance of Security Challenges and Improvements", Co-published by the IEEE computer and reliability societies, January/February 2010, [On-line περιοδικό], διαθέσιμο στην ιστοσελίδα: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5403158

[17] Top Threats to Cloud Computing (2010) V1.0 Prepared by the Cloud Security Alliance, διαθέσιμο στην ιστοσελίδα:http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Σχήματα

[1] Αναπαράσταση υπολογιστικού νέφους, οριζόμενο από τα 5 χαρακτηριστικά του, τα 3 μοντέλα υπηρεσιών και τα 4 μοντέλα ανάπτυξής του (σχήμα 1.5), NIST working definition, διαθέσιμο στην ιστοσελίδα: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

[2] Ευθυγράμμιση των προτύπων του NIST-FISMA με το μοντέλο του υπολογιστικού νέφους (πίνακας 1), Alignment of NIST-FISMA standard with the cloud computing model, διαθέσιμο στην ιστοσελίδα: http://www.ict.swin.edu.au/personal/malmorsy/Pubs/cloud2011.pdf

[3] Ασύμμετρες υπηρεσίες υπολογιστικού νέφους (Σχήμα 2.4.1), Asymmetric cloud services, διαθέσιμο στην ιστοσελίδα: http://www.imi.kyushu-u.ac.jp/PDF/SSCC2011-proceedings.pdf

[4] Μοντέλο ροής δεδομένων (Σχήμα 2.4.2), Data flow model, διαθέσιμο στην ιστοσελίδα:http://www.imi.kyushu-u.ac.jp/PDF/SSCC2011-proceedings.pdf

[5] Αναπαράσταση σεναρίου χειρόγραφης καταγραφής ιατρικών δεδομένων (Εικόνα 3.2.1), Current scenario, διαθέσιμο στην ιστοσελίδα: http://www.healthlawyers.org/Members/PracticeGroups/HIT/Toolkits/Documents/Cloud%20Computing%20Resource%20Toolkit/2_ArticlesAndPapers/Rolim-Cloud_Computing_Solution_for_Patient%27s_Data_Collection%20in%20Health%20Care%20Institutions.pdf

[6] Αρχιτεκτονική του μοντέλου (Εικόνα 3.2.2),Proposed solution, διαθέσιμο στην ιστοσελίδα: http://www.healthlawyers.org/Members/PracticeGroups/HIT/Toolkits/Documents/Cloud%20Computing%20Resource%20Toolkit/2_ArticlesAndPapers/Rolim-Cloud_Computing_Solution_for_Patient%27s_Data_Collection%20in%20Health%20Care%20Institutions.pdf

[7] Αναπαράσταση συσχετίσεων του μοντέλου (Εικόνα 3.2.3), Proof-of-concept design, διαθέσιμο στην ιστοσελίδα: http://www.healthlawyers.org/Members/PracticeGroups/HIT/Toolkits/Documents/Cloud%20Computing%20Resource%20Toolkit/2_ArticlesAndPapers/Rolim-Cloud_Computing_Solution_for_Patient%27s_Data_Collection%20in%20Health%20Care%20Institutions.pdf

[8] Παράδειγμα κρυπτογράφησης ιατρικού φακέλου (4.7.3) State of the art on data interoperability and management, διαθέσιμο στην ιστοσελίδα: http://www.infobiomed.org/paginas_en/D11_State_of_Art_Data.pdf