ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ
ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΨΗΦΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ ΥΓΕΙΑΣ ΣΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

(CLOUD COMPUTING)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΑΠΑΔΑΤΟΣ Γ. ΔΗΜΗΤΡΙΟΣ – ΑΘΑΝΑΣΙΟΣ

Επιβλέπων: Διονύσιος – Δημήτριος Κουτσούρης.

Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2011

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ
ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΨΗΦΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ ΥΓΕΙΑΣ ΣΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

(CLOUD COMPUTING)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΑΠΑΔΑΤΟΣ Γ. ΔΗΜΗΤΡΙΟΣ – ΑΘΑΝΑΣΙΟΣ

Επιβλέπων: Διονύσιος – Δημήτριος Κουτσούρης.

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή επιτροπή την 14 Ιουνίου 2011

Διονύσιος-Δημήτριος	Κωνσταντίνα Νικήτα	Παναγιώτης Τσανάκας
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2011

.....

ΠΑΠΑΔΑΤΟΣ Γ. ΔΗΜΗΤΡΙΟΣ- ΑΘΑΝΑΣΙΟΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Κουτσούρη Διονύσιο-Δημήτριο για την εμπιστοσύνη που μου έδειξε στην ανάθεση αλλά και στην ανάπτυξη της παρούσας αυτής ενδιαφέρουσας εργασίας.

Επίσης θα ήθελα να ευχαριστήσω τον συνάδελφο και μέλος του Εργαστηρίου Βιοϊατρικής Τεχνολογίας του Ε.Μ.Π. κ Γκιόκα Κωνσταντίνο, για τις συμβουλές και την καθοδήγησή του κατά τη διάρκεια εκπόνησης της διπλωματικής μου.

Τέλος να ευχαριστήσω τους συνάδελφους και φίλους Ρεμούνδου Ευαγγελία και Φωτιάδη Αναστασία αλλά και τον υποψήφιο διδάκτορα Τσίρμπα Χαράλαμπο, για τον άπλετο χρόνο τους αλλά και τη βοήθειά τους που μου προσέφεραν στη συγγραφή της διπλωματικής μου.

Περίληψη

Η παρούσα διπλωματική έχει σα στόχο την παρουσίαση της νέας διαδικτυακής τεχνολογίας που ονομάζεται υπολογιστικό νέφος (Cloud Computing). Γίνεται μια εκτενής αναφορά στα μοντέλα υπηρεσιών της συγκεκριμένης τεχνολογίας αλλά και τα χαρακτηριστικά τους καθώς και τους σημαντικότερους φορείς που παρέχουν ως υπηρεσία το Cloud Computing. Σημαντικό είναι να διαπιστώσουμε πως συνεργάζονται οι υπηρεσίες υγείας με το υπολογιστικό νέφος, κάτι που περιγράφεται στα κεφάλαια που ακολουθούν. Μεγάλη πρόκληση ήταν το πάντρεμα παραδοσιακών ιατρικών μηχανημάτων με την νέα ψηφιακή υπηρεσία του υπολογιστικού νέφους. Μέσα από όλα αυτά διαπιστώνουμε πόσο εύκολο ήταν να γίνει μετάβαση στο νέο αυτό περιβάλλον τόσο από θέμα εξοπλισμού αλλά και από θέμα προσαρμογής από την πλευρά των χρηστών.

Λέξεις κλειδιά.

Cloud computing, IaaS, Paas, SaaS, EC2, Azure, HealthVault, Eucalyptous, OpenNebula, Hadoop.

Abstract

The present study's purpose is to introduce us to a series of new web technologies described by the term cloud computing. A detailed account is given concerning service models of cloud computing and their main characteristics as well as a listing of the main cloud providers. The study also focuses on the application of cloud computing to health services, as is described in the following chapters. A new challenge is presented by the joining of traditional medical machinery to the new digital services of cloud computing. Our ultimate conclusion depicts the easy transition to cloud technology, considering both the equipment availability and the users' adaptability to the new environment.

Key Words

Cloud computing, IaaS, Paas, SaaS, EC2, Azure, HealthVault, Eucalyptous, OpenNebula, Hadoop.

Περιεχόμενα.

Κεφάλαιο 1 (Cloud Computing). 14

Εισαγωγή Cloud Computing – Γενικά και State of the Art 15

1.1 Αρχιτεκτονική Cloud Computing 18

1.2 Χαρακτηριστικά 20

1.2.1 On-demand self-service. 20

1.2.2 Broad network access 20

1.2.3 Resource pooling. 20

1.2.4 Rapid elasticity 21

1.2.5 Measured Service 21

1.2.6 Sharing of infrastructure: 21

1.3 Μοντέλα Υπηρεσιών. 22

1.3.1 Cloud Software as a Service (SaaS). 22

1.3.2 Cloud Platform as a Service (PaaS). 23

1.3.3 Cloud Infrastructure as a Service (IaaS). 23

1.4 Μοντέλα Ανάπτυξης (Deployment Models): 26

1.4.1 Private cloud. 26

1.4.2 Community cloud. 27

1.4.3 Public cloud. 27

1.4.4. Hybrid cloud. 28

Healthcare applications using cloud computing 30

DiskAgent (https://www.diskagent.com/) 30

TC3 ((Total Claims Capture & Control) Health 30

MedCommons 30

Διαχείριση των Δεδομένων στο Cloud ή Grid 31

Κεφάλαιο 2 (Φορείς Cloud Computing). 33

Εισαγωγή 34
2.1 Amazon S3 (Simple Storage Service) 34
2.2 Google App Engine 35
2.3 Windows Azure 36
2.4 Eucalyptus 37
2.4.1. Αρχιτεκτονική Eucalyptus. 38
2.5 Open Nebula 39
2.6 Απαιτήσεις. 41
2.6.1 Multitenancy: 41
2.6.2 Elasticity: 41
2.6.3 Scalability: 41
2.6.4 Load and Tenant Balancing: 41
2.6.5 Availability: 42
2.7 Κέρδη όταν μια εφαρμογή έχει δημιουργηθεί για να λειτουργεί στο cloud. 43
Κεφάλαιο 3 (Ψηφιακές υπηρεσίες υγείας στο Cloud Computing) 44
Εισαγωγή 45
3.1 Ψηφιακές υπηρεσίες υγείας. 45
3.1.1 caBIG (cancer Biomedical Informatics Grid) 47
3.1.2. *Cap3* 50
3.1.3 GTM & MDS Interpolation 52
3.1.4 Συλλογή πληροφοριών ασθενούς σε ιατρικά διαγνωστικά κέντρα μέσω Cloud Comptuing. 52
3.1.5 Μια λύση μέσω υπολογιστικού νέφους για το ολοκληρωμένου πληροφοριακού συστήματος νοσοκομείου, Hospital Information System (HIS). 56
3.1.5.1 Κίνητρο 57
3.1.5.2 Πρόταση 60
3.1.5.3 Σχεδιασμός ιατρικών συσκευών βασισμένες στο cloud 62
3.1.5.4 Συμπέρασμα 63

3.1.6 Google Health 63
3.1.7 Microsoft HealthVault 68
3.2 Σύγκριση υπηρεσιών Cloud Computing. 72
Κεφάλαιο 4 (Ασφάλεια). 89
Εισαγωγή 90
Ασφάλεια 90
4.1 Απαιτήσεις Ασφάλειας 91
4.1.1 Αυθεντικοποίηση (Authentication): 91
4.1.2 Εμπιστευτικότητα (Confidentiality): 92
4.1.3 Εξουσιοδότηση (Authorization): 92
4.1.4 Ακεραιότητα (Integrity): 92
4.1.5 Μη αποποίηση ευθύνης (Non- repudiation): 92
4.1.6 Διαθεσιμότητα (Availability): 92
4.2 Ασφάλεια Εφαρμογών Ηλεκτρονικού Εμπορίου 93
4.3 Πρωτόκολλο Ασφάλειας SSL 93
4.3.1 Αρχιτεκτονική του SSL 96
4.3.2 SSL Record Protocol 99
4.3.3 Αντοχή του SSL σε Γνωστές Επιθέσεις 101
4.4 Transport Layer Security Protocol, TLS 103
4.5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ 105
4.5.1 Περιεχόμενα πολιτικής ασφαλείας: 105
4.5.2 Ζητήματα που αντιμετωπίζει: 106
4.5.3 ΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΣΤΗ ΣΥΝΤΑΞΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ 108
4.5.4 ΣΧΕΤΙΚΗ ΝΟΜΟΘΕΣΙΑ ΣΤΟΝ ΕΛΛΗΝΙΚΟ ΧΩΡΟ 110
4.5.5 Έλεγχος και Εποπτεία: 115
4.6 Συστήματα Firewalls 116
4.6.1 Η Αναγκαιότητα Χρήσης των Firewalls 119

4.6.2 Επιθέσεις 119
4.6.3 Μέσα Προστασίας 121
4.6.4 Αρχές Ασφάλειας 123
4.6.5 Πλάνο Ασφάλειας 124
4.7 Πύλες Εφαρμογών (Application Gateways) 127
4.7.1 Πληρεξούσιοι Εξυπηρετητές (Proxy Servers) 128
4.7.2 Πλεονεκτήματα και Μειονεκτήματα Πυλών Εφαρμογών (και Proxy Servers) 129
4.7.3 Υβριδικά Συστήματα Ασφάλειας 130
4.7.4 Ψηφιακές Υπογραφές 135
4.8 Η Σημερινή Πραγματικότητα 136
4.9 Διαχείριση της Πρόσβασης των Χρηστών 137
4.9.1 Δήλωση χρηστών 138
4.9.2 Διαχείριση προνομιακών δικαιωμάτων 138
4.9.3 Διαχείριση κωδικών πρόσβασης (password) 139
4.9.4 Ευθύνες Χρηστών 139
4.10 Ασφάλεια στο Cloud 140
4.10.1 Πρότυπα ασφαλείας. 141
Επίλογος. 143
Βιβλιογραφία. 145

Πίνακας περιεχομένων εικόνων.

Σχήμα 1. 1 Τυπική κατανάλωση ισχύος φορητού Η/Υ. 16

Σχήμα 1. 2 Απαιτήσεις υπολογιστικής ισχύος σε διάστημα 12 μηνών..... 17

Σχήμα 1. 3 Αρχιτεκτονική Cloud Computing 18

Σχήμα 1. 4 Τυπικό διάγραμμα cloud computing 20

Σχήμα 1. 5 Ένας υλοποιημένος εικονικός διακομιστής που φιλοξενεί τρία εικονικά μηχανήματα κάθε ένα από τα οποία τρέχει διαφορετικά λειτουργικά συστήματα και χρήση στοίβας λογισμικού. 21

Σχήμα 1. 6 Η στοίβα του υπολογιστικού νέφους. 22

Σχήμα 1. 7 Αρχιτεκτονικές μοντέλων υπηρεσιών Cloud Computing..... 24

Σχήμα 1. 8 Κατηγορίες προσφερόμενων υπηρεσιών ανάλογα με τον τύπο του cloud. 24

Σχήμα 1. 9 Οι προσφερόμενες υπηρεσίες του cloud computing και τα μοντέλα ανάπτυξης. 25

Σχήμα 1. 10 Τύποι σύννεφων βασισμένα σε μοντέλα ανάπτυξης. 26

Σχήμα 1. 11 Παράδειγμα. 28

Σχήμα 1. 12 Κατηγορίες προσφορών κάθε τύπου υπηρεσίας. 29

Σχήμα 1. 13 Σύγκλιση των διαφόρων προκαταβολών που οδηγούν στην εμφάνιση νέφους υπολογιστών..... 32

Σχήμα 2. 1 Λογότυπο Google App Engine..... 35

Σχήμα 2. 2 Λογότυπο Windows Azure 36

Σχήμα 2. 3 Λογότυπο Eucalyptous 37

Σχήμα 2. 4 Αρχιτεκτονική υψηλού επιπέδου του Eucalyptous. 38

Σχήμα 2. 5 Αρχιτεκτονική υψηλού επιπέδου Open Nebula..... 40

Σχήμα 2. 6 Μοντέλο δικτύου για Open Nebula..... 41

Σχήμα 2. 7 Κόστος Cloud σε σχέση με τα συμβατικά μοντέλα. 42

Σχήμα 3. 1 Λογότυπο caBIG 47
Σχήμα 3. 2 Αρχιτεκτονική caBIG 48
Σχήμα 3. 3 *Ένα παράδειγμα λειτουργίας του CaBig στο cloud* 49
Σχήμα 3. 4 Εξελιξιμότητα των εφαρμογών του CAP3 51
Σχήμα 3. 5 Απόδοση των εφαρμογών του CAP3. 52
Σχήμα 3. 6 Τρέχον σενάριο 54
Σχήμα 3. 7 Λύση μέσω cloud computing του προηγούμενου σενάριου. 55
Σχήμα 3. 8 Προτεινόμενη τελική λύση 56
Σχήμα 3. 9 Standard HIS framework based on DICOM protocol 57
Σχήμα 3. 10 The cloud 59
Σχήμα 3. 11 Κατασκευή του HIS που βασίζεται στο cloud 61
Σχήμα 3. 12 Block διάγραμμα εξοπλισμού λήψης ιατρικής εικόνας στο cloud 63
Σχήμα 3. 13 Διαστρωματική Αρχιτεκτονική του Google Health. 64
Σχήμα 3. 14 Πρότυπα ιστού. 65
Σχήμα 3. 15 Πρότυπα ιατρικής πληροφόρησης. 65
Σχήμα 3. 16 Πάροχοι ιατρικής πληροφορίας. 66
Σχήμα 3. 17 Προφίλ κάθε χρήστη στο google health 67
Σχήμα 3. 18 Δειπαφή Rest του google Health 67
Σχήμα 3. 19 Λογότυπο Microsoft Health Vault 68
Σχήμα 3. 20 Πλατφόρμα Health Vault 69
Σχήμα 3. 21 Αλυσίδα παροχής Ιατρικής πληροφορίας. 70
Σχήμα 3. 22 Αρχές σχεδιασμού health Vault 71
Σχήμα 3. 23 Αρχιτεκτονική Microsoft HealthVault 71
Σχήμα 3. 24 Πάροχοι cloud. 72
Σχήμα 3. 25 Πίνακας σύγκρισης παρόχων Cloud 74

Σχήμα 4. 1 Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης. 91

Σχήμα 4. 2 Αρχιτεκτονική Τοποθέτηση του SSL 96

Σχήμα 4. 3 Λειτουργία του SSL Record Protocol 100

Σχήμα 4. 4 Ανάπτυξη περιστατικών ασφάλειας. 109

Σχήμα 4. 5 Εξυπηρετητής τοποθετημένος μέσα από το firewall. 117

Σχήμα 4. 6 Εξυπηρετητής τοποθετημένος έξω από το firewall 118

Σχήμα 4. 7 Πρόσβαση του εξυπηρετητή με τον έξω κόσμο. 119

Σχήμα 4. 8 Τοποθέτηση μιας πύλης εφαρμογών μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου 128

Σχήμα 4. 9 Ένα διπλοσυνδεδεμένο firewall. 131

Σχήμα 4. 10 Ένας σχηματισμός firewall υπολογιστή διαλογής. 133

Σχήμα 4. 11 Ένας σχηματισμός firewall υποδικτύου διαλογής. 134

Σχήμα 4. 12 Έκταση του ελέγχου και της προστασίας σε κάθε υπηρεσία. 142

Επίλογος 1. Ποια είναι η άποψή σας για την τρέχουσα κατάσταση του cloud computing; Πηγή: IDC, 2009 143

Επίλογος 2 Τι οδήγησε τον οργανισμό μας στην επιλογή να επιλέξετε υπηρεσίες cloud computing; Πηγή: IDC, 2009 144

Επίλογος 3 Πόσο σημαντικό είναι για τον οργανισμό μας, ένας προμηθευτής cloud computing υπηρεσιών να έχει τα παρακάτω χαρακτηριστικά; Πηγή: IDC, 2009 144

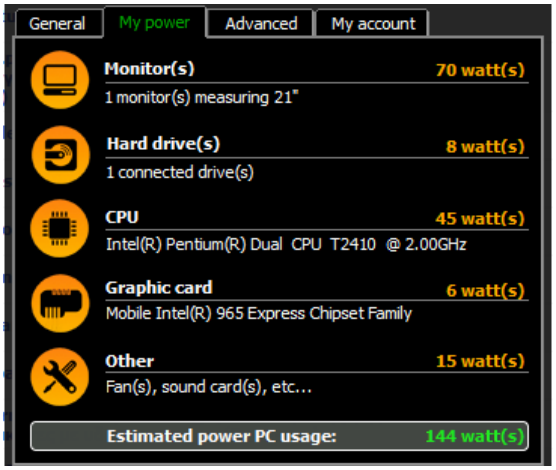
Κεφάλαιο 1.

Cloud Computing

Εισαγωγή Cloud Computing – Γενικά και State of the Art

Η βασική αρχή του υπολογιστικού νέφος (cloud computing) είναι η υποστήριξη της εύκολης δικτυακής πρόσβασης σε μια ομάδα (pool) από παραμετροποιήσιμους υπολογιστικούς πόρους (όπως δίκτυα, εξυπηρετητές, αποθηκευτικούς πόρους, εφαρμογές, υπηρεσίες), οι οποίοι είναι διαθέσιμοι με την ελάχιστη προσπάθεια διαχείρισης και αλληλεπίδρασης από τον πάροχο της συγκεκριμένης υπηρεσίας. Το συγκεκριμένο μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από πέντε σημαντικά χαρακτηριστικά, τρία μοντέλα υπηρεσίας και τέσσερα μοντέλα ανάπτυξης

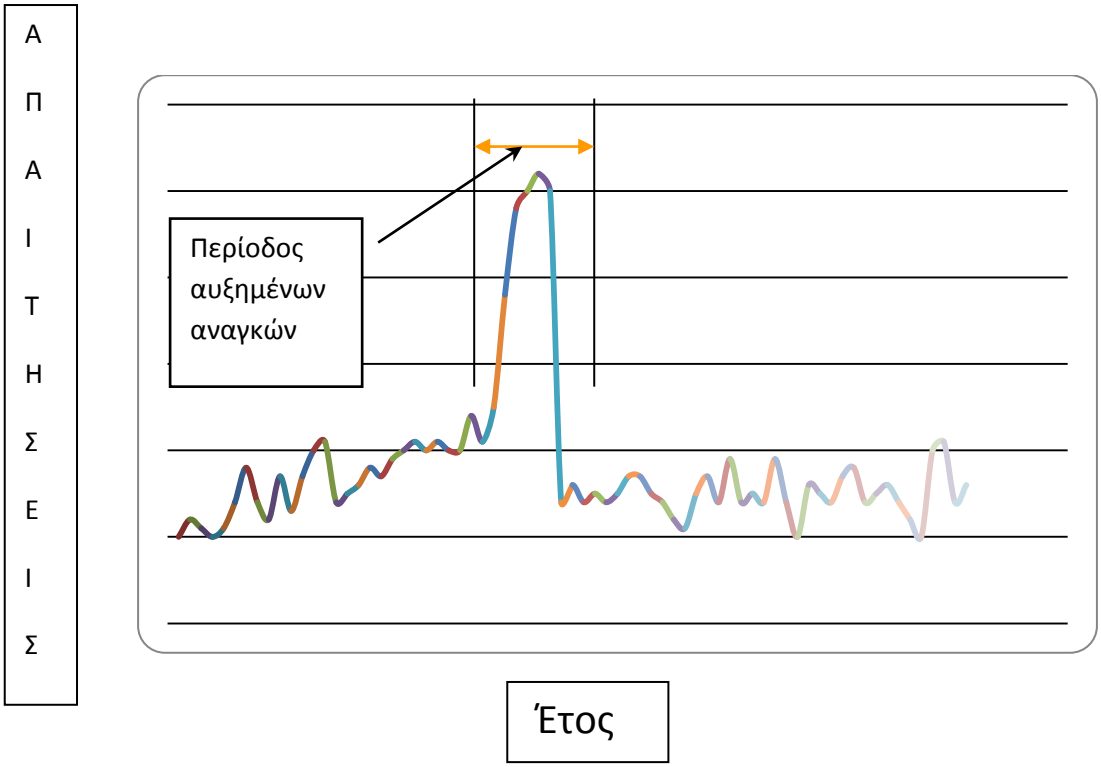
Η μεγάλη ανάπτυξη της τεχνολογίας, καθώς και η ευκολία χρήσης πολλών υπηρεσιών μέσω του διαδικτύου έχει αυξήσει τις ανάγκες σε τεχνολογικές υποδομές τόσο σε απλούς χρήστες όσο και στις εταιρίες παροχής ψηφιακών υπηρεσιών. Για να μπορούν οι απλοί χρήστες να κάνουν χρήση ψηφιακών υπηρεσιών και ειδικότερα υπηρεσιών που παρέχονται από το διαδίκτυο, θα πρέπει να έχουν στη διάθεσή τους όλο τον κατάλληλο εξοπλισμό. Συγκεκριμένα ένα Η/Υ με δυνατότητα δικτύωσης. Από την πλευρά πάλι των εταιριών που θέλουν να κάνουν χρήση διαφόρων ψηφιακών υπηρεσιών, οι απαιτήσεις είναι περισσότερο αυξημένες. Σε επαγγελματικό επίπεδο, αυτό που πρέπει να λάβουμε σοβαρά υπ'όψιν μας, είναι ο αριθμός των χρηστών που θα χρειαστεί να κάνουν χρήση των υπηρεσιών, καθώς και η πιθανότητα να γίνει χρήση του εξοπλισμού από όλους ταυτόχρονα ή μεμονωμένα. Ο τρόπος χρήσης είναι αυτός που θα δημιουργήσει και τις απαιτήσεις σε υπολογιστική ισχύ αλλά και αποθηκευτικό χώρο. Επίσης ο αριθμός των χρηστών θα επηρεάσει σε μεγάλο βαθμό τη πιθανότητα επέκτασης του δικτύου της εταιρίας. Η αύξηση των χρηστών που κάνουν χρήση μιας υπηρεσίας, προκαλεί αύξηση αναγκών σε υποδομές. Αυτό προκαλεί οικονομική επιβάρυνση, αλλά επιβάρυνση και σε ενεργειακό επίπεδο. Όσο περισσότεροι Η/Υ λειτουργούν, άρα τροφοδοτικά και ηλεκτρονικά κυκλώματα, τόσο αυξάνει και η κατανάλωση ηλεκτρικής ισχύος. Μια τυπική κατανάλωση ισχύος σε ένα φορητό υπολογιστή που γίνονται καταχωρήσεις στοιχείων αλλά και επεξεργασία αυτών φαίνεται στην παρακάτω εικόνα.



Σχήμα 1. 1 Τυπική κατανάλωση ισχύος φορητού Η/Υ.

Αν λοιπόν είναι μεγάλος ο αριθμός των Η/Υ που χρησιμοποιούνται καταλαβαίνουμε πως πέρα από οικονομικό, το βάρος γίνεται και ενεργειακό.

Ένας παράγοντας που πρέπει να λάβουμε σοβαρά σημασία είναι και η συχνότητα χρησιμοποίησης της ψηφιακής υπηρεσίας και κατά επέκταση και του εξοπλισμού που χρησιμοποιείται προκειμένου να γίνει σωστή χρήση αυτής. Πρέπει δηλαδή να δούμε σε τι συχνότητα χρησιμοποιείται η υπηρεσία μέσα στο μήνα αλλά και μέσα στο έτος. Υπάρχουν περιπτώσεις όπως σε εφορίες ή νοσοκομεία, που σε συγκεκριμένες περιόδους μέσα στο έτος, υπάρχει αυξημένη ανάγκη καταχωρήσεων και επεξεργασίας δειγμάτων, όπως η περίοδος φορολογικών δηλώσεων ή και περίοδος εισαγωγής νεοσύλλεκτων στο σώματα των Ε.Δ.. Σε αυτές τις περιπτώσεις που δεν είναι και οι μοναδικές, η ανάγκη αυξημένων αναγκών διαρκεί λίγο. Είναι επιβεβλημένη όμως ανάγκη οι απαιτήσεις αυτές να πρέπει να καλυφθούν. Είναι ασύμφορο όμως να επενδύονται χρήματα για να δημιουργηθούν υποδομές οι οποίες έχουν πολλές δυνατότητες αλλά δεν πρόκειται να αξιοποιηθούν πλήρως. Αυτό θα είναι ασύμφορο και οικονομικά, ενεργειακά αλλά και γραφειοκρατικά.



Σχήμα 1. 2 Απαιτήσεις υπολογιστικής ισχύος σε διάστημα 12 μηνών

Το παραπάνω διάγραμμα, περιγράφει τις απαιτήσεις υπολογιστικής ισχύος μέσα σε διάστημα 12 μηνών για μια υπηρεσία-εταιρία που κάνει χρήση μιας ψηφιακής υπηρεσίας η οποία παρουσιάζει αυξημένες απαιτήσεις, συγκεκριμένες περιόδους του έτους, (πχ διάρκεια εισαγωγής νεοσύλλεκτων για ένα στρατιωτικό νοσοκομείο).

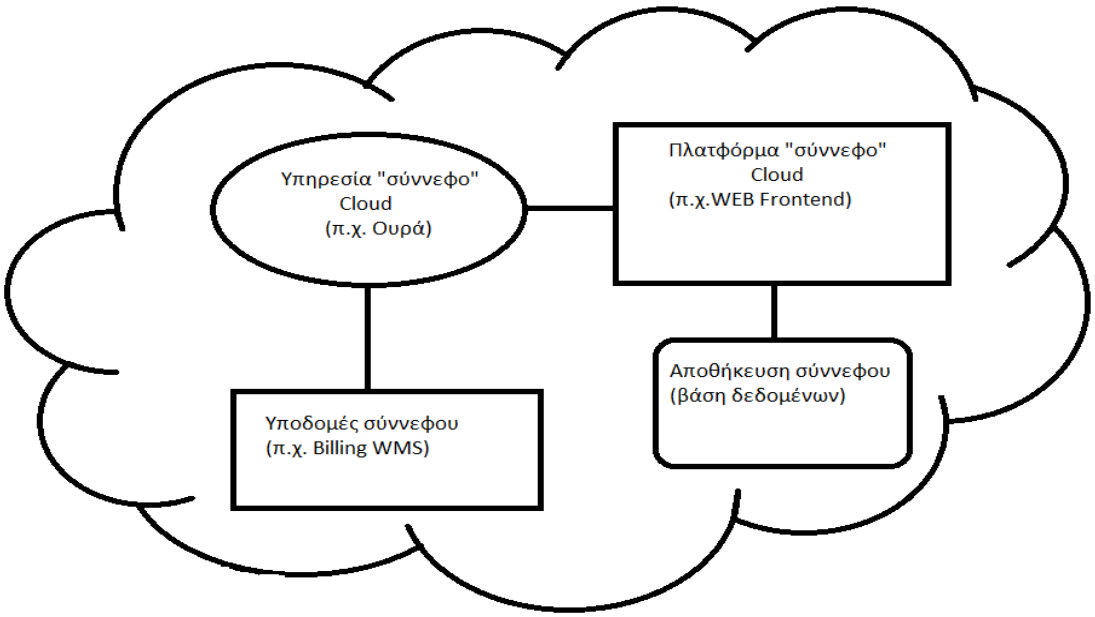
Ακόμα η συνεχόμενη ανάπτυξη της τεχνολογίας, έχει σαν συνέπεια να θεωρούνται πολλοί Η/Υ ξεπερασμένοι μετά από μικρό χρονικό διάστημα, διότι έχουν δημιουργηθεί νέοι με περισσότερες δυνατότητες και χαρακτηριστικά πολλές φορές ασύμβατα με της προηγούμενης γενιάς. Αυτό έχει σαν συνέπεια να μην μπορεί να υπάρξει αναβάθμιση αλλά αντικατάσταση. Ακόμα η συνεχόμενη ανάπτυξη στην τεχνολογία του λογισμικού, προκαλεί ανάγκη συνεχούς αναβάθμισης σε επίπεδο hardware στους Η/Υ.

Συνοψίζοντας βλέπουμε πως υπάρχει μια συνεχής ζήτηση πόρων (χρήματα, υπολογιστική ισχύ, ενεργειακές απαιτήσεις), και το όφελος που πρόκειται να ληφθεί κάποιες φορές είναι μικρότερο. Αυτές τις ανάγκες έρχεται να καλύψει το τεχνολογικό περιβάλλον των υπολογιστικών νεφών (cloud computing).

Μια λύση που υπάρχει για να λυθούν τα συγκεκριμένα προβλήματα απαιτήσεων, είναι το τεχνολογικό περιβάλλον των υπολογιστικών νεφών

(cloud computing). Η έννοια του cloud computing αποτελεί μια νέα προσέγγιση στον χώρο των κατανεμημένων συστημάτων η οποία όμως χρησιμοποιεί και κάποιες τεχνολογίες που προϋπήρχαν. Σχετικά με τον ορισμό της έννοιας έχουν γίνει πολλές προσπάθειες οι οποίες όμως δεν καλύπτουν όλες τις πτυχές του συστήματος με αποτέλεσμα την γενίκευση της έννοιας με τέτοιον τρόπο που cloud computing να θεωρείται κάθε σύστημα το οποίο επιτρέπει ανάθεση υπολογιστικών και αποθηκευτικών υπηρεσιών εξωτερικά. Ως κύριο χαρακτηριστικό της υπηρεσίας είναι το διαδίκτυο (internet).

Πρόκειται για μια υπηρεσία που ασχολείται με την ανάπτυξη και χρήση της τεχνολογίας των Η/Υ μέσω του διαδικτύου. Σε αυτή την υπηρεσία όλες οι πληροφορίες αποθηκεύονται μέσα στο «σύννεφο», αλλά και οι εφαρμογές εκτελούνται μέσα από το «σύννεφο». Στο σχήμα που ακολουθεί φαίνεται η αρχιτεκτονική αυτής της τεχνολογίας.



Σχήμα 1. 3 Αρχιτεκτονική Cloud Computing

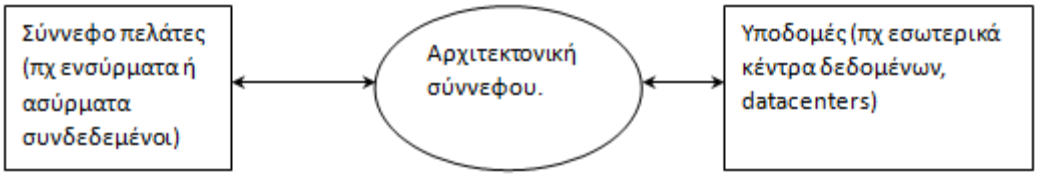
1.1 Αρχιτεκτονική Cloud Computing

Η βασική έννοια της τεχνολογίας υπολογιστικών νεφών τοποθετείται στο 1960 όταν ο John McCarthy πρότεινε, η διαδικασία υπολογισμών μέσων μηχανημάτων κάποια μέρα θα οργανωθεί και θα στηθεί σαν μια δημόσια εφαρμογή. Εφαρμογές όπως αντιϊκή προστασία μέσω ίντερνετ, google Docs,

Gmail και άλλες εφαρμογές που τρέχουν μέσω διαδικτύου είναι εφαρμογές Cloud computing.

Αυτό που μας προσφέρει η υπηρεσία υπολογιστικών νεφών, είναι εξοικονόμηση σε όλα τα προβλήματα που αναφέραμε προηγουμένως. Από τη στιγμή που μπορούμε να νοικιάσουμε από ένα πάροχο υπηρεσιών μια υπηρεσία που καλύπτει τις ανάγκες μας, έχουμε γλυτώσει σε πρώτο στάδιο την ανάγκη ανάπτυξης και υποστήριξης της υπηρεσίας. Συγκεκριμένα προκειμένου να μπορέσει να εκτελεστεί σε ένα εξυπηρετητή (server) μια υπηρεσία, χρειάζεται να υπάρχει κάποιος διαχειριστής που θα έχει την ευθύνη της σωστής και συνεχής παροχής αυτής. Η διαδικασία αυτή προϋποθέτει τεχνογνωσία και χρόνο. Προκειμένου να μπορέσει να συγκροτηθεί σωστά η υποδομή που θα λειτουργήσει η υπηρεσία, χρειάζεται η ανάλογη προκήρυξη διαγωνισμού για να μπορέσει να βρεθεί η καλύτερη και πιο συμφέρουσα λύση. Αντί λοιπόν να δημιουργηθεί ένας μεγάλος διαγωνισμός με πολλές προτάσεις, διοργανώνεται ένας οποίος θα αφορά μόνο το cloud computing. Σε αυτό το στάδιο, η παροχή της υπηρεσίας γίνεται από λίγους παρόχους. Συνεπώς το όφελος που προκύπτει είναι μεγάλο διότι θα προκύψει ακόμα πιο γρήγορα η εκτέλεση της υπηρεσίας λόγω της μείωσης του χρόνου της γραφειοκρατίας.

Η νεφοϋπολογιστική προσφέρεται από κέντρα δεδομένων (data centers) μέσω του διαδικτύου. Η νεφοϋπολογιστική υποδομή αποτελειται σήμερα από υπηρεσίες που προσφέρονται μέσω κέντρων δεδομένων που δημιουργούνται σε εξυπηρετητές (servers) με διάφορα επίπεδα ψηφιακών τεχνολογιών. Μερικά από τα κύρια χαρακτηριστικά της νεφοϋπολογιστικής είναι η ελαχιστοποίηση της επενδυτικής δαπάνης των πελατών, η χρησιμοποίηση καλύτερης ποιότητας λογισμικού με χαμηλότερο κόστος και η δυνατότητα των χρηστών να χρησιμοποιούν την υπολογιστική τεχνολογία ασχέτως της θέσης τους ή των εργαλείων που διαθέτουν. Το προβλεπόμενο αποτέλεσμα της ανάπτυξης της νεφοϋπολογιστικής είναι η συγκέντρωση υπολογιστικής ισχύος σε λιγότερους χώρους με χαμηλό κόστος εγκατάστασης και λειτουργίας, καθώς και συγκέντρωση λογισμικού σε λιγότερα κέντρα στα οποία η δημιουργία, η συντήρηση και η υποστήριξη του νεφολογισμικού θα γίνεται παγκόσμια από λιγότερες ομάδες ικανών επιστημόνων. Ενω η νεφοϋπολογιστική υπόσχεται πολλά οφέλη σε εταιρείες και άτομα, ενέχει μερικούς σοβαρούς κινδύνους που αφορούν στην ασφάλεια των δεδομένων. Η νεφοϋπολογιστική θεωρείται από τους ειδικούς το απώτατο βήμα ολοκλήρωσης της παγκοσμιοποίησης.



Σχήμα 1. 4 Τυπικό διάγραμμα cloud computing

Παραπάνω φαίνεται ένα τυπικό διάγραμμα δικτύου. Αυτό μας δείχνει τον τρόπο που κάποιος πελάτης (client) μέσω του εξοπλισμού του

1.2 Χαρακτηριστικά.

Ουσιώδη Χαρακτηριστικά:

1.2.1 On-demand self-service. Ο χρήστης μπορεί να μονομερώς να χρησιμοποιεί υπολογιστικούς πόρους, όπως χρόνος του εξυπηρετητή και αποθηκευτικούς πόρους δικτύου αυτόματα, ανάλογα με τις ανάγκες του, χωρίς να απαιτείται διάδραση από τον πάροχο της συγκεκριμένης υπηρεσίας.

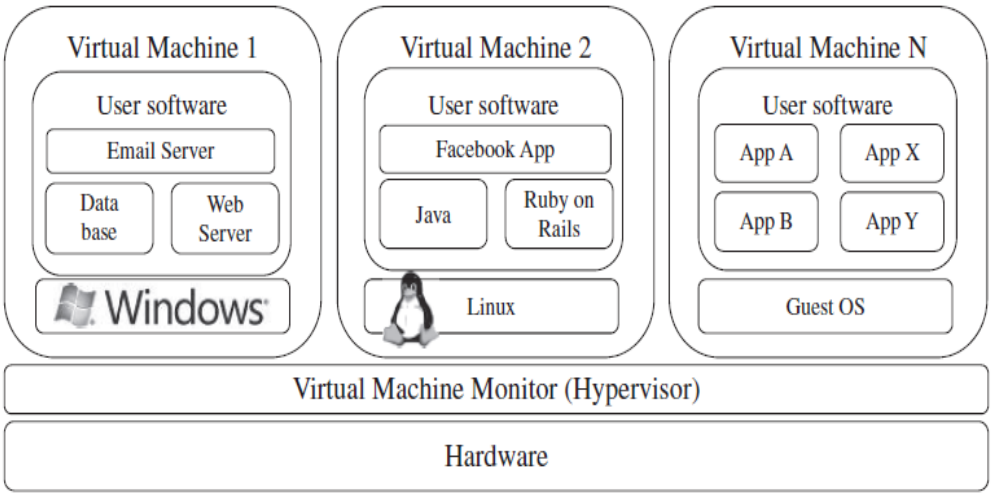
1.2.2 Broad network access. Οι δυνατότητες / πόροι είναι διαθέσιμοι μέσα από το δίκτυο στο οποίο μπορεί κάνεις ν έχει πρόσβαση μέσα από γνωστούς μηχανισμούς, οι οποίοι προωθούν την χρήση ετερογενών τερματικών συσκευών στην πλευρά του τελικού χρήστη (όπως κινητά Τηλέφωνα, laptops και PDAs).

1.2.3 Resource pooling. Οι υπολογιστικοί πόροι του παροχέα είναι συγκεντρωμένοι έτσι ώστε να μπορούν αν εξυπηρετήσουν παράλληλα πολλούς πελάτες χρησιμοποιώντας το μοντέλο multi-tenant, με διαφορετικούς φυσικούς και εικονικούς πόρους να έχουν αντιστοιχηθεί δυναμικά ανάλογα με την ζήτηση του κάθε πελάτη. Ο χρήστης δεν έχει τον έλεγχο ή την γνώση για την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να έχει την δυνατότητα να καθορίσει σε σχετικά αφηρημένο επίπεδο την ακριβή τοποθεσία (όπως χώρα, περιοχή ή data center). Οι πόροι μπορεί να είναι αποθηκευτικός χώρος, υπολογιστική ισχύ, μνήμη, εύρος ζώνης και εικονικές μηχανές (virtual machines).

1.2.4 Rapid elasticity *(Ταχεία Ελαστικότητα).* Οι πόροι αυτοί μπορούν με πολύ ευέλικτο τρόπο να αυξηθούν σε πολύ γρήγορα, σε πολλές περιπτώσεις με αυτόματο τρόπο, έτσι ώστε να μην υπάρχει διάδραση με τον πελάτη, με σκοπό την αποφυγή χρονοβόρων διαδικασιών.

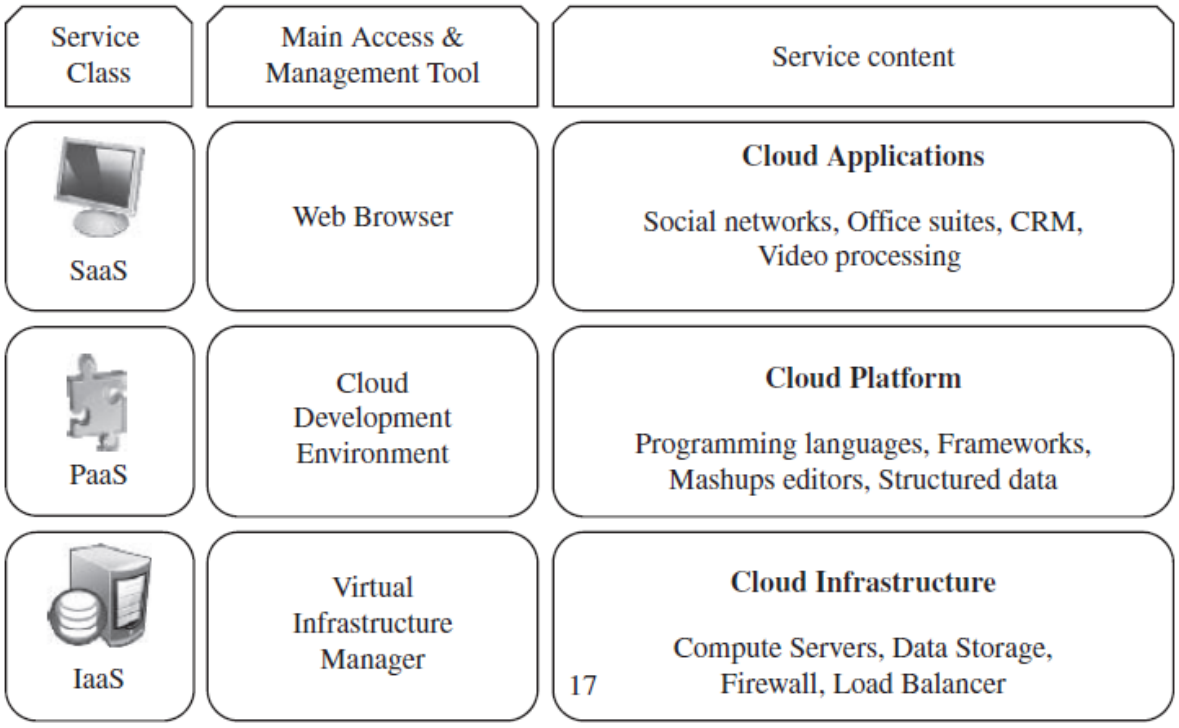
1.2.5 Measured Service *(Μετρούμενη Υπηρεσία). Τα cloud συστήματα έχουν την δυνατότητα αυτόματα να ελέγχουν και να βελτιώνουν τους διαθέσιμους πόρους χρησιμοποιώντας ένα μηχανισμό μέτρησης, ανάλογα με τον τύπο της προσφερόμενης υπηρεσίας. Οι χρησιμοποιούμενοι πόροι μπορούν να ελέγχονται και να παρακολουθούνται χωρίς να γίνονται αντιληπτοί τόσο στον παροχέα όσο και στον χρήστη της χρησιμοποιούμενης υπηρεσίας.*

1.2.6 Sharing of infrastructure: Το φυσικό hardware που εκτελεί το λογισμικό δεν έχει αντιστοίχηση 1:1, δηλαδή ο εξυπηρετητής (server) μπορεί να εκτελεί λειτουργίες πολλών εικονικών εξυπηρετητών επιτρέποντας έτσι εξοικονόμηση πόρων. Άρα οι τελικοί χρήστες μπορούν να έχουν περισσότερα οφέλη με λιγότερους πόρους (hardware) και μπορεί τώρα ο πάροχος υπηρεσίας να πουλήσει τους ανεκμετάλλευτους πόρους αλλού πλέον αν εκείνος το επιθυμεί.



Σχήμα 1. 5 Ένας υλοποιημένος εικονικός διακομιστής που φιλοξενεί τρία εικονικά μηχανήματα κάθε ένα από τα οποία τρέχει διαφορετικά λειτουργικά συστήματα και χρήση στοίβας λογισμικού.

1.3 Μοντέλα Υπηρεσιών.



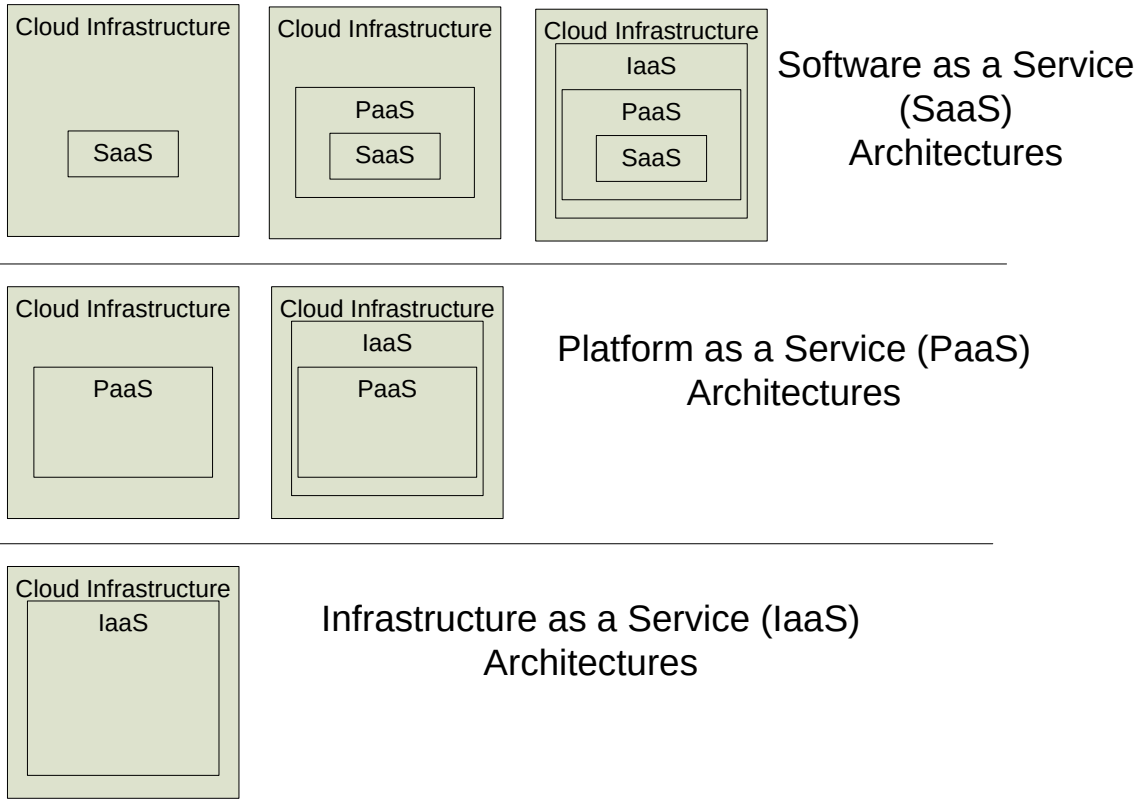
Σχήμα 1. 6 Η στοίβα του υπολογιστικού νέφους.

1.3.1 Cloud Software as a Service (SaaS). Οι δυνατότητα που παρέχεται στον χρήση είναι να μπορεί να χρησιμοποιήσει τις εφαρμογές του παροχέα σε μιας υποδομή cloud. Οι εφαρμογές είναι προσβάσιμες μέσα από διεπαφές ή εργαλεία όπως για παράδειγμα ένας Internet Browser. Ο χρήστης δεν έχει την δυνατότητα να διαχειρίζεται ή να ελέγχει την υποδομή που μπορεί να αποτελείται από το δίκτυο, τους εξυπηρετητές, λειτουργικά συστήματα, αποθηκευτικοί χώροι ή ακόμα και ειδικές δυνατότητες της εφαρμογής όπως περιορισμοί στην παραμετροποίηση της εφαρμογής για τον συγκεκριμένο χρήστη. Ένα τέτοιο παράδειγμα είναι η εφαρμογή του web mail. Ο τελικός χρήστης δε χρειάζεται να κατανοήσει και να μπορεί να υποστηρίξει τη

φιλοσοφία της υπηρεσίας αλλά μόνο να μπορεί να τη χρησιμοποιήσει μέσα από τη διεπαφή που διαθέτει (φυλλομετρητής).

1.3.2 Cloud Platform as a Service (PaaS). Η δυνατότητα που παρέχεται στον χρήστη είναι να αναπτύσσει μεσα στην υποδομή του cloud εφαρμογές οι οποίες δημιουργούνται με την χρήση μιας γλώσσας προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο της υπηρεσίας. Ο χρήστης δεν ελέγχει η διαχειρίζεται την υποδομή του cloud, αλλά έχει τον έλεγχο της αναπτυσσόμενης εφαρμογής και μπορεί επίσης να έχει και της δυνατότητα παραμετροποίησης του περιβάλλοντος στο οποίο βρίσκεται η εφαρμογή. Οι πάροχοι υπηρεσιών PaaS συνήθως προσφέρουν μια ομαδοποίηση λογισμικού και υποδομής σε μορφή προγραμματιζόμενου περιβάλλοντος, και παρέχεται στον τελικό χρήστη ένα σύννεφο στο οποίο μπορεί να φιλοξενήσει τις δικές του εφαρμογές ή υπηρεσίες.

1.3.3 Cloud Infrastructure as a Service (IaaS). Η δυνατότητα που παρέχεται στον χρήστη να έχει τον έλεγχο βασικών υπολογιστικών πόρων και εφαρμογών. Ο χρήστης της υπηρεσίας δεν έχει την δυνατότητα να ελέγχει την υποδομή του cloud, αλλά έχει την δυνατότητα να ελέγχει το λειτουργικό σύστημα, τον αποθηκευτικό χώρα καθώς επίσης και τις αναπτυσσόμενες εφαρμογές και πιθανόν να έχει και περιορισμένων έλεγχο σε κάποιους δικτυακούς πόρους όπως για παράδειγμα firewalls.



Σχήμα 1. 7 Αρχιτεκτονικές μοντέλων υπηρεσιών Cloud Computing

Infrastructure services
- Storage
- Compute
- Services management
- Networking, firewalls, load balancers, and so on.

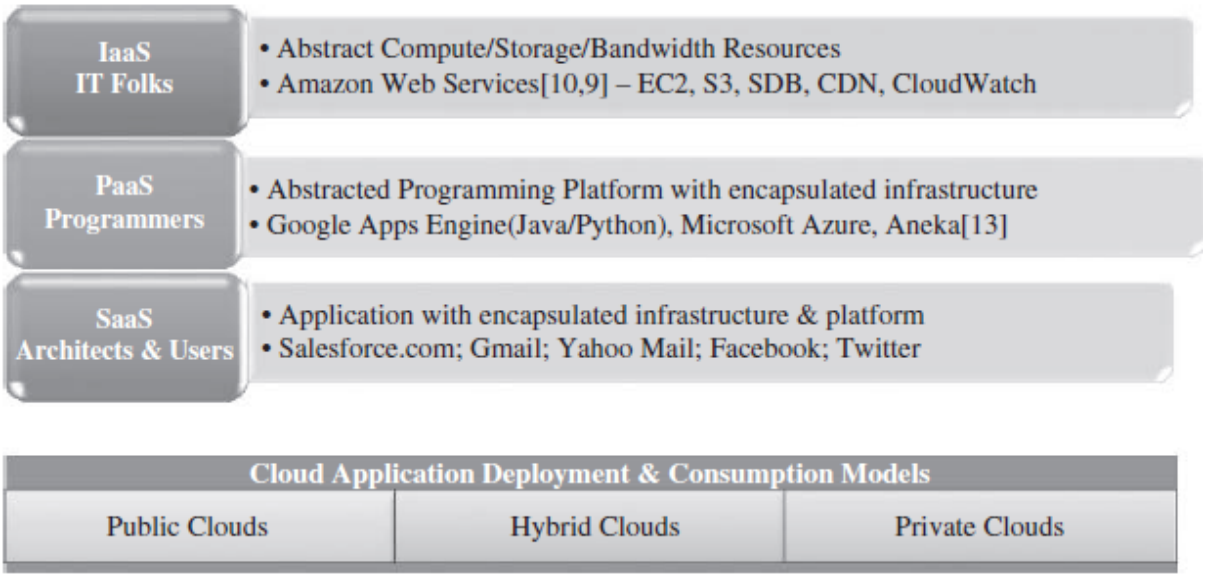
Software services
- Billing
- Financials
- Legal
- Sales
- Desktop productivity
- Human resources
- Content management
- Collaboration
- Social networks
- Backup and recovery
- CRM
- Document management

Cloud platforms
- Public clouds
- Private coluds
- Open clouds
- Custom clouds

Platform services
- General purpose
- Business intelligence
- Integration
- Development and testing
- Database

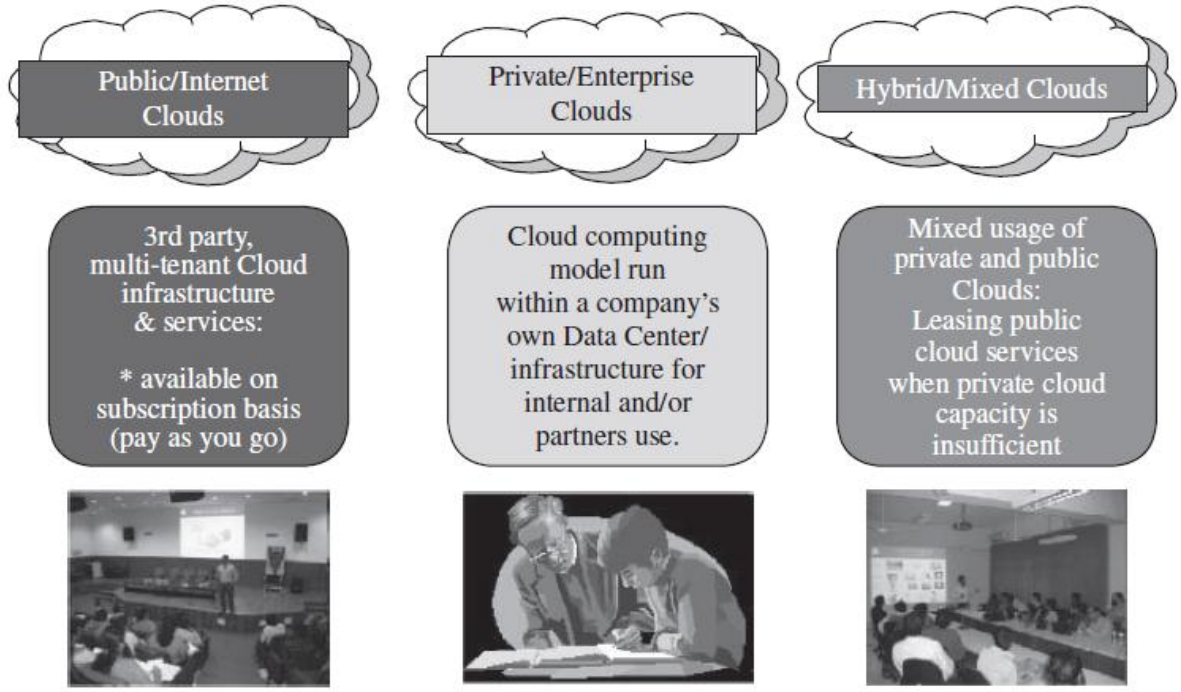
Cloud software
- Data
- Appliances
- Compute
- Cloud management
- File storage

Σχήμα 1. 8 Κατηγορίες προσφερόμενων υπηρεσιών ανάλογα με τον τύπο του cloud.



Σχήμα 1. 9 Οι προσφερόμενες υπηρεσίες του cloud computing και τα μοντέλα ανάπτυξης.

1.4 Μοντέλα Ανάπτυξης (Deployment Models):



Σχήμα 1. 10 Τύποι σύννεφων βασισμένα σε μοντέλα ανάπτυξης.

1.4.1 Private cloud. *Η υποδομή του cloud λειτουργεί αποκλειστικά για ένα οργανισμό. Μπορεί να διαχειρίζεται από τον ίδιο τον οργανισμό ή από κάποιον τρίτο και μπορεί να βρίσκεται στης κτιριακές υποδομές του οργανισμού. Σε αντίθεση με τα Public Clouds, τα Private Clouds είναι εσωτερικά φιλοξενούμενα. Η σφραγίδα ενός ιδιωτικού cloud συνήθως αφιερώνεται σε οργανισμούς. Οι οργανισμοί στην προσπάθεια να αναπτύξουν τα ιδιωτικά clouds, εφαρμόζουν εικονικοποίηση μέσα στα δικά τους κέντρα δεδομένων. Μια λέξη προσοχής: «Η περιγραφή του ιδιωτικού Cloud μας απελευθερώνει από τους περιορισμούς του δημόσιου Cloud που μόνο κακό κάνουν σε αυτό το μοντέλο Cloud. Η πειθαρχεία μέσα στις εφαρμογές των cloud τα καθιστά περισσότερο ενδιαφέροντα και λιγότερο δαπανηρά σε αντίθεση με τη τα συμβατικά IT. Τα ιδιωτικά cloud θα μπορούσαν να είναι πιο περιορισμένα σε σχέση με τα αντίστοιχα δημόσια αντίστοιχά τους, και πιθανώς θα ικανοποιήσουν εκείνες τις ανάγκες που τα δημόσια δεν μπορούν να εξετάσουν.»*

Αν και τα ιδιωτικά σύννεφα είναι ικανοποιητικά καλά, κάποιες από τις ανησυχίες ασφάλειας που ισχύουν στα δημόσια cloud, στα ιδιωτικά δεν ισχύουν. Ακριβώς όμως επειδή είναι ιδιωτικά δε σημαίνει ότι είναι και πιο ασφαλή. Στο ιδιωτικό σύννεφο, εκτιμήσεις όπως εξασφάλιση του εικονικου

περιβάλλοντος(που είναι το λογισμικό, το φυσικό υλικό (hardware), και το firmware) γίνονται από τον πελάτη, εν αντιθέση με το κοινό cloud, που όλα αυτά τα αναλαμβάνει ο πάροχος υπηρεσίας. Κατά συνέπεια, σε συγκρίσεις του ιδιωτικού με το κοινό Cloud, είναι δύσκολο να κάνουν γενικεύσεις για το ποιο είναι ασφαλέστερο από τα δύο. Ένα ιδιωτικό cloud προσφέρει τη δυνατότητα να επιτύχουμε μεγαλύτερη ασφάλεια. Το πραγματικό πλεονέκτημα ενός ιδιωτικού cloud είναι ότι ο πάροχος έχει το ενδιαφέρον για να κάνει το περιβάλλον της διεπαφής να βρίσκεται περισσότερο κοντά στις ανάγκες του εκμισθωτή.

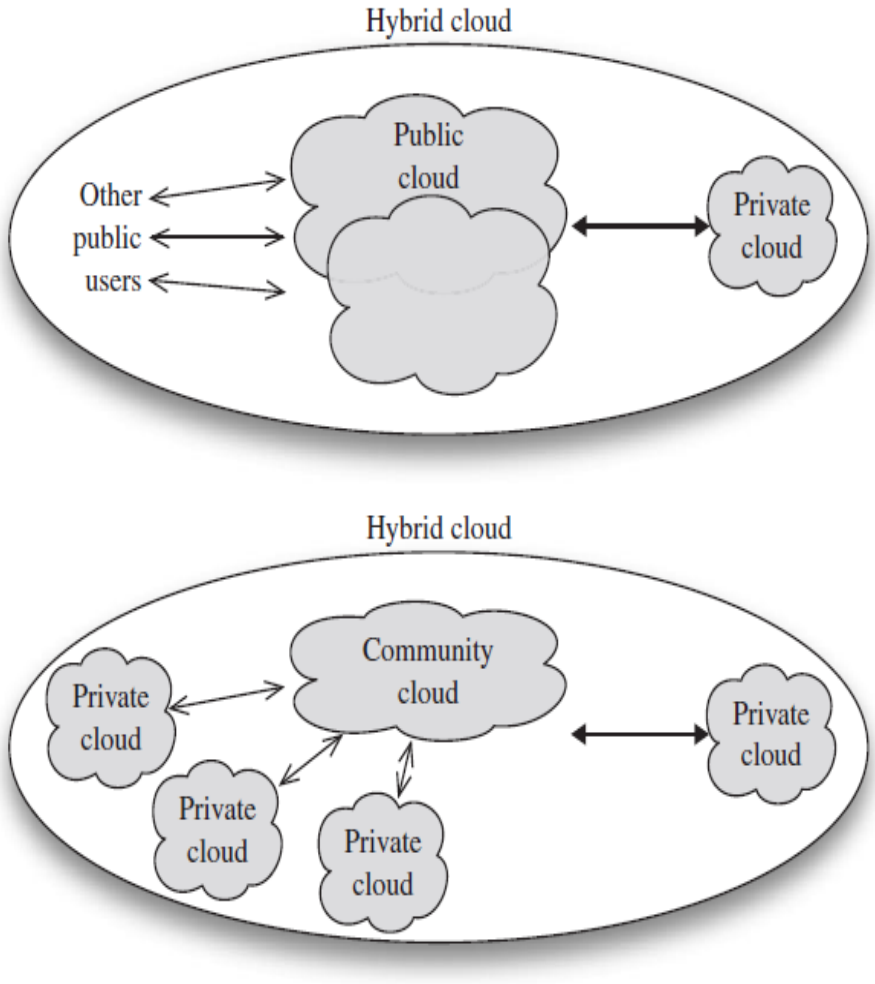
1.4.2 Community cloud. *Η υποδομή του cloud είναι διαμοιρασμένη σε διάφορους οργανισμούς και υποστηρίζει προκαθορισμένες κοινότητες που μπορεί να έχουν κοινές απαιτήσεις, σε επίπεδο ασφάλειας, λειτουργικότητας, αποστολής. Μπορεί να διαχειρίζεται είτε από ένα οργανισμό είτε από κάποιον εξωτερικό παροχέα και μπορεί να βρίσκεται στις κτηριακές υποδομές του οργανισμού. Η υπόσχεση των Community Clouds είναι ότι επιτρέπουν πολλαπλές ανεξάρτητες οντότητες για να κερδίσουν τα κόστη-κέρδη ενός κοινού μη δημόσιου σύννεφου, αποφεύγοντας την ασφάλεια και ρυθμιστικές ανησυχίες που μπορούν να υπάρξουν σε ένα κοινό σύννεφο που δεν τα έχει προβλέψει στο SLA του. Αυτό το πρότυπο έχει τεράστιες δυνατότητες για τις οντότητες ή τις επιχειρήσεις που υπόκεινται σε ρυθμιστικές συμμορφώσεις ή περιορισμούς. Τα διάφορα Community clouds θεωρούνται από τις Ηνωμένες Πολιτείες και την Ευρωπαϊκή ένωση ως τοπικά επίπεδα. Αυτό έχει μεγάλο νόημα δεδομένου ότι υπάρχουν πολλαπλάσια οφέλη και στα δύο ως μεμονωμένες οντότητες καθώς επίσης και συλλογικά.*

1.4.3 Public cloud. *Η* υποδομή του cloud μπορεί να είναι διαθέσιμη στο κοινό ή σε ένα μεγάλη ομάδα από οργανισμούς/επιχειρήσεις και να ανήκει σε ένα οργανισμό που διαχειρίζεται υπηρεσίες cloud. Στην απλούστερη εκδοχή του ένα δημόσιο σύννεφο (public cloud) είναι διαθέσιμο εξωτερικά στον τελικό χρήστη με μικρό περιορισμό για το ποιος μπορεί να γίνει χρήστης της υπηρεσίας με πληρωμή. Οι πιο κοινές μορφές του public cloud είναι αυτές που είναι προσβάσιμες μέσω του διαδικτύου. Τα τελευταία χρόνια έχει υπάρξει τεράστια ανάπτυξη του public cloud με αποτέλεσμα να υπάρχει μεγάλη προσφορά σε υπηρεσίες IaaS από εταιρίες όπως η Amazon με την υπηρεσία EC2, την IBM BlueCloud και την Rackspace cloud offering. Άλλες μορφές προφοράς public cloud σε υπηρεσίες PaaS γίνονται από την Google με το AppEngine & το Windows Azure.

Στο βασικό επίπεδο, τα δημόσια σύννεφα έχουν μοναδικά στοιχεία ασφάλειας και κριτήρια αξιολόγησης σε σχέση με τα ιδιωτικά σύννεφα (Private Clouds). Τα public cloud μπορούν να διαμορφωθούν από τους παρόχους υπηρεσιών

που θέλουν μια υποδομή μεγάλης δυναμικότητας και ένα ευρύ φάσμα πελατών. Ως αποτέλεσμα τα δεδομένα μπορούν να αποθηκευτούν σε κοινά μέσα αποθήκευσης, κάτι που καθιστά απαραίτητη την κωδικοποίηση των δεδομένων για μεγαλύτερη ασφάλεια. Πρέπει να αναφερθεί πως η υπηρεσία του public cloud αντιμετωπίζεται με εμπιστοσύνη από τους συνδρομητές τέτοιων υπηρεσιών.

1.4.4. Hybrid cloud. Η cloud υποδομή είναι μια σύνθεση από ένα η περισσότερα clouds (private, community, or public) οι οποίοι είναι ξεχωριστές οντότητες και επιτρέπουν την μεταφορά τόσο των δεδομένων όσο και των εφαρμογών (e.g., cloud bursting for load-balancing between clouds).

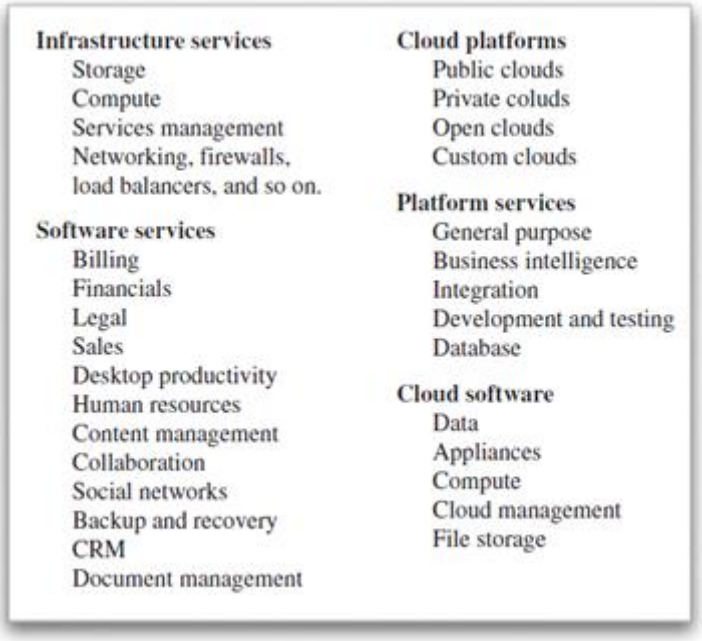


Σχήμα 1. 11 Παράδειγμα.

Στη παραπάνω εικόνα μπορούμε με να δείξουμε δυο παραδείγματα πως ένας οργανισμός μπορεί να εκμεταλλευτεί τις δυνατότητές του ιδιωτικού του cloud

και να επεκτείνει τις δυνατότητές του κοινού cloud έτσι ώστε να δημιουργήσει ένα υβριδικό μοντέλο. Τα υβριδικά σύννεφα είναι ότι ακριβώς περιγράφει το όνομά τους. Τα σύννεφα αυτά διαμορφώνονται από τους οργανισμούς όταν δημιουργούν ιδιωτικά σύννεφα, και θέλουν οι κοινότητες τους να έχουν διασύνδεση με τα δημόσια σύννεφά τους για συγκεκριμένους σκοπούς. Η διασύνδεση του ιδιωτικού με το δημόσιο σύννεφο για την εξυπηρέτηση συγκεκριμένων σκοπών δημιουργεί το υβριδικό σύννεφο. Πραγματικά ένα υβριδικό cloud μπορεί να δημιουργηθεί από τη σύνδεση τριών cloud, ένα δημόσιο, ένα ιδιωτικό και ένα community. Πολλοί οργανισμοί επεκτείνουν το εσωτερικό ιδιωτικό τους cloud για την κρίσιμη υποδομή τους και ικανοποιούν ανάγκες που δεν είναι οικονομικές για να δημιουργηθούν εσωτερικά.

Ένα κοινό παράδειγμα θα ήταν για τον έλεγχο της εξασφάλισης της ποιότητας της υπηρεσίας. Για την παράδειγμα ένα εσωτερικό σύννεφο μπορεί να χρησιμοποιηθεί για να εκτελεί την υποδομή μιας επιχείρησης, ενώ η επιχείρηση μπορεί να έχει την ανάγκη να δοκιμάσει μια αναβάθμιση. Μπορεί να γίνει συμφέρον να πληρώνει μια επιχείρηση για τη χωρητικότητα ενός κοινού cloud, για λίγους μήνες και όταν ολοκληρωθεί η αναβάθμιση του δικούς ιδιωτικού σύννεφου, να σταματήσει τη χρήση του κοινού σύννεφου.



Σχήμα 1. 12 Κατηγορίες προσφορών κάθε τύπου υπηρεσίας.

Healthcare applications using cloud computing

Υπάρχουν αρκετά παραδείγματα από εφαρμογές που παρέχουν cloud capabilities στον τομέα της υγείας. Ο τομέας της υγείας είναι αρκετά ευαίσθητος τομέας ειδικά ώς προς την διαχείριση και ασφάλεια των δεδομένων. Για αυτό το λόγο η μεταφορά και διαχείριση των δεδομένων στο Internet και ειδικότερα σε ένα cloud σύστημα θα πρέπει να πληροί βασικές προϋποθέσεις (καθορισμένες από τον οργανισμό HIPAA).

Παρακάτω παρουσιάζονται cloud εφαρμογές στην υγεία που έχουν αναπτυχθεί και είναι συμβατές με της οδηγίες της HIPAA.

DiskAgent (https://www.diskagent.com/)

Η diskagent είναι μια υπηρεσία cloud, η οποία παρέχει την δυνατότητα σε οργανισμούς υγείας να αποθηκεύουν τα δεδομένα τους συνεχώς, τους προστατεύει από απώλεια δεδομένων ακόμα και στην περίπτωση που τα δεδομένα αυτά έχουν κλαπεί. Δεν παρέχει ασφάλεια μόνο σε επίπεδο αποτυχίας υλικού, αλλά προστατεύει τα δεδομένα σε περίπτωση κλοπής χρησιμοποιώντας μια δυνατότητα απομακρυσμένης αναζήτησης και καταστροφής για τον εντοπισμό υλικού που αναζητείται και την απομακρυσμένη διαγραφή των ευαίσθητων δεδομένων. Η συγκεκριμένη εφαρμογή χρησιμοποιεί την υπηρεσία (Amazon S3), έτσι ώστε τα δεδομένα του χρήστη να αποθηκεύονται σε πολλά και απομακρυσμένα κέντρα δεδομένων.

TC3 ((Total Claims Capture & Control) Health

Η συγκεκριμένη εφαρμογή παρέχει ένα μεγάλο εύρος από υπηρεσίες κυρίως ανάλυσης δεδομένων και μείωσης κόστους σε οργανισμούς υγείας. Χρησιμοποιεί τις υπηρεσίες Amazon EC2, S3 και SQS έτσι ώστε να αυξάνει και να μειώνει την υπολογιστική ικανότητα που διαθέτει ώστε να ικανοποιείται το συμβόλαιο (SLA) με τους εκάστοτε χρήστες/πελάτες. Ανάλογα με τις εκάστοτε απαιτήσεις που έχει η TC3 κάνει χρήση των πόρων του AWS on-demand, χωρίς καθυστερήσεις και χρονοβόρες διαδικασίες και με πολύ μικρότερο κόστος αφού χρησιμοποιεί πόρους από το cloud μόνο όταν τις χρειάζεται.

MedCommons

Η εταιρεία MedCommon είναι παρέχει υπηρεσίες ηλεκτρονικού ιατρικού φακέλου δίνονται στους χρήστες άμεση πρόσβαση στο ιατρικό ιστορικό τους, ενώ παρέχει την μεταφορά αυτής της πληροφορίας με γρήγορο και ασφαλή

τρόπο σους παροχείς υγείας Ουσιαστικά χρησιμοποιεί την υπηρεσία Amazon S3, EC2 and Elastic IP για την ασφαλή δημιουργία ενός λογαριασμού υγείας και την αποθήκευση όλου του ιατρικού ιστορικού του χρήστη. Χρησιμοποιώντας το λογαριασμό αυτό ο χρήστης μπορεί να ανεβάσει δεδομένα όπως PDF files, DICOM imaging, CCR information, και άλλα σχετικά ιατρικά στοιχεία.

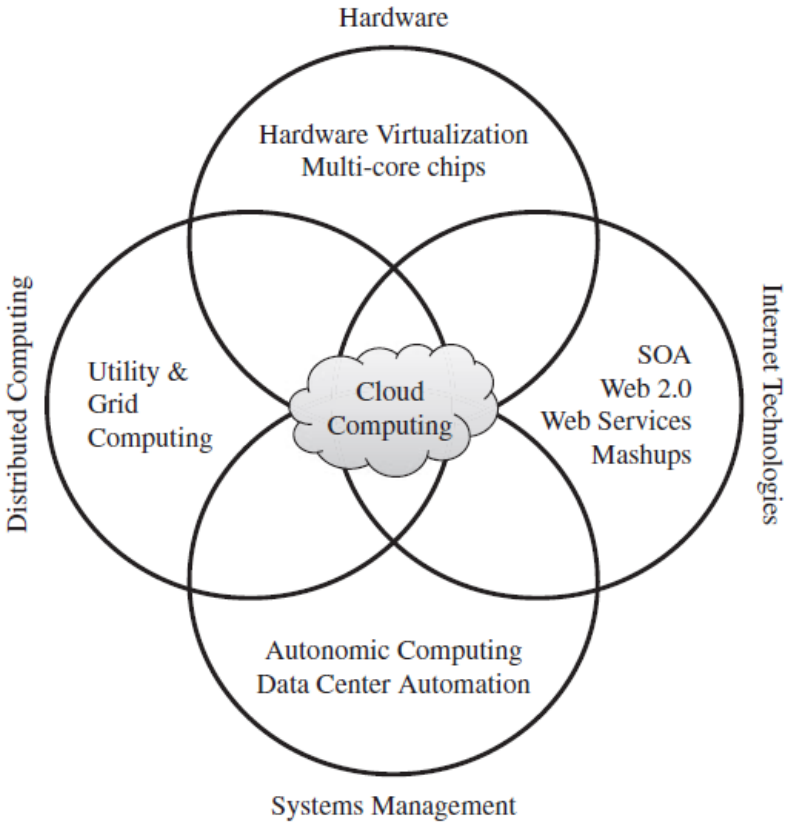
Διαχείριση των Δεδομένων στο Cloud ή Grid

Η διαχείριση των δεδομένων (αποθήκευση ανάκτηση, απόκτηση) μέσα σε ένα cloud ή grid γίνεται με διαφορετικούς τρόπους ανάλογα την χρήση και τις απαιτήσεις των δεδομένων. Σε πολύ χαμηλό επίπεδο γίνεται η χρήση των συμβατικών τρόπων αποθήκευσης και διαχείρισης δεδομένων, είτε με την χρήση Βάσεων Δεδομένων (RDMS) και αρχειακών (File Based) συστημάτων είτε με την χρήση καινούριων τεχνολογιών όπως Persistent Clouds, MapReduce (για την διαχείριση μεγάλου μεγέθους δεδομένων). Σημαντικό ρόλο στην διαχείριση των δεδομένων αλλά και των εφαρμογών, έχει η χρήση μεταδεδομένων (MetaData). Κατά την διαχείριση μεγάλου μεγέθους δεδομένων με διαφορετικές απαιτήσεις (security, integrity, importance), η χρήση μεταδεδομένων είναι ο πιο ασφαλής και ευέλικτος τρόπος αν «επεξηγήσει» τις απαιτήσεις των δεδομένων με τέτοιο τρόπο ώστε οι υπηρεσίες δεδομένων στα πιο κάτω επίπεδα να είναι σε θέση να διαφοροποιήσουν τα δεδομένα με τέτοιο τρόπο ώστε να ικανοποιούνται οι απαιτήσεις αυτών. Η χρήση των Service Oriented Architectures (SOA) τεχνολογιών στα συστήματα cloud είναι αρκετά διαδεδομένη τόσο για την διαχείριση των εφαρμογών όσο και για την διαχείριση των δεδομένων. Πιο συγκεκριμένα η χρήση των web services είναι αρκετά διαδεδομένη για την διαχείριση τόσο των δεδομένων ενός IaaS cloud αλλά και για την διαχείριση εφαρμογών SaaS cloud.Στα πλαίσια της συγκεκριμένης ΕΕ θα μελετηθούν όλες οι δυνατές τεχνολογίες διαχείρισης των ιατρικών δεδομένων (αποθήκευση ανάκτηση, απόκτηση) μέσα σε ένα cloud και θα φτιαχτεί πλατφόρμα (portal) για την υλοποίηση τους σε υπάρχουσες υποδομές cloud ή grid (πχ. Amazon, Hellas Grid).

Παραδοτέα

Π1 Αναφορά και Αξιολόγηση των διαθέσιμων τεχνολογιών διαχείρισης των ιατρικών δεδομένων (αποθήκευση ανάκτηση, απόκτηση) μέσα σε ένα cloud ή grid.

Π2. Ανάπτυξη Πλατφόρμα; (portal) για την υλοποίηση τους σε υπάρχουσες υποδομές cloud ή grid (πχ. Amazon, Hellas Grid).



Σχήμα 1. 13 Σύγκλιση των διαφόρων προκαταβολών που οδηγούν στην εμφάνιση νέφους υπολογιστών

Κεφάλαιο 2.

Φορείς Cloud Computing

Εισαγωγή

Με το ξεκίνημα της υπηρεσίας Cloud Computing, υπήρξε η ανάγκη στήριξης της και παροχής της υπηρεσίας από διάφορους φορείς. Η Amazon, η Google και η Microsoft είναι από τους πιο σημαντικούς παρόχους υπηρεσιών cloud. Όπως όμως συμβαίνει και με το λογισμικό, έτσι και στην υπηρεσία cloud, υπάρχουν εφαρμογές Open Source, οι οποίες βασίζονται σε συγκεκριμένη πλατφορμα, και διευκολύνουν τον χρήστη να προσαρμόσει τις ανάγκες του στα μέτρα του. Η open source πλατφορμα έχει την ευελιξία ότι μπορεί να προσαρμοστεί από τον χρήστη τον ίδιο και δεν υπάρχει σε προτυποποιημένη μορφή. Θα γνωρίσουμε την αρχιτεκτονική και τον τρόπο λειτουργίας αυτών των υπηρεσιών.

2.1 Amazon S3 (Simple Storage Service)

Η Υπηρεσία Amazon S3 είναι μια online διαδικτυακή υπηρεσία αποθήκευσης δεδομένων που προσφέρεται από την Amazon Web Services. Το Amazon S3 παρέχει αποθήκευση δεδομένων μέσα από μια απλή διαδικτυακή διεπαφή (interface). Η Amazon προώθησε το S3, την πρώτη ευρέως διαθέσιμη διαδικτυακή εφαρμογή στις Ηνωμένες πολιτείες το Μάρτιο του 2006, και στην Ευρώπη το Νοέμβριο του 2007. Ξεκίνησε χρέωνοντας τους χρήστες ανάλογα με το χωρητικότητα που αποθήκευαν αλλά και ανάλογα με το εύρος ζώνης που χρησιμοποιούσαν για κατέβασμα αλλά και για ανέβασμα πληροφορίας. Αυτή τη στιγμή το S3 δίνει κάθε μήνα 99,9% ποσοστό εγγύησης για την υπηρεσία που διαθέτει.

Ο σχεδιασμός του Amazon S3 είναι τέτοιος ώστε να προσφέρει, διαβάθμιση, υψηλή διαθεσιμότητα και χαμηλό κόστος καθυστέρησης αλλά και τιμής. Το S3 αποθηκεύει αυθαίρετα αντικείμενα μεγέθους 5 TB (terabytes), ακολουθούμενα από 2 KB μεταδεδομένων. Αυτά τα αντικείμενα οργανώνονται σε μεγάλες ποσότητες που η κάθε μία ανήκει στην Amazon Web Services, και αναγνωρίζονται από ένα μοναδικό κλειδί που έχει εκχωρηθεί από τον κάθε χρήστη. Τα ονόματα των μεγάλων ποσοτήτων (buckets) καθώς και των κλειδιών έχουν επιλεχθεί έτσι ώστε τα αντικείμενα να έχουν διευθυνσιοδοτηθεί και να μπορούν να εντοπιστούν χρησιμοποιώντας τις παρακάτω HTTP διευθύνσεις (links):

i. http://s3.amazonaws.com/bucket/key
ii. http://bucket.s3.amazonaws.com/key

iii. http://bucket/key (where bucket is a DNS CNAME record pointing tobucket.s3.amazonaws.com)

2.2 Google App Engine

Σχήμα 2. 1 Λογότυπο Google App Engine

Η Google App Engine χρησιμοποιεί επίσης το ακρονύμιο GAE και είναι μια πλατφόρμα για ανάπτυξη και φιλοξενία διαδικτυακών εφαρμογών σε κέντρα δεδομένων που τα διαχειρίζεται η Google. Είναι μια τεχνολογία υπολογιστικού νέφους (cloud computing). Εξομοιώνει εφαρμογές ανάμεσα σε πολλαπλούς διακομιστές και κέντρα δεδομένων. Άλλες εφαρμογές υπολογιστικού νέφους περιλαμβάνουν παροχές όπως τις Amazon Web Services & Microsoft's Azure Services Platform. Η διαφορά με του Google App Engine είναι ότι το AWS είναι IaaS ενώ το App Engine είναι PaaS. Η Google App Engine είναι δωρεάν μέχρι ενός συγκεκριμένου σημείου χρησιμοποιούμενων πηγών. Εξτρά χρεώσεις υπάρχουν για επιπλέον χρήση αποθηκευτικού χώρου, εύρος ζώνης που χρησιμοποιήθηκε, ή επιπλέον ανάγκη υπολογιστικής ισχύος που απαιτήθηκε από την εφαρμογή.

Αυτή τη στιγμή οι γλώσσες προγραμματισμού που μπορούν να υποστηριχθούν είναι Java, Python αλλά και προεκτάσεις τους όπως άλλες JVM γλώσσες όπως Groovy, JRuby, Scala, Clojure,Jython, και ειδικές εκδόσεις του Quercus.

Ορισμένοι περιορισμοί που υπάρχουν είναι ότι οι προγραμματιστές έχουν πρόσβαση μόνο για ανάγνωση στα αρχεία συστήματος του App Engine. Η εφαρμογή μας μπορεί να χρησιμοποιήσει μόνο εικονικά αρχεία συστήματος. Ακόμα το App Engine μπορεί να εκτελέσει κώδικα που καλείται από HTTP αίτηση. Οι χρήστες πρέπει να πούμε πως μπορούν να ανεβάσουν Python modules, μόνο αν είναι αμιγώς Python. Αν είναι C ή Pyrex, δεν υποστηρίζονται. Οι εφαρμογές Java δεν μπορούν να δημιουργήσουν νέα μηνύματα και μπορούν να χρησιμοποιούν μόνο μια υποκατηγορία από τις κλάσεις από την JRE κλασική έκδοση. Τα πρωτόκολλα SSL/HTTPS είναι διαθέσιμα μέσω *.appspot.com domains και όχι μέσω των Google Apps Domains.

Κάποιες σημαντικές διαφορές συγκρίνοντας την με άλλες κλιμακούμενες υπηρεσίες φιλοξενίας όπως η Amazon EC2, είναι ότι η App Engine παρέχει περισσότερες υποδομές για να γίνει εύκολο να δημιουργηθούν κλιμακούμενες εφαρμογές, οι οποίες βέβαια μπορούν να εκτελέσουν περιορισμένου εύρους εφαρμογές που σχεδιάστηκαν για αυτές τις υποδομές. Ακόμα ενώ άλλες υπηρεσίες αφήνουν τους χρήστες να εγκαταστήσουν και να ρυθμίσουν σχεδόν

κάθε *NIX συμβατό λογισμικό, η App Engine απαιτεί από τους προγραμματιστές να χρησιμοποιούν μόνο τις υποστηριζόμενες γλώσσες, APIs και πλαίσια (frameworks). Τα τρέχοντα APIs επιτρέπουν αποθήκευση αλλά και ανάκτηση δεδομένων από ένα μεγάλο πίνακα μη σχετικών βάσεων δεδομένων, ώστε να μπορούν να κάνουν HTTP αιτήσεις, να στέλνουν e-mail αλλά και να κάνουν προσωρινή αποθήκευση δεδομένων (caching). Οι περισσότερες υπάρχουσες διαδικτυακές εφαρμογές δεν μπορούν να τρέξουν στο App Engine χωρίς τροποποίηση γιατί απαιτούν μια σχετική βάση δεδομένων.

2.3 Windows Azure

Σχήμα 2. 2 Λογότυπο Windows Azure

Η υπηρεσία Windows Azure Platform είναι μια πλατφόρμα υπολογιστικού νέφους που προσφέρεται από τη Microsoft, και επιτρέπει στους χρήστες της να αναπτύσσουν εφαρμογές αλλά και δεδομένα μέσα στο σύννεφο (cloud). Έτσι η Windows Azure Platform ταξινομείται ως PaaS. Η πλατφόρμα αποτελείται από διάφορες υπηρεσίες κατά παραγγελία που φιλοξενούνται σε βάσεις δεδομένων της Microsoft και εμπορευματοποιούνται μέσω τριών εμπορικών πακέτων. Αυτά είναι τα Windows Azure (ένα λειτουργικό σύστημα που παρέχει κλιμακούμενες υπολογιστικές και αποθηκευτικές ευκολίες), το SQL Azure (μια βασισμένη σε νέφος έκδοση του SQL server), και την Windows Azure AppFabric (μια συλλογή από υπηρεσίες που υποστηρίζουν εφαρμογές και στο νέφος αλλά και στις προϋποθέσεις).

Η Windows Azure Platform είναι μια πλατφόρμα εφαρμογών (application platform) στο νέφος που επιτρέπει στα κέντρα δεδομένων (datacenters) της Microsoft, να υποδέχονται αλλά και να τρέχουν εφαρμογές. Παρέχει ένα λειτουργικό σύστημα νέφους που καλείται Windows Azure που εξυπηρετεί ως runtime για τις εφαρμογές και παρέχει ένα σύνολο από εφαρμογές που επιτρέπουν ανάπτυξη, διαχείριση και φιλοξενία εφαρμογών.

Η Windows Azure έχει τρία βασικά στοιχεία: υπολογισμούς, αποθήκευση και Fabric.

Η πλατφόρμα περιλαμβάνει πέντε υπηρεσίες : Live Services, SQL Azure (πρώην SQLServices), AppFabric (πρώην NET Services.), SharePoint Services και Dynamics CRMυπηρεσίες - τις οποίες οι προγραμματιστές μπορούν να χρησιμοποιήσουν για να χτίσουν τις εφαρμογές που θα τρέχουν στο σύννεφο . Μια βιβλιοθήκη client, σε διαχειριζόμενο κώδικα, αλλά και συναφή εργαλεία παρέχονται για την ανάπτυξη εφαρμογών νέφους σε Visual Studio. Η Κλιμάκωση και η αξιοπιστία ελέγχονται από τον ελεγκτή Windows Azure Fabric, ώστε οι υπηρεσίες και το περιβάλλον να μην διαλύσουν, αν κάποιος από τους εξυπηρετητές σταματήσει να λειτουργεί μέσα στα κέντρα δεδομένων της Microsoft και παρέχει διαχείριση των διαδικτυακών εφαρμογών όπως πόρους μνήμης και διαχείριση φορτίου δεδομένων.

2.4 Eucalyptus

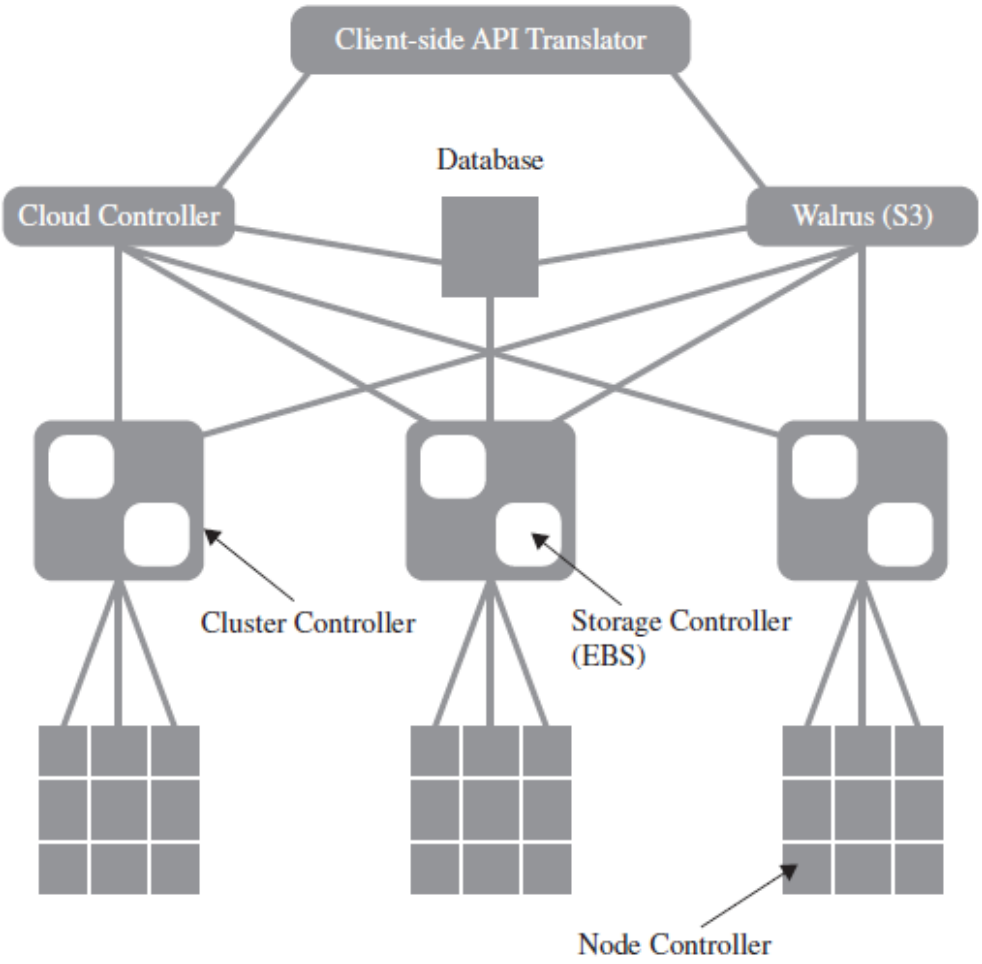
Σχήμα 2. 3 Λογότυπο Eucalyptous

Το Eucalyptus ήταν μία από τις πρώτες open source εφαρμογές που επικεντρώθηκε στην δημιουργία των IaaS σύννεφων. Δημιουργήθηκε έτσι ώστε να παρέχει μια εφαρμογή ανοιχτού κώδικα (open source) όμοια σε λειτουργία όπως το Amazon Web Services API. Έτσι οι χρήστες μπορούν να αλληλεπιδρούν με το eucalyptus cloud χρησιμοποιώντας τα ίδια εργαλεία που χρησιμοποιούν ώστε να έχουν πρόσβαση στο Amazon EC2. Επιπλέον όμως, παρέχεται ένα σύννεφο αποθήκευσης API για την αποθήκευση των γενικών δεδομένων των χρηστών και VM εικόνων. Ανακεφαλαιώνοντας το Eucalyptus παρέχει τα ακόλουθα :

- Linux-based controller
- EC2-compatible (SOAP, Query) , S3-compatible (SOAP, REST) CLI και Web portal interfaces
- Xen, KVM, και VMWare backends
- Amazon EBS-compatible virtual storage devices
- Interface to the Amazon EC2 public cloud
- Εικονικά δίκτυα, virtual networks.

2.4.1. Αρχιτεκτονική Eucalyptus.

Η αρχιτεκτονική του Eucalyptous όπως φαίνεται στο παρακάτω σχήμα, αποτελεί συστατικό στοιχείο κάθε συστήματος σε υψηλό επίπεδο ως αυτόνομη υπηρεσία Web με τα ακόλουθα στοιχεία υψηλού ελέγχου.



Σχήμα 2. 4 Αρχιτεκτονική υψηλού επιπέδου του Eucalyptous.

Node controller (NC): Ελέγχει την εκτέλεση, επιθεώρηση και τον τερματισμό των περιπτώσεων (VM) εικονικών μηχανών στον χώρο που φιλοξενούνται και εκτελούνται.
Cluster controller (CC): Συλλέγουν πληροφορίες σχετικά με τις εκτελέσεις των (VM) αλλά και τις προγραμματίζουν σε συγκεκριμένους node controllers (NC), τόσο καλά όσο διαχειρίζονται τις περιπτώσεις εικονικών δικτύων.
Storage controller (SC): Είναι μια υπηρεσία λήψης/αποθήκευσης που εφαρμόζει τη διεπαφή του Amazon's S3 και παρέχει τον τρόπο αποθήκευσης και πρόσβασης της πληροφορίας που έχει χρησιμοποιηθεί από το χρήστη.

Cloud controller (CLC): Είναι το σημείο εισόδου για το cloud για απλούς χρήστες και διαχειριστές. Θέτει ερωτήματα στους διαχειριστές κόμβων για πληροφορίες και πόρους, παίρνει αποφάσεις προγραμματισμού ενεργειών υψηλού επιπέδου, και εφαρμόζει όλα αυτά κάνοντας αιτήματα (requests) στους ελεγκτές συμπλεγμάτων (cluster controllers).
Walrus (W): Είναι το εξάρτημα του ελεγκτή που διαχειρίζεται την πρόσβαση στις υπηρεσίες αποθήκευσης μέσα στον Eucalyptous. Τα αιτήματα αποστέλλονται στον Walrus χρησιμοποιώντας τις διεπαφές SOAP ή REST.

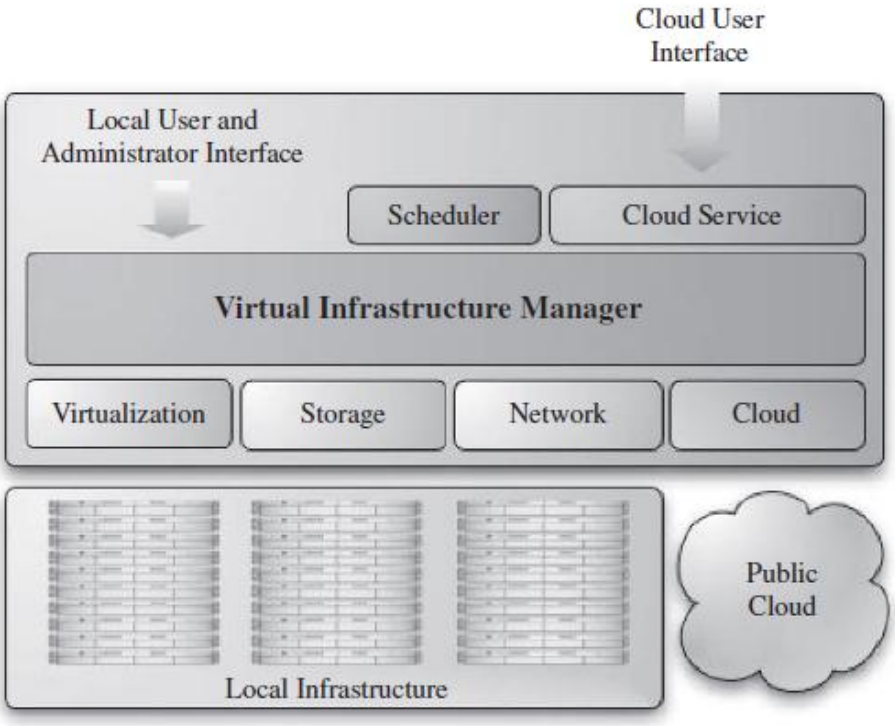
2.5 Open Nebula

Το Open Nebula είναι μία από τις πιο πλούσιες open source εφαρμογές. Αρχικά είχε σχεδιαστεί για την διαχείριση εικονικών υποδομών και περιλάμβανε απομακρυσμένες διεπαφές που καθιστούσαν υλοποιήσιμη την κατασκευή των public σύννεφων. Συνολικά, τέσσερις APIs είναι διαθέσιμες :

- XML-RPC
- Libvirt
- EC2 (Query) APIs
- OpenNebula Cloud API (OCA)

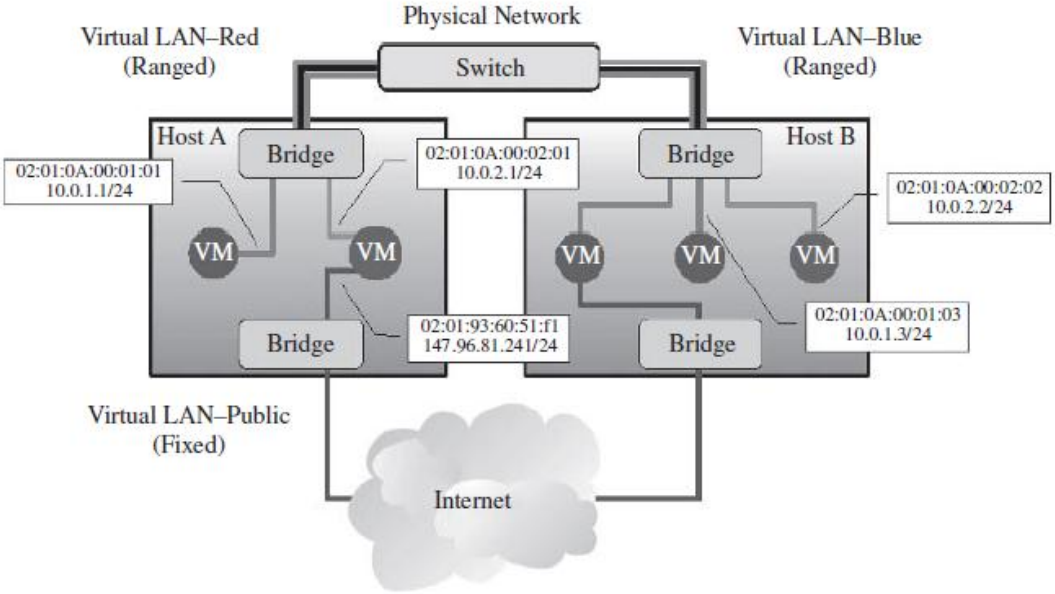
Η αρχιτεκτονική του περιλαμβάνει διάφορα εξειδικευμένα συστατικά. Η κύρια ενότητα της αρχιτεκτονικής του περιλαμβάνει φυσικούς διακομιστές και τους hypervisors τους ,τους κόμβους αποθήκευσης και τα network fabric. Η διαχείριση των εργασιών εκτελούνται από οδηγούς που αλληλεπιδρούν με τα API των hypervisors, με τις συσκευές αποθήκευσης και τις τεχνολογίες δικτύων των δημόσιων σύννεφων. Ανακεφαλαιώνοντας το open Nebula ακόλουθες δυνατότητες (με βάση το Linux ελεγκτή):

- CLI, XML-RPC, EC2-compatible Query και OCA interfaces
- Xen, KVM, και VMware backend
- interface to public clouds (Amazon EC2, ElasticHosts)
- virtual networks
- dynamic resource allocation
- advance reservation of capacity.



Σχήμα 2. 5 Αρχιτεκτονική υψηλού επιπέδου Open Nebula

Δικτύωση: Γενικά, υπηρεσίες που αναπτύσσονται στο σύννεφο, από μια συστοιχία υπολογιστών (computing cluster) προς την κλασική three-tier επαγγελματική εφαρμογή, απαιτεί πολλαπλά αλληλένδετα εικονικά μηχανήματα (VM), με ένα εικονικό δίκτυο εφαρμογών (VAN) να είναι ο συνδετικός κρίκος μεταξύ τους. Ο OpenNebula δυναμικά δημιουργεί αυτά τα εικονικά δίκτυα εφαρμογών (VAN's) και ακολουθεί τις MAC διευθύνσεις που χρησιμοποιήθηκαν στο δίκτυο για τις υπηρεσίες των (VM's). Πρέπει να σημειώσουμε ότι αναφερόμαστε σε τοπικά δίκτυα layer 2. Άλλες υπηρεσίες TCP/IP, όπως DNS, NIS ή NFS είναι ευθύνη της υπηρεσίας.



Σχήμα 2. 6 Μοντέλο δικτύου για Open Nebula

2.6 Απαιτήσεις.

Προκειμένου να επιτευχθούν οι στόχοι που έχουν τεθεί και αξιοποιώντας την προηγούμενη εμπειρία η Yahoo! θέτει μια σειρά από απαιτήσεις οι οποίες περιγράφονται παρακάτω.

2.6.1 Multitenancy: οι υπηρεσίες που παρέχει το cloud πρέπει να υποστηρίζουν διαφορετικές εφαρμογές. Οι εφαρμογές μπορούν να διαμοιράζονται πληροφορίες αλλά εκτελούνται απομονωμένα. Τέλος η ανάπτυξη μιας νέας εφαρμογής θα πρέπει να απαιτεί μικρή προσπάθεια.

2.6.2 Elasticity: Η εφαρμογές πρέπει να είναι σε θέση να διαπραγματεύονται και να λαμβάνουν επιπλέον πόρου προκειμένου να καλύπτουν τις διαρκώς αυξανόμενες ανάγκες τους σε υπολογιστική ισχύ και αποθηκευτική δυνατότητα

2.6.3 Scalability: Το σύστημα πρέπει να ανακατανέμει τα δεδομένα σε περίπτωσης εισαγωγής νέου υλικού.

2.6.4 Load and Tenant Balancing: Δυνατότητα μεταφοράς φορτίου ανάμεσα στους εξυπηρετητές για να αποφευχθεί υπερφόρτωση. Δηλαδή σε περίπτωση που για κάποιον λόγο προκύψει πολλαπλασιασμός του φορτίου σε κάποια εφαρμογή θα πρέπει με κάποιον τρόπο να υποστηριχθεί αυτό το νέο φορτίο.

2.6.5 Availability: Το σύστημα πρέπει να συνεχίζει την λειτουργία του ακόμα και σε περίπτωση υψηλών ποσοστών αποτυχίας. Δηλαδή σε περίπτωση αποτυχίας εξυπερετητών ή δικτύων οι υπηρεσίες του cloud πρέπει να παραμένουν ανεπηρέαστες και να παρέχονται χωρίς κανένα πρόβλημα.

Security: Κρίσιμο σημείο γιατί παραβίαση της ασφάλειας του συστήματος θα προκαλέσει πρόβλημα και στις εφαρμογές.

Operability: Λειτουργικότητα συστημάτων και διασυνδέσεων των συστημάτων του cloud. Για πιο εύκολη διαχείριση.

Metering: Παρακολούθηση της χρησιμοποίηση των πόρων από της εφαρμογές για λήψη αποφάσεων και υπολογισμό κόστους.

Global: Τοποθέτηση των υπηρεσιών «κοντά» στον χρήστη για μείωση καθυστερήσεων.

Simple API's: Διευκόλυνση της ανάπτυξης των εφαρμογών που χρησιμοποιούν το cloud.

Costs/Economic Metrics	Status Quo: 1,000 Server (Non-Virtualized) Environment	Scenario 1: Public Cloud	Scenario 2: Hybrid Cloud	Scenario 3: Private Cloud
Investment Phase Costs FY10–12 (BY09 M$)	$0	$3.0	$6.1	$7.0
O&S Phase Costs FY10–22 (BY09 M$)	$77.3	$22.5	$28.9	$31.1
Total LCCs (BY09 M$)	$77.3	$25.5	$35.0	$38.1
Economic Metrics:				
NPV (BY09 M$)	N/A	$41.8	$33.7	$31.1
BCR	N/A	15.4	6.8	5.7
DPP (Years)	N/A	2.7	3.5	3.7

Σχήμα 2. 7 Κόστος Cloud σε σχέση με τα συμβατικά μοντέλα.

2.7 Κέρδη όταν μια εφαρμογή έχει δημιουργηθεί για να λειτουργεί στο cloud.

Κέρδος	Περιγραφή
Πρόσβαση από παντού	Οι διαδυκτιακές εφαρμογές παρέχουν τη δυνατότητα πρόσβασης της εφαρμογής από οποιοδήποτε σημείο, χωρίς την εγκατάσταση λογισμικού VPN. Η τοποθέτηση ενός web front end στην υπάρχουσα εφαρμογή παρέχει περιορισμένη πρόσβαση χειρισμού από οπουδήποτε.
Ενοποιημένες εφαρμογές	Οι σύγχρονες cloud εφαρμογές επιτρέπουν σε επιχειρήσεις με διεσπαρμένα γραφεία να ενοποιήσουν λειτουργίες και να γλυτώσουν χρήματα ελαχιστοποιώντας πολλαπλά συστήματα και διαδικασίες διαχείρισης
Χαμηλότερο κόστος συντήρησης	Οι διαδυκτιακές εφαρμογές εξασφαλίζουν κέρδος χρημάτων στις επιχειρήσεις ελαχιστοποιώντας τα κόστη από εγκατάσταση client εφαρμογών αλλά και συντηρήσεων των εφαρμογών αυτών.
Κινητές (mobile) εφαρμογές	Οι μηχανικοί εφαρμογών για το cloud, προβλέπουν τη χρήση τους και από φορητές συσκευές, διότι το cloud είναι παντού όπως και οι φορητές συσκευές. Η εύκολη πρόσβαση στο διαδύκτιο μέσω φορητών συσκευών (Wi-Fi, 3G) καθιστά την πρόσβαση στις εφαρμογές απαραίτητη.
Μείωση κίνησης πακέτων δικτύου.	Η χρήση μιας πεπαλαιωμένης εφαρμογής στο cloud μπορεί να δημιουργήσει μεγάλη κίνηση σε ένα δίκτυο. Όλες οι παλιές εφαρμογές έχουν χτιστεί για να λειτουργούν σε τοπικό δίκτυο ενώ οι cloud εφαρμογές για να λειτουργούν στο διαδύκτιο. Όσο εμπλέκονται στην εφαρμογή περισσότεροι άνθρωποι που θα έχουν πρόσβαση από διάφορα μέρη, οι εφαρμογές cloud θα υπερτερούν έναντι των εφαρμογών που έχουν φτιαχτεί για τοπικό δίκτυο και λειτουργούν στο cloud.

Κεφάλαιο 3

Ψηφιακές υπηρεσίες υγείας στο Cloud

Εισαγωγή

Η ανάπτυξη της τεχνολογίας του υπολογιστικού νέφους, έδειξε σημάδια πως θα μπορούσα να δημιουργηθούν οφέλη και στον τομέα της υγείας. Υπήρξε η ανάγκη θα δημιουργηθεί ένα κοινό υπόβαθρο σε κάποιους τομείς. Η εισαγωγή ενός ασθενούς σε νοσοκομείο, θα οδηγήσει σε κάποιες ιατρικές εξετάσεις και κατ'επέκταση σε κάποιες ιατρικές διαγνώσεις. Όταν ένας ασθενής λοιπόν υπάρξει σε κάποια άλλη πόλη θα ήταν ιδανικό και θεμιτό να μπορεί να υπάρχει πρόσβαση στις πληροφορίες αυτές. Ένας τρόπος με τον οποίο μπορεί να γίνεται αποθήκευση αλλά και πιθανή επεξεργασία αποτελεσμάτων είναι μέσω του cloud computing. Το δυναμικό περιβάλλον του υπολογιστικού νέφους μας δίνει τη δυνατότητα να μπορούμε να αποθηκεύουμε πληροφορίες ανάλογα με τις ανάγκες μας. Ορισμένα από τα προβλήματα που υπήρξαν βέβαια είναι η προσαρμογή σε ένα νέο περιβάλλον (όχι ορατό) και η εξικοίωση με τις νέες τεχνολογίες. Ακόμα πρέπει να πούμε πως υπάρχουν πολλές παροχημένες ιατρικές συσκευές που θα υπήρχε πρόβλημα να μπορέσουν να ενσωματωθούν στο νέο ψηφιακό περιβάλλον.

3.1 Ψηφιακές υπηρεσίες υγείας.

Η ανάπτυξη της τεχνολογίας στον τομέα της πληροφορικής και του διαδικτύου, έχει βοηθήσει στην δημιουργία νέων υπηρεσιών στον τομέα της υγείας. Μεταξύ αυτών είναι ο Ηλεκτρονικός Φάκελος ασθενούς, υπηρεσίες τηλεϊατρικής, φορετά και φορητά συστήματα παρακολούθησης ασθενών (wearable and portable monitoring systems), δικτυακές πύλες υγείας, και άλλα εργαλεία που βασίζονται σε τεχνολογίες πληροφορικής και επικοινωνιών και που επικουρούν την πρόληψη, διάγνωση, θεραπεία, παρακολούθηση της υγείας και των παραμέτρων του τρόπου ζωής.

Ο Ηλεκτρονικός φάκελος ασθενούς περιλαμβάνει προσωπικές πληροφορίες, καθώς και ιατρικές όπως ιστορικό και αποτελέσματα ιατρικών εξετάσεων. Η υπηρεσία αυτή παρέχει πληροφορίες που βρίσκονται αποθηκευμένες σε ένα σημείο, και είναι προσβάσιμες από περισσότερα σημεία.

Όλες αυτές οι ιατρικές συσκευές σε συνδυασμό με την αναπτυγμένη τεχνολογία, μας δίνουν τη δυνατότητα να μπορούν να εξυπηρετηθούν περιπτώσεις που δεν είναι δυνατή η πρόσβαση γιατρού, αδύνατη η μετακίνηση ασθενή, αλλά και πάνω από όλα η δυνατότητα του ασθενή να μπορεί να παρακολουθείται χωρίς να αλλάζει τις καθημερινές του συνήθειες και ρυθμούς. Η συνεχόμενη όμως αύξηση αναγκών να εξυπηρετηθεί μεγαλύτερο εύρος ασθενών αλλά και διαφορετικών ιατρικών περιπτώσεων,

έχει οδηγήσει σε αύξηση απαιτήσεων σε επίπεδο τεχνολογίας λογισμικού, hardware, και δικτύων.

Μια λύση που υπάρχει για να λυθούν τα συγκεκριμένα προβλήματα απαιτήσεων, είναι το τεχνολογικό περιβάλλον των υπολογιστικών νεφών (cloud computing). Η έννοια του cloud computing αποτελεί μια νέα προσέγγιση στον χώρο των κατανεμημένων συστημάτων η οποία όμως χρησιμοποιεί και κάποιες τεχνολογίες που προϋπήρχαν. Σκοπός του είναι η παροχή ως υπηρεσιών πόρων όπως, η υπολογιστική ισχύ και η αποθηκευτική δυνατότητα , στους χρήστες του συστήματος. Σχετικά με τον ορισμό της έννοιας έχουν γίνει πολλές προσπάθειες οι οποίες όμως δεν καλύπτουν όλες τις πτυχές του συστήματος με αποτέλεσμα την γενίκευση της έννοιας με τέτοιον τρόπο που cloud computing να θεωρείται κάθε σύστημα το οποίο επιτρέπει ανάθεση υπολογιστικών και αποθηκευτικών υπηρεσιών εξωτερικά

Οι επιστήμονες στις μέρες μας έχουν κατακλυστεί από την αυξανόμενη ποσότητα των πληροφοριών που απορρέουν από τις αμέτρητες πηγές που υπάρχουν σε κάθε πεδίο της επιστήμης. Παραδείγματα είναι η αναπαραγωγή του DNA,η πολυπλοκότητα του υιού HIV και του καρκίνου και άλλα πολλά .Καθώς υπάρχουν αμέτρητες πληροφορίες η προεπεξεργασία, η επεξεργασία και η ανάλυση αυτών είναι ένα πρόβλημα που απασχολεί την κοινότητα των μηχανικών. Μία από τις υποσχέσεις της τεχνολογίας cloud είναι η δυνατότητα να ενώνει υπολογιστικές πηγές για να λύσει τα επιστημονικά μυστήρια της εποχής μας. Από βιοϊατρική άποψη, η πρόκληση να ενώσουμε την «σκέψη» με τους υπολογιστές αναδύεται. Εκτός από την περιπλοκότητα του υλικού που πρέπει να ληφθεί σοβάρα υπόψη, τίθεται και το θέμα της ευαισθησίας του υλικού λόγω θέματος χρόνου και άποψης του κάθε πολίτη. Η cloud τεχνολογία προσφέρει υπολογιστικές τεχνολογίες μέσω του διαδικτύου οι οποίες μπορούν εύκολα να αγοραστούν μέσα σε λίγα λεπτά χρησιμοποιώντας μόνο μια πιστωτική κάρτα. Ειδικά στην ιατρική τα οφέλη που απορρέουν από την χρήση της cloud τεχνολογίας είναι πολλά. Σε αυτό το κεφάλαιο παρουσιάζονται οι πιθανές βιοιατρικές εφαρμογές της cloud τεχνολογίας όπως το CAP3, το caBIG, το GTM interpolation και το MDS interpolation.

3.1.1 caBIG (cancer Biomedical Informatics Grid)

Σχήμα 3. 1 Λογότυπο caBIG

Η πολυπλοκότητα του καρκίνου έχει ωθήσει τους επιστήμονες στην αναζήτηση νέων τρόπων για να συγκεντρώνουν και να αναλύουν τις πληροφορίες από διαφορετικές πηγές . Υπάρχει μία επιτακτική ανάγκη για στάνταρ εφαρμογές ,κοινά μοντέλα πληροφοριών και υποδομής λογισμικού έτσι ώστε να ενθαρρυνθεί η αποτελεσματική πρόσβαση και διανομή των κατανεμημένων υπολογιστικών πηγών στην έρευνα του καρκίνου. Η ανάγκη αυτή είναι αισθητή σε όλα τα στάδια της βιοιατρικής έρευνας. Η βασική και η κλινική μελέτη έχει ταχύτατα εξαρτηθεί από προχωρημένες τεχνολογίες πληροφοριών για την διαχείριση, την ανταλλαγή και την ανάλυση διαφορετικών βιοιατρικών πληροφοριών.

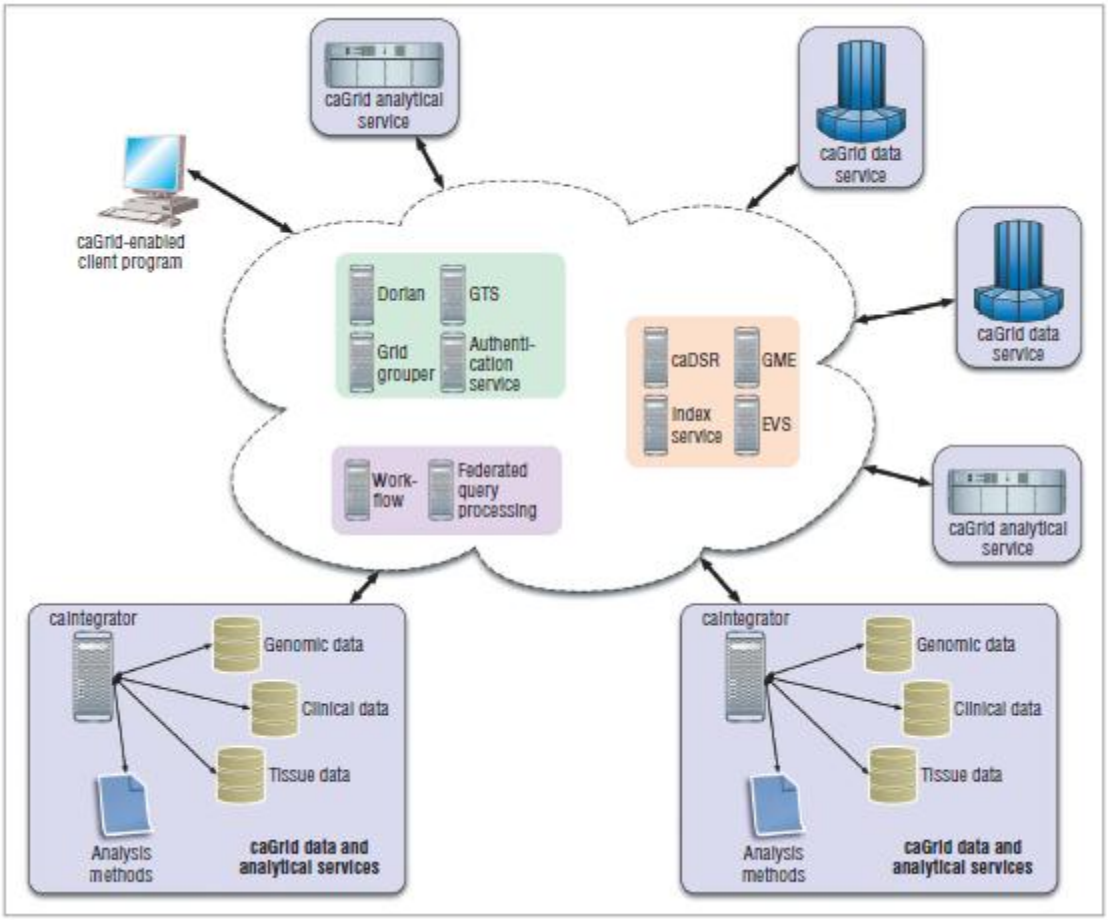
Παρόλο που η πληθώρα των πληροφοριών όσον αφορά τα θέματα καρκίνου συλλέγονται από το εθνικό ινστιτούτο καρκίνου, ο οποιοσδήποτε ερευνητής που θέλει να ασχοληθεί με τα θέματα αυτά έρχεται αντιμέτωπος με προκλήσεις που αφορούν την ανακάλυψη, την ανάκτηση και την ανάλυση των πληροφοριών σχετικές με το πεδίο έρευνάς του. Επίσης υπάρχουν πολλές πληροφορίες σε διάφορα sites που μπορούν να χρησιμοποιηθούν για την έρευνα του κάθε ερευνητή. Όμως ακόμη και οι πληροφορίες που αντιστοιχούν στην ίδια βιολογική οντότητα μπορεί να έχουν άλλες αντιπροσωπεύσεις , να έχουν άλλα ονόματα και άλλες τιμές στοιχείων. Όμοια και τα προγράμματα ανάλυσης σε διαφορετικά sites μπορεί να δέχονται διαφορετικές εισόδους, να έχουν διαφορετικές διεπάφες και να δίνουν διαφορετικές εξόδους .

Αναγνωρίζοντας την ανάγκη για αποτελεσματική διανομή των πληροφοριών και των πηγών και την έλλειψη της προχωρημένης τεχνολογίας λογισμικού το εθνικό ινστιτούτο καρκίνου ξεκίνησε το 2004 ένα διεθνούς κλίμακας πρόγραμμα γνωστό ως cancer Biomedical Informatics Grid (caBIG) . Ο στόχος αυτού του προγράμματος είναι να δημιουργήσει ένα δίκτυο ανάμεσα στα κέντρα πληροφοριών του καρκίνου και στα εργαστήρια έρευνας σε όλες τις χώρες έτσι ώστε να καταφέρει να συνδυάσει όλες τις πληροφορίες και όλες τις ειδικότητες ερευνητών. Για να επιτευχθεί αυτός ο στόχος η κοινότητα που ασχολείται με το πρόγραμμα αυτό αναπτύσσει τα στάνταρ, τις πολιτικές, τις κατευθυντήριες γραμμές, τα εργαλεία και την υποδομή υλικολογισμικού ώστε να επιτρέψει την αποτελεσματικότερη διανομή των στοιχείων. Έχει επικεντρωθεί κυρίως στο να θέσει τα στάνταρ στο μοίρασμα των

υπολογιστικών πηγών και δεδομένων έτσι ώστε να θεραπεύσει τον καρκίνο. Με αυτόν τον τρόπο αλλάζει εντελώς ο τρόπος που γίνεται η έρευνα καρκίνου, καθώς δημιουργείται ένα δίκτυο στο οποίο ολόκληρη η κοινότητα που ασχολείται με θέματα καρκίνου μπορεί να συνδεθεί ελεύθερα ανά πάσα στιγμή. Έτσι μπορούμε να μοιραστούμε πολύτιμες πληροφορίες και να σώσουμε πολύτιμο χρόνο για νέες ανακαλύψεις.

Πριν από το caBIG πρόγραμμα γινόταν μία ερευνητική προσπάθεια από το NCI Center for Bioinformatics (NCICB) έτσι ώστε να εκτιμηθεί η κατάσταση της ήδη υπάρχουσας τεχνολογίας και η διαθεσιμότητα σε εργαλεία. Τα αποτελέσματα είχαν δημοσιευτεί το 2004 στο

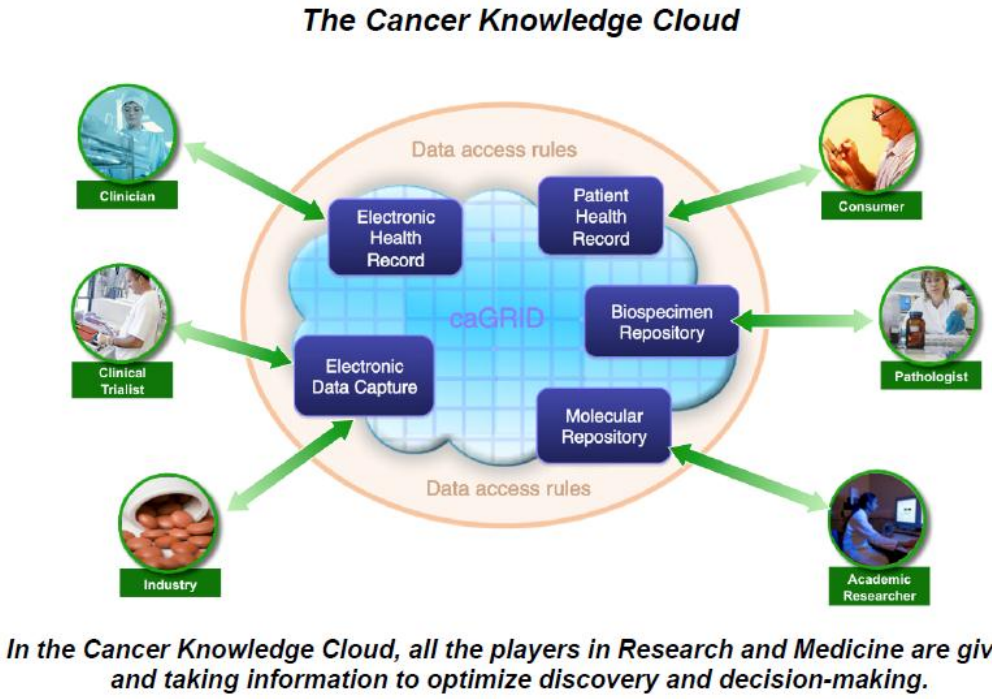
https://cabig.nci.nih.gov/guidelines_documentation/caGRIDWhitepaper.pdf



Σχήμα 3. 2 Αρχιτεκτονική caBIG

Η αρχιτεκτονική του caBIG είναι βασισμένη σε μία πλατφόρμα η οποία επιτρέπει την συνεργασία και την ανταλλαγή πληροφοριών μεταξύ 60 και άνω κέντρων καρκίνου καθώς επίσης και της κυβέρνησης αλλά και διδακτικών και ιδιωτικών ογκολογικών ινστιτούτων. Η θεμελιώδης αρχιτεκτονική είναι βασισμένη σε υπηρεσίες διαδικτύου .

Με τη χρήση της τεχνολογίας cloud το caBIG πρόγραμμα μπορεί να τελειοποιηθεί μειώνοντας δραματικά τον χρόνο της διαδικασίας ανάκτησης πληροφοριών αλλά και εφαρμογών της caBIG με τον πιο αποτελεσματικό αλλά και οικονομικό τρόπο. Οι ομάδες που θα χρησιμοποιήσουν την τεχνολογία cloud θα είναι σε θέση να μειώσουν δραστικά τις δυσχέρειες, το χρόνο, τα λάθη αλλά και τις δαπάνες της διατήρησης του υλικού και του λογισμικού στα κέντρα καρκίνου. Η χρήση των υποδομών της τεχνολογίας cloud θα παρέχει ευκολότερη είσοδο στην κοινότητα caBIG ,ιδίως για τα κέντρα καρκίνου τα οποία μπορεί να μην διαθέτουν IT πόρους για να λειτουργήσουν την υποδομή.



Σχήμα 3. 3 *Ένα παράδειγμα λειτουργίας του CaBig στο cloud*

Αρχικά οι πληροφορίες θα είναι προσβάσιμες σε όλους τους γιατρούς, ερευνητές και ερευνητικά εργαστήρια μέσω της cloud τεχνολογίας. Αυτές οι πληροφορίες μπορεί να είναι γενικές ή να είναι συγκεκριμένες πληροφορίες σχετικές με τον καρκίνο (όπως για παράδειγμα η έρευνα του NCI η οποία

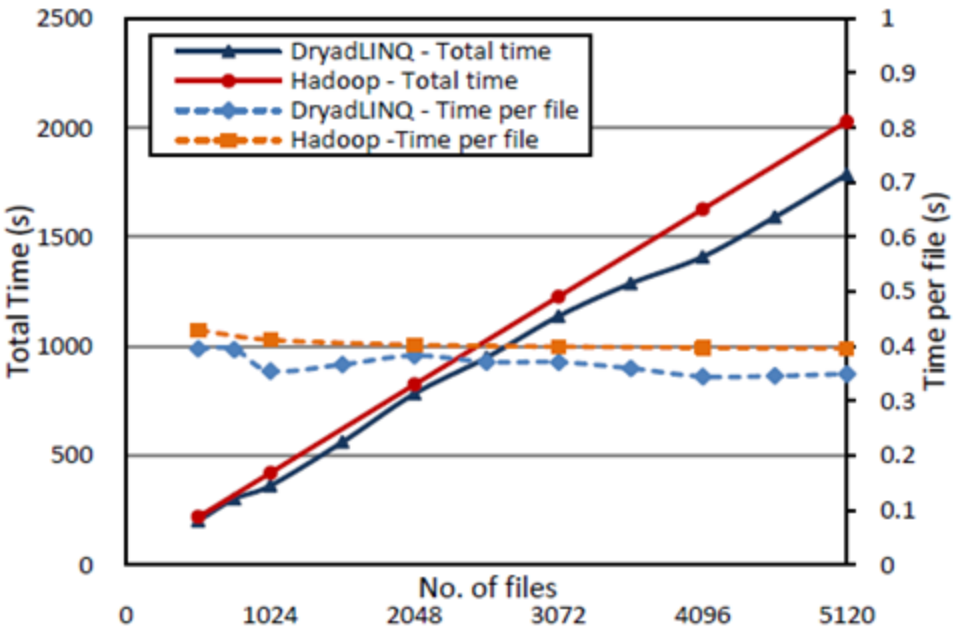
προσπαθεί να απεικονίσει ολόκληρο το γονίδιο του καρκίνου (http://cancergenome.nih.gov) έτσι ώστε να γίνει κατανοητός ο παιδικός καρκίνος (http://target.cancer.gov)). Όλες αυτές οι πληροφορίες οι οποίες θα βρίσκονται στο cloud θα είναι κατανοητές και από τα μηχανήματα αλλά και από τους χρήστες χάρη στις σημασιολογικές υπηρεσίες υποδομής του NCI το οποίο παρέχει κάποιου τύπου ταυτόχρονης μετάφρασης για παγκόσμια επικοινωνία.

Ύστερα , καθώς το περιεχόμενο των πληροφοριών μέσα στο cloud θα εμπλουτίζεται, οι πληροφορίες αυτές θα μπορούν να χρησιμοποιηθούν στην έρευνα καθώς και σε κλινικές ερωτήσεις υγείας. Για παράδειγμα εξουσιοδοτημένοι ερευνητές θα μπορούν να αναλύουν όλες τις πληροφορίες (χρησιμοποιώντας τα εργαλεία και τις εφαρμογές του caBIG) συσχετίζοντας τις κλινικές και γονιδιακές πληροφορίες. Έτσι θα μπορούν να υποθέτουν σχέσεις (για παράδειγμα εάν το γονίδιο x συνδέεται με τον πρόωρο θάνατο από ασθένεια του γονιδίου y) και να ψάχνουν αν αυτές οι σχέσεις είναι αληθής. Θα μπορούν να συγκρίνουν τα αποτελέσματα από ασθενείς με παρόμοια συμπτώματα που τους έχουν δοθεί διαφορετικές θεραπείες και μετά να τα συγκρίνουν με γονιδιακά προφίλ για να εξακριβώσουν εάν κάποιες κατηγορίες φαρμάκων δουλεύουν καλύτερα σε κάποιες ομάδες ανθρώπων με συγκεκριμένα γονιδιακά χαρακτηριστικά.

Εκτός από τα παραπάνω, οι ασθενείς θα μπορούν να συμμετέχουν στην ροή πληροφοριών που αφορά την δική τους κλινική και γονιδιακή εικόνα . Εάν οι ασθενείς είναι σε θέση να γνωρίζουν εκ των προτέρων την προδιάθεση του οργανισμού τους στον καρκίνο ή άλλες ασθένειες ,αυτό σίγουρα θα τους ωθήσει σε ένα υγιεινότερο τρόπο ζωής.

3.1.2. *Cap3*

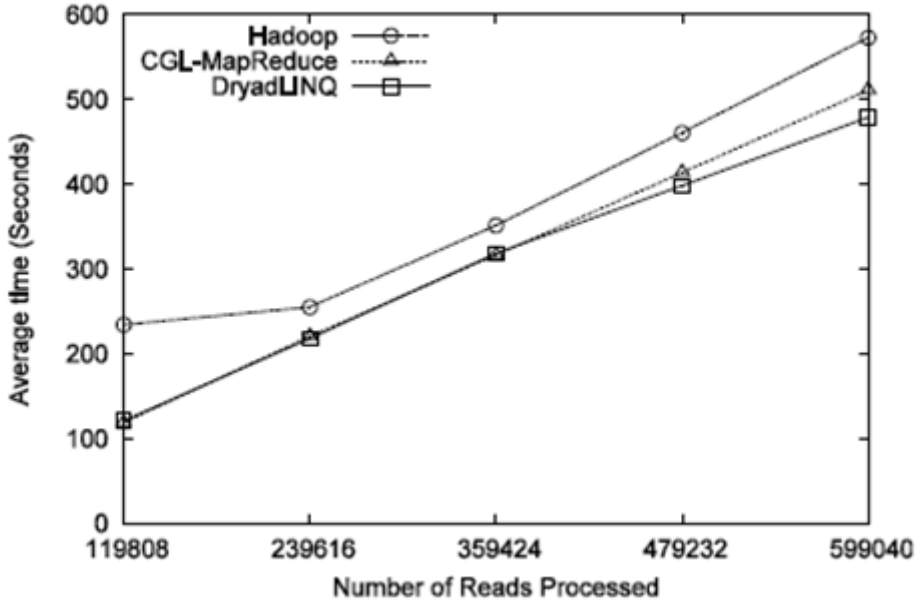
Το Cap3 είναι ένα πρόγραμμα assembly το οποίο συγκεντρώνει DNA ακολουθίες με διαδικασίες ευθυγράμμισης και συγχώνευσης από σχετικές ακολουθίες DNA. Ο CAP3 αλγόριθμος αφαιρεί τις <<φτωχές>> περιοχές των κομματιών του DNA, υπολογίζει τα κοινά σημεία μεταξύ δύο διαφορετικών κομματιών DNA, προσδιορίζει και αφαιρεί τα λανθασμένα εικονικά κοινά σημεία, ενώνει τα κομμάτια DNA και τελικά μέσα από πολλαπλές διαδικασίες στοίχισης και ευθυγράμμισης παράγει μία ολόκληρη ακολουθία DNA.



Σχήμα 3. 4 Εξελιξιμότητα των εφαρμογών του CAP3

Το CAP3 πρόγραμμα διαβάζει από ένα αρχείο εισαγωγής μία συλλογή από ακολουθίες γονιδίων και καταγράφει τα αποτελέσματα. Η φύση της συγκεκριμένης εφαρμογής καθιστά εξαιρετικά εύκολη την χρήση τεχνολογιών cloud και πιο συγκεκριμένα των τεχνολογιών Hadoop, Dryadlinq και cGL-MapReduce.

Αυτές οι τρεις τεχνολογίες cloud έχουν ήδη εφαρμοστεί στο CAP3 πρόγραμμα για να μελετηθεί η ευχρηστία του. Τα παρακάτω διαγράμματα δείχνουν την επίδοση και την εξελιξιμότητα των τεχνολογιών Hadoop, Dryadlinq και cGL-MapReduce στα πλαίσια του CAP3 . Φαίνεται λοιπόν ότι και οι τρεις χρόνοι εκτέλεσης των τεχνολογιών λειτουργούν σχεδόν εξίσου καλά για το CAP3 πρόγραμμα πράγμα που ευνοεί την χρήση τεχνολογιών cloud στο συγκεκριμένο πρόγραμμα.



Σχήμα 3. 5 Απόδοση των εφαρμογών του CAP3.

3.1.3 GTM & MDS Interpolation

Οι MDS και GTM είναι γνωστοί σαν αλγόριθμοι για την μείωση των διαστάσεων οι οποίοι βρίσκουν με υψηλή ακρίβεια τις πληροφορίες μιας πολύ μικρής περιοχής από έναν μεγάλο πολυδιάστατο χώρο. Παρόλο που και οι δύο αυτοί αλγόριθμοι έχουν ως στόχο την βέλτιστη μείωση της διάστασης, μόνο ο MDS μπορεί να χρησιμοποιηθεί σε ακολουθία DNA αφού ο GTM βρίσκει μία μη γραμμική χαρτογράφηση βασισμένη στο γκαουσιανό πρότυπο πυκνότητας πιθανότητας σε αντίθεση με τον MDS που προσπαθεί να κατασκευάσει μία χαρτογράφηση στη διάσταση του στόχου υπολογίζοντας όμως και τις πληροφορίες των εγγύς περιοχών.

3.1.4 Συλλογή πληροφοριών ασθενούς σε ιατρικά διαγνωστικά κέντρα μέσω Cloud Comptuing.

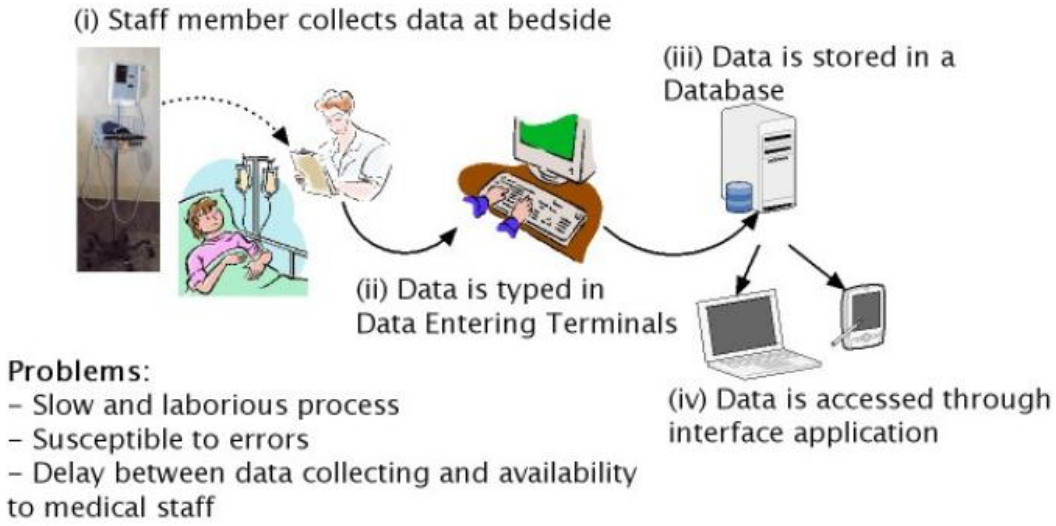
Οι υπάρχουσες διαδικασίες συλλογής ζωτικών πληροφοριών για τους ασθενείς απαιτούν πολύ δουλειά εργαστηριακής εργασίας για τη συλλογή, είσοδο και την ανάλυση των δεδομένων. Αυτές οι διαδικασίες είναι συνήθως αργές και εμπεριέχουν πιθανότητες σφάλματος, πράγμα που καθιστά αδύνατη την πρόσβαση και επεξεργασία σε πραγματικό χρόνο των δεδομένων του

ασθενούς. Αυτό το σενάριο λόγω των δυσκολιών, συγκρατεί τις κλινικές διαγνώσεις και τις δυνατότητες επιτήρησης. Έτσι προτείνεται μια λύση για να αυτοματοποιήσουμε αυτές τις διαδικασίες χρησιμοποιώντας «ανιχνευτές» προσαρμοσμένους στους υπάρχοντες ιατρικούς εξοπλισμούς που είναι διασυνδεδεμένοι για να ανταλλάσουν πληροφορίες. Η πληροφορία γίνεται διαθέσιμη στο cloud από το σημείο που γίνεται επεξεργασία από τον ειδικό συστημάτων και διανείμετε στο ιατρικό προσωπικό.

Η τηλεϊατρική επιτρέπει απομακρυσμένη διάγνωση και επιτήρηση ασθενών. Εγγυάται ευελιξία, ασφάλεια και αξιοπιστία στα μοντέρνα ιατρικά-διαγνωστικά κέντρα.

Απαραίτητα είναι η ευελιξία, η ευκολία στην παραμετροποίηση, τη διαχείριση, να είναι αναβαθμίσιμα και αυτό-ρυθμιζόμενα τα συστήματα που χρησιμοποιούνται για την τηλεϊατρική. Πολύ σημαντικό είναι η λήψη βιο-σημάτων από ασθενείς, η διανομή τους και η επεξεργασία αυτών των σημάτων. Μια λύση για να αυτοματοποιήσει αυτές τις διαδικασίες από την πλευρά του κρεβατιού, τη λήψη των σημάτων, τη διανομή τους μέχρι και την ασύρματη πρόσβαση των πληροφοριών από το προσωπικό του νοσοκομείου, παρουσιάζεται παρακάτω. Η λύση βασίζεται σε ασύρματους αισθητήρες και αντίστοιχες εφαρμογές διαχείρισης τους. Η προσφορά αυτής της εφαρμογής επεκτείνεται σε δύο πεδία. Το κοινωνικό αλλά και το επιστημονικό. Στο κοινωνικό επιδικνείουμε την πρωτοπορία αλλά και το χαμηλό κόστος υλοποίησης για να αναδείξουμε την ποιότητα ιατρικής βοήθειας. Στο επιστημονικό πεδίο αναπτύσσονται προκλήσεις για την ενσωμάτωση σύνδεσης πρωτοποριακών αισθητήρων με παραδοσιακές ιατρικές συσκευές, και να μπορεί το οι υπηρεσίες cloud να συλλέγουν, επεξεργάζονται και να διανέμουν ζωτικά σήματα ασθενών.

Αυτή η ιδέα είναι οργανωμένη όπως φαίνεται στο παρακάτω σχήμα.

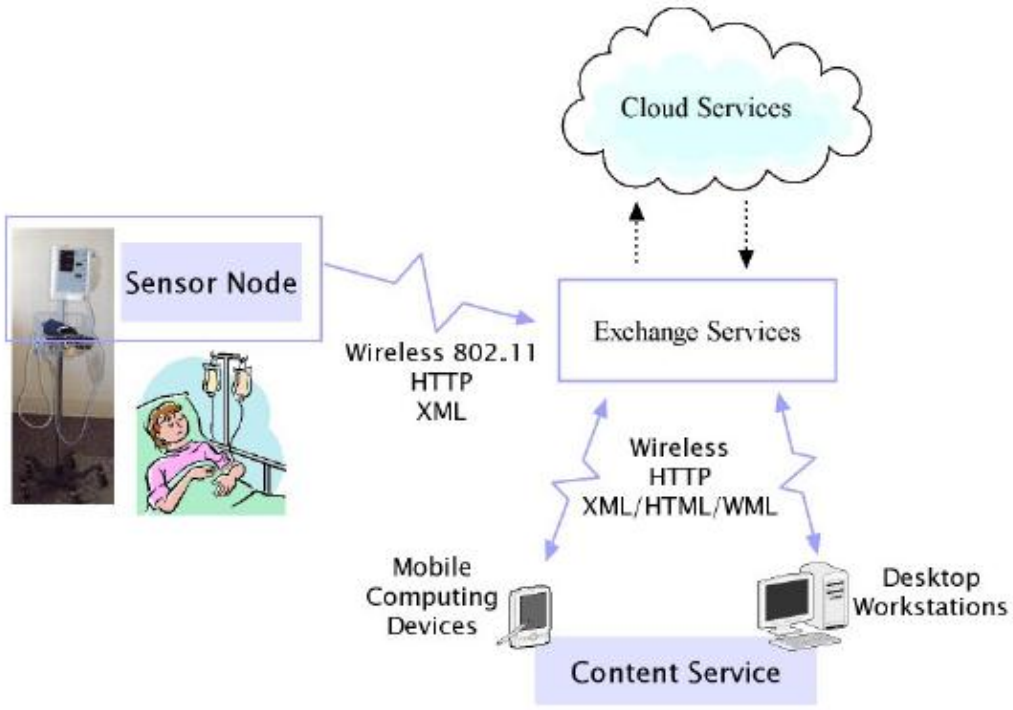


Σχήμα 3. 6 Τρέχον σενάριο

i) Ένα μέλλος του προσωπικού συλλέγει τα δεδομένα του ασθενούς στο κρεβάτι και τα γράφει σε ένα υπολογιστικό φύλλο.
ii) Οι σημειώσεις εισάγονται σε μηχανήματα εισαγωγής δεδομένων.
iii) Η πληροφορία μεταδίδεται σε ένα διακομιστή (server) που οργανώνει, κατηγοριοποιεί και κάνει προσβάσιμη την πληροφορία μέσω μιας διεπαφής, και
iv) Σε αυτό το σημείο το προσωπικό μπορεί και έχει πρόσβαση στην πληροφορία μέσω ειδικής διεπαφής

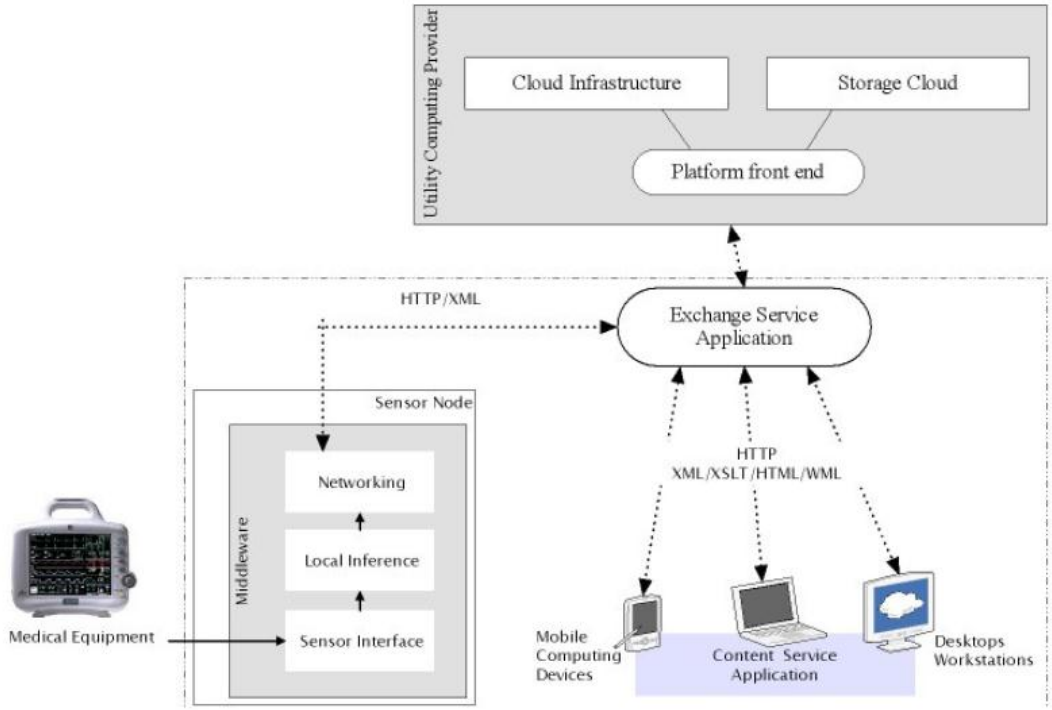
Είναι σαφές ότι υπάρχει καθυστέρηση μεταξύ της συλλογής πληροφοριών και της προσβασιμότητας της πληροφορίας. Αυτό είναι ανεπιθύμητο και αποτρέπει επιτήρηση σε πραγματικό χρόνο των ζωτικών σημάτων του ασθενούς, περιορίζοντας έτσι τις δυνατότητες των κλινικών εφαρμογών.

Μπορούμε να εστιάσουμε σε ένα ειδικό σετ ειδικών εφαρμογών υπολογιστών, που ονομάζεται υπολογιστικό νέφος (cloud computing). Μπορεί να θεωρηθεί το περιβάλλον που περιέχει τους ασύρματους αισθητήρες που έχουν συνδεθεί με τις παραδοσιακές ιατρικές συσκευές σαν σύννεφο, και να συνδεθούν για να ξεκινήσουν να συλλέγουν και να μεταδίδουν πληροφορίες. Οι υπολογιστικοί πόροι (διαθέσιμοι Η/Υ) είναι ρυθμισμένοι για να λαμβάνουν, αποθηκεύουν, επεξεργάζονται και διανέμουν τις πληροφορίες.



Σχήμα 3. 7 Λύση μέσω cloud computing του προηγούμενου σενάριου.

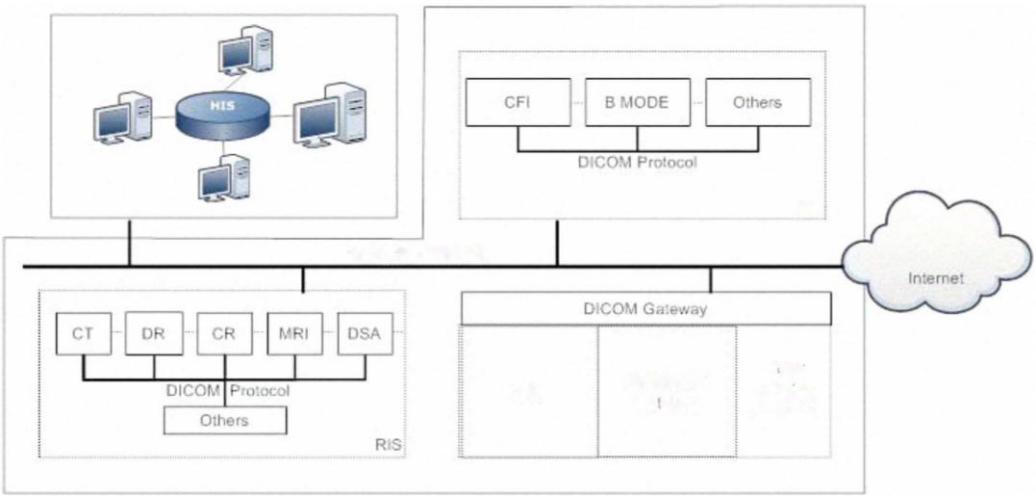
Οι αισθητήρες είναι εφοδιασμένοι με λογισμικό το οποίο συλλέγει, κωδικοποιεί και μεταδίδει την πληροφορία μέσω ασύρματου δικτύου για να αποθηκευτεί. Η υπηρεσία ανταλλαγής λειτουργεί σαν μεσίτης μεταξύ τοπικής και απομακρυσμένης υπηρεσίας. Είναι υπεύθυνο για να λαμβάνει την πληροφορία από τους αισθητήρες και να την αποστέλλει στην κατάλληλη υπηρεσία αποθήκευσης που φιλοξενείται στο σύννεφο. Ακόμα συλλέγει αιτήσεις (requests) από την υπηρεσία περιεχομένου για να ανακτήσει πληροφορία από την υπηρεσία του σύννεφου, της οποίας η λειτουργικότητα είναι διπλή: (ι) Είναι για να παρέχει υπηρεσίες αποθήκευσης της πληροφορίας και (ιι) παρέχει μια πλατφόρμα για ανάπτυξη, δοκιμή και εξέλιξη των εφαρμογών που χρειάζονται από το ιατρικό προσωπικό.



Σχήμα 3. 8 Προτεινόμενη τελική λύση

3.1.5 Μια λύση μέσω υπολογιστικού νέφους για το ολοκληρωμένου πληροφοριακού συστήματος νοσοκομείου, Hospital Information System (HIS).

Το Hospital Information System (HIS) αναφέρεται στο υπολογιστικό σύστημα το οποίο εφαρμόζεται στην ιατρική διαχείριση των πληροφοριών. Καλύπτει όλες τις νοσοκομειακές υπηρεσίες και περιλαμβάνει το εργαστηριακό σύστημα πληροφοριών (Laboratory Information System(LIS)), το ακτινολογικό σύστημα πληροφοριών (Radiology Information System (RIS)), το σύστημα πληροφοριών υπερήχων (Ultrasound Information System(UIS)) και πολλά άλλα. Η δομή του HIS βασίζεται στο πρωτόκολλο DICOM (Σχήμα 3.9) .



Σχήμα 3. 9 Standard HIS framework based on DICOM protocol

Μέχρις στιγμής στο HIS έχουν ευρέως υιοθετηθεί τεχνολογίες όπως η αρχειοθέτηση εικόνων και συστημάτων επικοινωνίας (Picture Archiving and Communication System(PACS)), οι ηλεκτρονικοί φάκελοι ασθενών(Computerbased Patient Records(CPR)) και πολλές άλλες. Παρ' όλα αυτά, πρέπει να συνειδητοποιήσουμε ότι η αδυναμία της τεχνολογίας, η έλλειψη των κεφαλαίων και η καθυστερημένη έναρξη του καθιστά την HIS βιομηχανία λιγότερο επιτυχημένη απ' ότι άλλες. Ειδικότερα στα δημόσια νοσοκομεία τα προβλήματα είναι περισσότερα.

Προκειμένου να μειωθεί η δυσκολία κατασκευής του HIS είναι σημαντικό να υπάρξει μεγάλη ανταλλαγή πληροφοριών. Στην εικόνα 1 φαίνεται ότι υπάρχει διεπαφή για την σύνδεση του διαδικτύου αλλά υπάρχει έλλειψη κατάλληλης τεχνολογίας για την πραγματοποίηση της. Εκτός από το υψηλό κόστος παραγωγής της κατασκευής και διαχείρισης δεν υπάρχει και ικανοποιητική προσφορά ανταλλαγής πληροφοριών. Αν και έχει ήδη αρχίσει η εγκαθίδρυση ενός ομοιόμορφου ιατρικού αρχείου είναι ακόμη δύσκολό να επεκταθεί. Όλα αυτά τα προβλήματα αναμένεται να λυθούν χάρη στην καινοτομία της συνολικής δομής του HIS.

3.1.5.1 Κίνητρο

Η παραδοσιακή κατασκευή του HIS χρησιμεύει στο να βοηθήσει ώστε τα νοσοκομεία να είναι ανεξάρτητες και αυτόνομες μονάδες. Υπάρχουν όμως κάποια ερωτήματα που είναι δύσκολο να αποφευχθούν.

- Προβλήματα του παραδοσιακού HIS

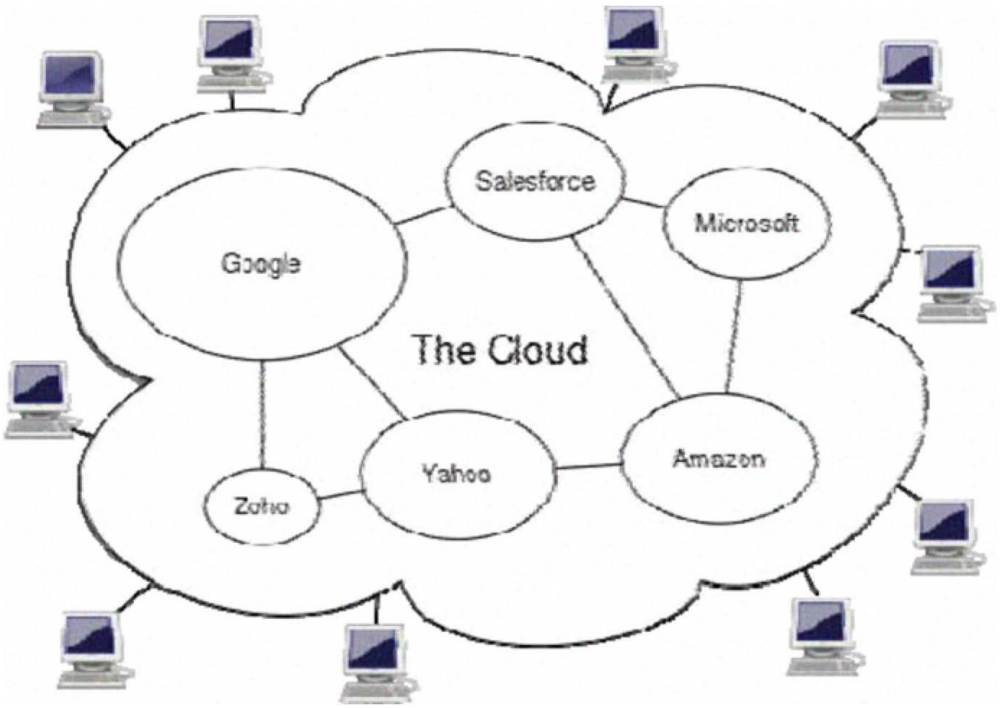
1. Η έλλειψη ενιαίων προτύπων για την ανταλλαγή δεδομένων που εφαρμόζεται στον ηλεκτρονικό φάκελο ασθενών (Computerbased Patient Records (CPR)) είναι ένα από τα βασικότερα προβλήματα. Όμως πριν την επίλυση αυτού του προβλήματος είναι σημαντικό να επιλυθούν τα προβλήματα που δημιουργούνται από τα διαφορετικά πρότυπα αποθήκευσης δεδομένων και μετάδοσης. Η ενοποιημένη μορφή και το περιεχόμενο αποθήκευσης δεδομένων αποτελούν την βάση για την επικοινωνία μεταξύ των συστημάτων. Δεδομένου ότι ένας ασθενής μπορεί να μην νοσηλεύεται σε ένα μόνο συγκεκριμένο νοσοκομείο αλλά σε πολλά ,αν αυτά έχουν ανεξάρτητα συστήματα πληροφοριών τότε κατά την διάρκεια μετάδοσης του ηλεκτρονικού φάκελού του μπορεί να μην αναγνωριστούν οι πληροφορίες εξαιτίας της ασυμβατότητας των πληροφοριακών συστημάτων. Την ίδια στιγμή, εντός ενός νοσοκομείου υπάρχει μεγάλος αριθμός ιατρικού εξοπλισμού όπως υπέρηχοι, αξονικοί τομογράφοι, ακτινολογικός εξοπλισμός, είδη εξοπλισμού παρακολούθησης και πολλά αλλά τα οποία παράγουν αριθμό δεδομένων διαφορετικών μορφών αποθήκευσης και μεθόδων κωδικοποίησης. Οι πληροφορίες ταξινόμησης και τα δεδομένα των προτύπων δεν είναι απολύτως ενιαία. Αν και υπάρχουν διασυνδέσεις μεταξύ των διάφορων συστημάτων , είναι πολύ δύσκολο να υλοποιηθεί η διασύνδεση μεταξύ των διάφορων υποσυστημάτων. Ως εκ τούτου, οι πληροφορίες δεν ανταλλάσσονται αποτελεσματικά μεταξύ των διάφορων νοσοκομείων, αλλά και πολλές φορές ακόμη και μεταξύ των διάφορων τμημάτων στο ίδιο νοσοκομείο, με αποτέλεσμα να έχουμε σπατάλη πόρων.
Υπάρχει πολύ υψηλό κόστος για την ανεξάρτητη κατασκευή του HIS. Έτσι κάθε νοσοκομείο που θέλει να δημιουργήσει μία πλήρης πλατφόρμα που να συνδυάζει όλες τις πτυχές όπως υλικό, λογισμικό, διαχείριση και συντήρηση πρέπει να ξοδέψει πολλά χρήματα. Κυρίως στα δημόσια νοσοκομεία είναι αδύνατο να δημιουργηθεί μία ανεξάρτητη πλατφόρμα καθώς αυτό θα σημαίνει σημαντική οικονομική επιβάρυνση για την παροχή ιατρικών υπηρεσιών στους πολίτες. Ακόμη και για τις ιδιωτικές κλινικές και για τα μεγάλα νοσοκομεία, η ανεξάρτητη κατασκευή του HIS είναι ένα βαρύ φορτίο που θα αύξανε σημαντικά το κόστος δαπανών των νοσοκομείων. Έτσι τα νοσοκομεία συνεχίζουν να χρησιμοποιούν το χαρτί για να καταγράφουν τις διάφορες πληροφορίες.

2. Είναι δύσκολο να διαχειριστεί και οι αναβαθμίσεις και οι συντηρήσεις των μεμονωμένων HIS απαιτούν χωριστή διαχείριση και συντήρηση. Τα προβλήματα που προκύπτουν κατά την διάρκεια λειτουργίας του HIS όπως οι τεχνικές ελλείψεις, η εσφαλμένη χρήση του λογισμικού ή η έλλειψη εμπειρογνωμόνων , η διαχείριση και η συντήρηση που απαιτεί συνεχείς επενδύσεις αποτελούν ένα μεγάλο κόστος για τα νοσοκομεία. Επίσης, τίθεται

και το θέμα της αναβάθμισης. Τα ανεξάρτητα HIS πρέπει να αναβαθμιστούν ξεχωριστά σε κάθε νοσοκομείο, με αποτέλεσμα πολλά τμήματα του HIS να μην έχουν την κατάλληλη τεχνική υποστήριξη.

- Σχετικά έργα

Για την επίλυση των παραπάνω προβλημάτων κλειδί είναι η από κοινού χρήση λογισμικού, υλικού και ιατρικών δεδομένων. Υπάρχουν ήδη κάποια σχετικά έργα που μπορούν να παρέχουν παρόμοιες λύσεις.
1. Οι εργασίες του Wang, J. W., Sun W., Ye, X. and Chen. S. T., "Construction of citizen healthy information system in Xiamen," δείχνουν ότι στην επαρχεία Fujian έχει δημιουργηθεί ένας ενιαίος ιατρικός φάκελος. Εκτιμάται ότι θα καλύψει πολλά νοσοκομεία για την επίτευξη του ηλεκτρονικού φακέλου ασθενή.
2. Η εργασία Waldrop, M., "Data center in a box - A shipping container stuffed with servers could usher in the era of cloud computing" προτείνει ένα HIS κατασκευασμένο με την τεχνολογία και την μέθοδο εφαρμογής XML. Αυτό μπορεί να καλύψει ικανοποιητικά την ένταξη και την ανταλλαγή πληροφοριών μεταξύ των νοσοκομείων όμως είναι πολύ δύσκολο να επεκταθεί.
Το cloud computing είναι ένα νέο μοντέλο εφαρμογής το οποίο έχει ευρύ χώρο για ανάπτυξη νοσοκομειακών πληροφοριών και είναι επεκτάσιμο και ευέλικτο.



Σχήμα 3. 10 The cloud

Cloud computing

- Ανάπτυξη

Το Cloud computing είναι ένα καινοτόμο μοντέλο δικτύου που προωθείται από εταιρίες όπως η Amazon, η Google, η Microsoft, η Yahoo και άλλες μεγάλες εταιρίες. Η Google είναι ο μεγαλύτερος χρήστης του Cloud computing με μηχανή αναζήτησης που βασίζεται σε περισσότερους από ένα εκατομμύριο servers στη διάθεση της. Η Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service (S3) παρέχουν υπηρεσίες κυρίως για επιχειρήσεις και η IBM's "Blue Cloud"
computing platform θα παρέχει ένα ανοιχτό cloud computing σύστημα για πελάτες με buy-to-use cloud platform.

- Cloud στην ιατρική υποθέσεων

Το Cloud computing παρέχει ένα νέο τρόπο για την επίλυση των προαναφερθέντων προβλημάτων. Ορισμένες μελέτες διεξήχθησαν πρόσφατα σε μια προσπάθεια χρήσης του cloud computing στην ιατρική υποθέσεων.

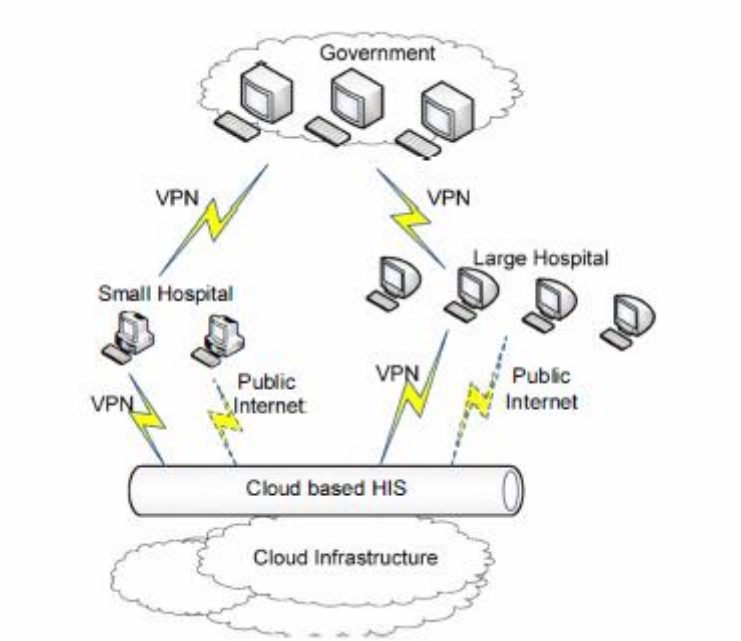
1. Η εργασία Tsumoto, S. and Hirano, S., "Data mining in hospital information system for hospital management," παρουσιάζει τα θέματα MIA (Medical Imaging Analysis) και προτείνει ένα νέο πλαίσιο που βασίζεται στην cloud computing αντίληψη για την έρευνα απεικόνισης του καρκίνου. Αν και η ανάλυση δεν έχει επικεντρωθεί θέματα νοσοκομείου οι δυσκολίες στην διεκπεραίωση των ιατρικών πληροφοριών και οι δυνατότητες του cloud computing αναλύονται λεπτομερώς.
2. Επιπλέον η εργασία των Rolim, C. 0., Koch, F. L., Westphall, C. 8., Werner, Fracalossi, A. and Salvador, G. S., "A cloud computing solution for patient's data collection in health care institutions"προτείνει το cloud computing για την συγκέντρωση των δεδομένων των ασθενών. Έτσι μπορεί να αυτοματοποιηθεί η διαδικασία από την συλλογή δεδομένων κλίνης σε πληροφορίες διανομής και απομακρυσμένης πρόσβασης από το ιατρικό προσωπικό.

Έτσι φαίνεται ότι το cloud computing λειτουργεί στο νοσοκομείο υποθέσεων και προτείνεται η περαιτέρω ανάπτυξή του.

3.1.5.2 Πρόταση

Η πρόταση μας είναι ένα ενιαίο σύστημα στο οποίο θα μοιράζονται οι πληροφορίες από διαφορετικά νοσοκομεία μέσω εικονικού ιδιωτικού δικτύου (VPN) και το οποίο θα έχει πρόσβαση στο διαδίκτυο. Η εικόνα 3 είναι η προτεινόμενη cloud – based κατασκευή του. Το τμήμα υγείας ορίζει τις private cloud για να αποθηκεύσουν και να διαχειριστούν σημαντικές πληροφορίες όπως οι υπηρεσίες πληροφορικής που στις οποίες βασίζονται τα μητρώα

ασθενών κλπ. Άλλα δεδομένα της διαχείρισης μπορούν να τεθούν σε commercial cloud server.



Σχήμα 3. 11 Κατασκευή του HIS που βασίζεται στο cloud

Το πλαίσιο αυτό είναι εύκολο να το καταλάβουμε με την προσθήκη μιας μονάδας δικτύου ή κέντρου ελέγχου στο οποίο θα μπορούν να επισυνάπτονται τα υπάρχοντα συστήματα. Η μονάδα του δικτύου θα είναι συνδεδεμένη στο σύννεφο, και θα μπορούν να χρησιμοποιούνται πόροι του σύννεφου για την επίτευξη υλικού, λογισμικού, και αποθήκευσης δεδομένων ανάλογα με τις ανάγκες. Χρησιμοποιώντας αυτή την μέθοδο αποκτάμε ρυθμιζόμενη ευέλικτη δομή. Είναι πολύ προσιτή η χρήση του cloud computing στις ιατρικές υπηρεσίες καθώς πολλά νοσοκομεία μπορούν να μοιραστούν την υποδομή που σχηματίζεται και έτσι να γίνονται πιο αποτελεσματικά μειώνοντας το κόστος κατασκευής. Στα μικρά νοσοκομεία, μπορούν να ενταχθούν περισσότερες επιχειρήσεις στο σύννεφο έτσι ώστε να απαλλαχτεί το μικρό νοσοκομείο από το βαρύ φορτίο της πλήρους κατασκευής και διαχείρισης.

Υπάρχουν πολλά πρακτικά πλεονεκτήματα όπως:

- Μείωση κόστους. Χρησιμοποιώντας το cloud computing, τα νοσοκομεία μπορούν να χρησιμοποιούν τις υπηρεσίες που παρέχονται από εκατομμύρια
  servers στο σύννεφο επιτυγχάνοντας υψηλή απόδοση σε χαμηλό κόστος.
- Ευέλικτο και επεκτάσιμο πλαίσιο. Το πλαίσιο του σύννεφου υποστηρίζει ετερογενή εξοπλισμό και συστήματα τροποποιήσιμης κλίμακας. Τα μικρά νοσοκομεία μπορούν να χρησιμοποιούν αρχικά ένα βασικό σετ λειτουργιών και καθώς το νοσοκομείο επεκτείνεται και γίνεται ολοένα

και μεγαλύτερο μπορεί εύκολα να μεγαλώσει την κλίμακά του μέσα στο σύννεφο μέσα σε σύντομο χρονικό διάστημα.

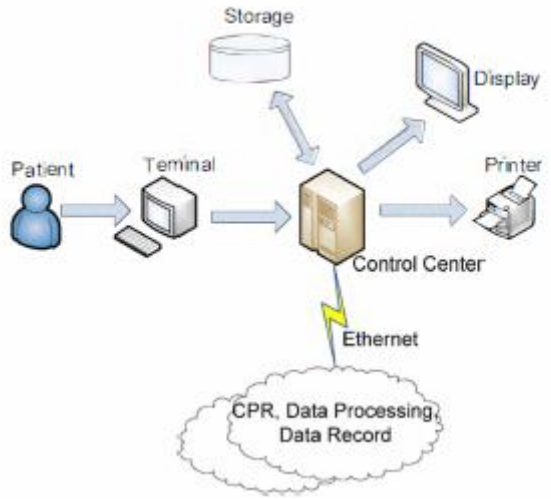
- Βελτίωση της ανταλλαγής πληροφοριών. Μέσα από το μοντέλο του σύννεφου μπορεί να υπάρξει συνεργασία μεταξύ των διάφορων ιατρικών φορέων για την ανοικοδόμηση της ανταλλαγής πληροφοριών.
- Μείωση των εξόδων συντήρησης. Η αρχιτεκτονική του τερματικού του χρήστη είναι απεριόριστη όσον αφορά το μοντέλο του cloud computing. Συνεπώς το τεχνικό προσωπικό δεν χρειάζεται να καταβάλει μεγάλη προσοχή στην αναβάθμιση του νοσοκομειακού hardware και η καθημερινή συντήρηση του διακομιστή παρέχεται από τον πάροχο υπηρεσιών του cloud. Έτσι το τεχνικό προσωπικό έχει περισσότερο χρόνο για άλλες εργασίες.
- Αξιόπιστη λειτουργία του διακομιστή. Τα στοιχεία του νοσοκομείου συγκεντρώνονται στον διακομιστή και έτσι αν δεν μπορεί να λειτουργήσει κανονικά ο server υπάρχει περίπτωση βασικά δεδομένα να χαθούν. Το μοντέλο του σύννεφου δίνει την δυνατότητα στα δεδομένα να αντιγραφούν γρήγορα από τον διακομιστή που απέτυχε σε έναν άλλο διακομιστή και να αρχίσει ένας νέος server να παρέχει τις υπηρεσίες του σε πραγματικό χρόνο.
- Περαιτέρω προοπτικές εφαρμογής: Έμπειροι γιατροί μεγάλων νοσοκομείων μπορούν να βοηθήσουν ασθενείς αγροτικών ιατρείων από τις εικόνες που θα συλλεχθούν και τα δεδομένα των ασθενών που θα σταλούν.

3.1.5.3 Σχεδιασμός ιατρικών συσκευών βασισμένες στο cloud

Για να δημιουργήσουμε ένα σύστημα τερματικού νοσοκομείου βασισμένο στο σύννεφο, εκτός από την εφαρμογή συστημάτων για αναβάθμιση, η καλύτερη προσέγγιση είναι η ανάπτυξη νέου ιατρικού εξοπλισμού, συμπεριλαμβανομένου και αυτών της απόκτησης εικόνας, παρακολούθησης, διαχείρισης κλπ. Βέβαια για την αποστολή στοιχείων από το τερματικό του νοσοκομείου πρέπει να συμπεριληφθούν και η επεξεργασία βίντεο και η αποθήκευση δεδομένων τα οποία διατίθενται στο σύννεφο μειώνοντας έτσι σημαντικά το κόστος εξοπλισμού και τις δυσκολίες συντήρησης. Η ιατρική εικόνα είναι σημαντική για την διάγνωση και γι' αυτό εφαρμόζεται το σύστημα επικοινωνίας και αρχειοθέτησης εικόνας (Picture Archiving and Communication System (PACS)). Ιατρικές συσκευές λήψεις ιατρικών εικόνων είναι συνήθως οι ακτινογραφία, η μαγνητική τομογραφία, το υπερηχογράφημα, η αξονική τομογραφία και υπάγονται σε διαφορετικές φυσικές αρχές για την υλοποίηση των μεθόδων απεικόνισης των ανθρώπινων εσωτερικών οργάνων, ιστών, αίματος κλπ.

Η παραδοσιακή συσκευή απόκτησης δεδομένων εικόνας θα πρέπει όχι μόνο να ολοκληρώνει τον ψηφιακό σχηματισμό εικόνας και την απόκτησή της αλλά και να επεξεργάζεται την εικόνα και να αποθηκεύει τα δεδομένα. Μια σειρά από

high-end εφαρμογές όπως ο τρισδιάστατος υπέρηχος απεικόνισης και το speckle noise attenuation επιτυγχάνονται μέσω αναβάθμισης του εξοπλισμού. Ωστόσο με την χρήση του σύννεφου η κάθε συσκευή μπορεί να απλοποιηθεί αναλόγως έτσι ώστε να ολοκληρωθεί το άκρο της συλλογής δεδομένων και εικόνων σχηματισμού βίντεο ύστερα από μία συμβατή μορφή δεδομένων προτύπου DICOM. Μέσω του υποσυστήματος δικτύου κατευθύνεται απευθείας στους κεντρικούς εξυπηρετητές του σύννεφου. Ύστερα γίνεται η παραλαβή δεδομένων και η επεξεργασία τους σε πραγματικό χρόνο. Το Σχήμα 3.12 δείχνει το βασικό διάγραμμα του ιατρικού εξοπλισμού εικονοληψίας βασισμένο στο σύννεφο.



Σχήμα 3. 12 Block διάγραμμα εξοπλισμού λήψης ιατρικής εικόνας στο cloud

3.1.5.4 Συμπέρασμα

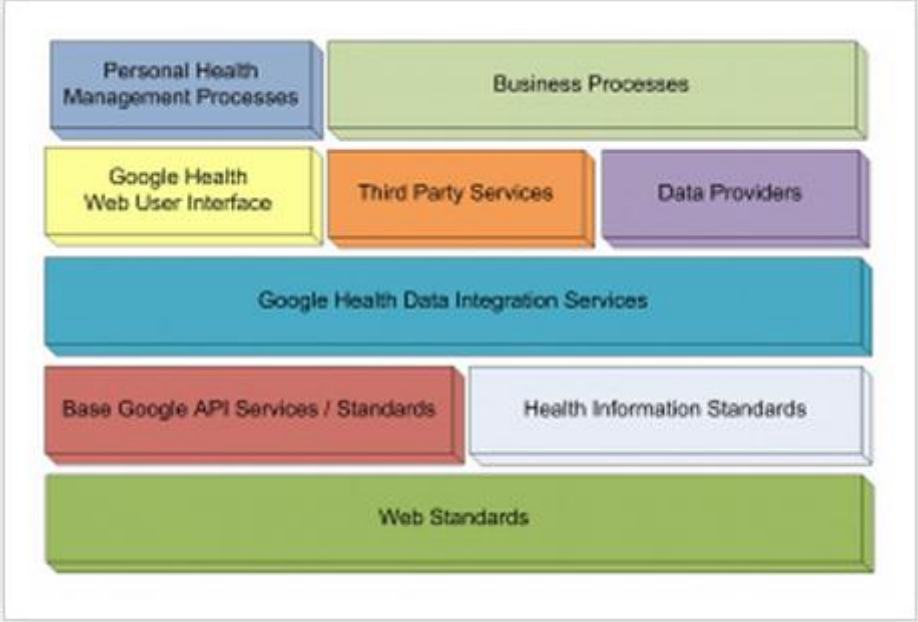
Αυτό το άρθρο περιγράφει το HIS με την χρήση του cloud computing. Συμπεραίνουμε ότι είναι ευέλικτο και επεκτάσιμο. Η χρήση του σύννεφου δεν μειώνει μόνο το κόστος κατασκευής αλλά παρέχει και ευρεία ιατρική εφαρμογή για μικρά και μεγάλα νοσοκομεία και γίνεται αποτελεσματική χρήση των πόρων. Επίσης, μειώνει τα έξοδα νοσηλείας και βελτιώνει την λειτουργική αποδοτικότητα. Η υποδομή του cloud συμβάλλει στην εξοικονόμηση χρόνου.

3.1.6 Google Health

Το Google Health είναι μια προσωπική υπηρεσία πληροφοριών υγείας από τη Google. Η υπηρεσία επιτρέπει στους χρήστες να εισάγουν τα αποτελέσματα των εξετάσεων τους ή και τις μετρήσεις διαφόρων παραμέτρων. Αυτό γίνεται είτε κάνοντας χρήση κάποιου λογαριασμού για να έχουμε πρόσβαση στην ειδική σελίδα εισαγωγής μετρήσεων. Οι προσφερμένες εθελοντικά πληροφορίες μπορούν να περιλάβουν τις «συνθήκες υγιεινής, τα φάρμακα, τις

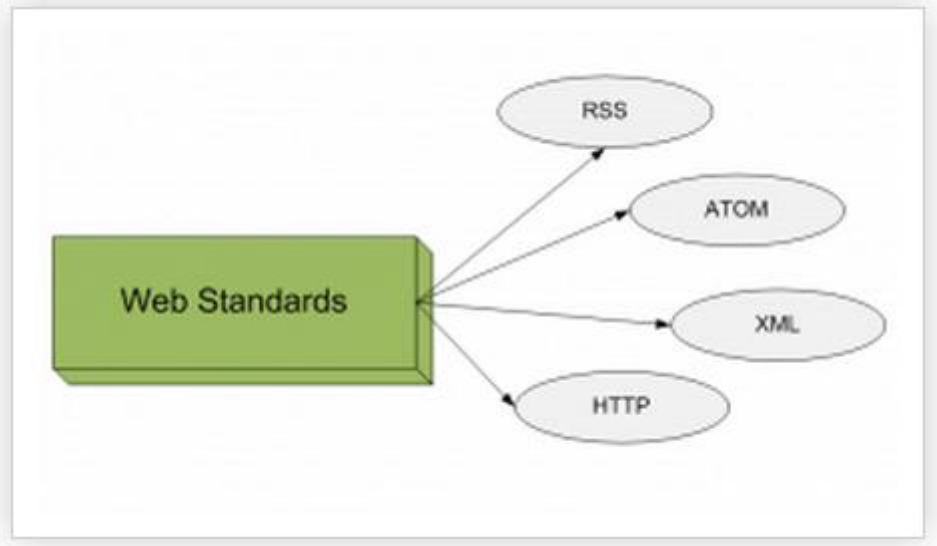
αλλεργίες, και τα αποτελέσματα εργαστηρίων». Μόλις εισαχθεί, το Google Health χρησιμοποιεί τις πληροφορίες για να παρέχει στο χρήστη ένα συγχωνευμένο αρχείο υγείας, πληροφορίες για τους όρους, και τις πιθανές αλληλεπιδράσεις μεταξύ των φαρμάκων, των όρων, και των αλλεργιών. Το Google Health όπως πολλά άλλα προϊόντα Google, είναι δωρεάν για να χρησιμοποιηθεί από τους καταναλωτές. Το Google Health είναι μια ελεύθερα επιλεγόμενη υπηρεσία, κάτι που σημαίνει ότι μπορεί μόνο να έχει πρόσβαση στις ιατρικές πληροφορίες που προσφέρονται εθελοντικά από τα άτομα. Δεν ανακτά οποιοδήποτε μέρος των ιατρικών αναφορών ενός προσώπου χωρίς τη ρητές συγκατάθεση και δράση του/της.

Αρχιτεκτονική Google health και ανάπτυξη εφαρμογής.
Το Google Health είναι ουσιαστικά μια κεντρική πλήμνη όπου οι μεμονωμένοι χρήστες μπορούν να διαχειριστούν τις πληροφορίες για την υγεία τους. Η βιομηχανία καλεί αυτό ένα προσωπικό αρχείο υγείας ή PHR.



Σχήμα 3. 13 Διαστρωματική Αρχιτεκτονική του Google Health.

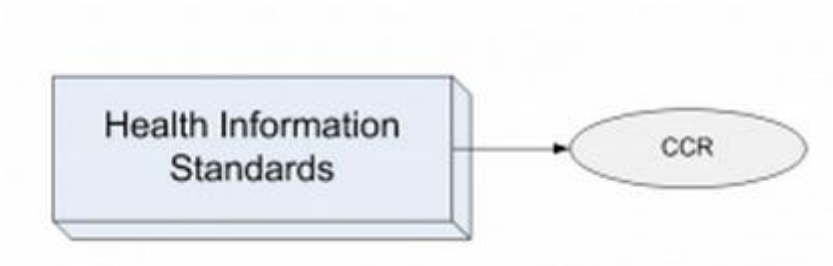
Πρότυπα ιστού.
Εκτός από τα γνωστά πρότυπα HTTP και XML για τα βασικά της επικοινωνίας, το Google στοιχείο API στηρίζεται επίσης σε κάποια περισσότερο εξειδικευμένα (think Web 2.0) πρότυπα σε RSS και το άτομο για να χειριστεί το syndication (ή τη διανομή) και την έκδοση.



Σχήμα 3. 14 Πρότυπα ιστού.

Πρότυπα υγείας

Μόνο τα τεχνικά πρότυπα από τη βιομηχανία υγειονομικής περίθαλψης που εφαρμόζεται από Google Health είναι το CCR (συνοχή του αρχείου προσοχής). Αυτό καλύπτει μια σημαντική σειρά των λεπτομερειών για την υγεία ενός χρήστη και την προσοχή που λαμβάνουν όπως τα αποτελέσματα της δοκιμής, οι αλλεργίες, το ύψος και το βάρος και πολύ περισσότερο.

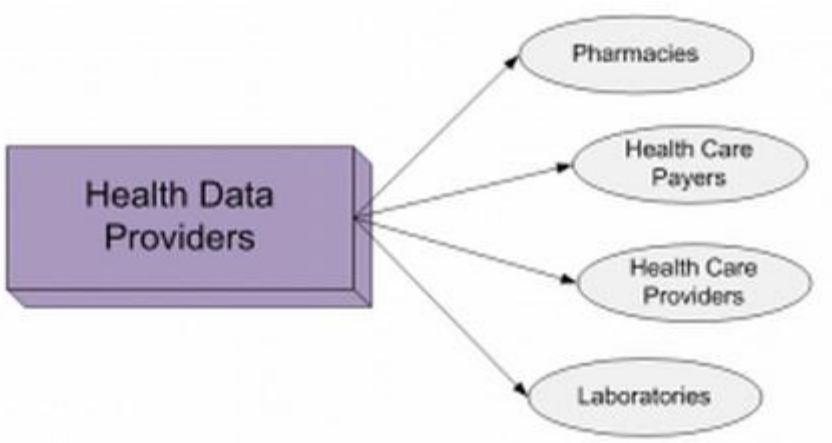


Σχήμα 3. 15 Πρότυπα ιατρικής πληροφόρησης.

Πάροχοι υπηρεσιών υγείας.

Το Google επιδιώκει ενεργά να υπογράψει επάνω τους συνεργάτες για να χρησιμεύσει ως οι προμηθευτές στοιχείων για το Google Health.

Οι χρήστες θα είναι σε θέση να εισαγάγουν τα στοιχεία τους στο σχεδιάγραμμα Google Health από τους προμηθευτές στοιχείων όπως τα φαρμακεία, τους πληρωτές υγειονομικής περίθαλψης, τους παροχείς υπηρεσιών υγείας, και τα εργαστήρια.



Σχήμα 3. 16 Πάροχοι ιατρικής πληροφορίας.

Κάθε άτομο είναι συνδεδεμένο με ένα προφίλ στο Google Health.

Σχήμα 3. 17 Προφίλ κάθε χρήστη στο google health

Η υπηρεσία google Health έχει ειδική διεπαφή REST για να διαχειρίζεται τα CCR δεδομένα.

Σχήμα 3. 18 Δειπαφή Rest του google Health

Ποια είναι τα κοινά στοιχεία ανάμεσα στο Microsoft HealthVault και Google Health:

* Και οι δύο επιχειρήσεις απαιτούν τους ίδιους τελικούς σκοπούς: Για να δημιουργήσουν τα ενσωματωμένα σε απευθείας σύνδεση περιβάλλοντα όπου μπορείτε να δημιουργήσετε και να αποθηκεύσετε τα προσωπικά αρχεία σας, παίρνετε τις πληροφορίες, βρίσκετε τους γιατρούς, κάνετε οι ιατρικοί διορισμοί, μεταβιβάζουν on-line, διαχειρίζονται τα φάρμακα, τις πληροφορίες μεριδίου με τους προμηθευτές και περισσότεροι. Το ΟΗ, και με τη Microsoft και Google, είναι εκεί πάντα ότι άλλος στόχος: για να εξουσιάσει τον κόσμο.

* Και οι δύο τεθειμένοι χρήστες στον έλεγχο αυτό που πηγαίνει στο αρχείο και ποιος έχει πρόσβαση σε τον. Εάν υπάρχει κάτι μάλλον δεν θα μοιραζόσαστε με τον εργοδότη σας, ασφαλιστική εταιρεία ή οποιαδήποτε άλλη, το αφήνει έξω.

* Και οι δύο είναι ελεύθερες βασισμένες στο WEB υπηρεσίες, σημαίνοντας μπορείτε να έχετε πρόσβαση στα αρχεία χωρίς κόστος από οποιοδήποτε υπολογιστή. Οι υπηρεσίες περιγράφονται ως τόσο ασφαλείς όσο και τις σε απευθείας σύνδεση τραπεζικές εργασίες. Και οι δύο επιχειρήσεις δεσμεύουν να μην μοιραστούν τις πληροφορίες σας χωρίς ρητή άδειά σας.

Σχήμα 3. 19 Λογότυπο Microsoft Health Vault

3.1.7 Microsoft HealthVault

Η Microsoft HealthVault είναι μια πλατφόρμα από τη Microsoft για να αποθηκεύσει και να διατηρήσει τις πληροφορίες υγείας και ικανότητας. Ξεκίνησε τον Οκτώβριο του 2007. ο ιστοχώρος είναι προσιτός στο www.healthvault.com και απευθύνεται και στα άτομα και στους επαγγελματίες υγειονομικής περίθαλψης.

Ένα αρχείο HealthVault αποθηκεύει τις πληροφορίες υγείας ενός ατόμου. Η πρόσβαση σε ένα αρχείο είναι μέσω ενός λογαριασμού (account) HealthVault, ο οποίος μπορεί να εγκριθεί για να έχει πρόσβαση στα αρχεία για πολλά ανεξάρτητα άτομα, έτσι ώστε μια μητέρα μπορεί να διαχειριστεί τα αρχεία για κάθε ένα από τα παιδιά της ή έναν για ένα γιο να μπορεί να έχει πρόσβαση στο αρχείο του πατέρα του για να τον βοηθήσει να εξετάσει τα ιατρικά ζητήματα. Η πρόσβαση στον λογαριασμό είναι μέσω του Windows Live ID ή ενός περιορισμένου συνόλου προμηθευτών OpenID.

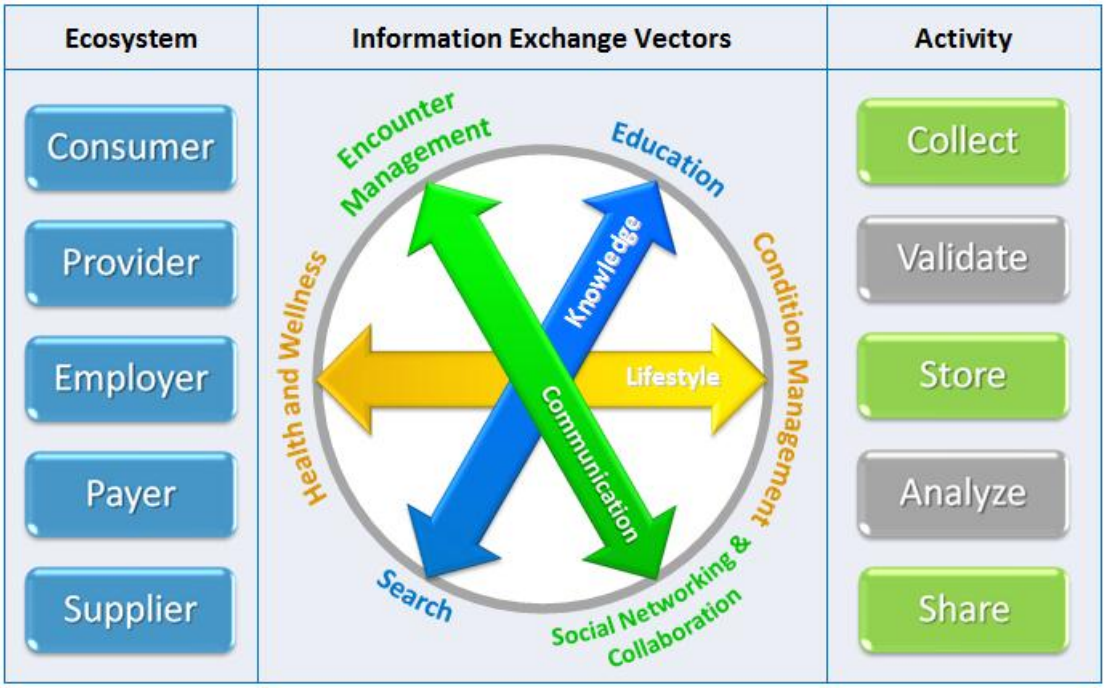
Πλατφόρμα HealthVault:

Σχήμα 3. 20 Πλατφόρμα Health Vault

Λόγοι ενσωμάτωσης στο HealthVault

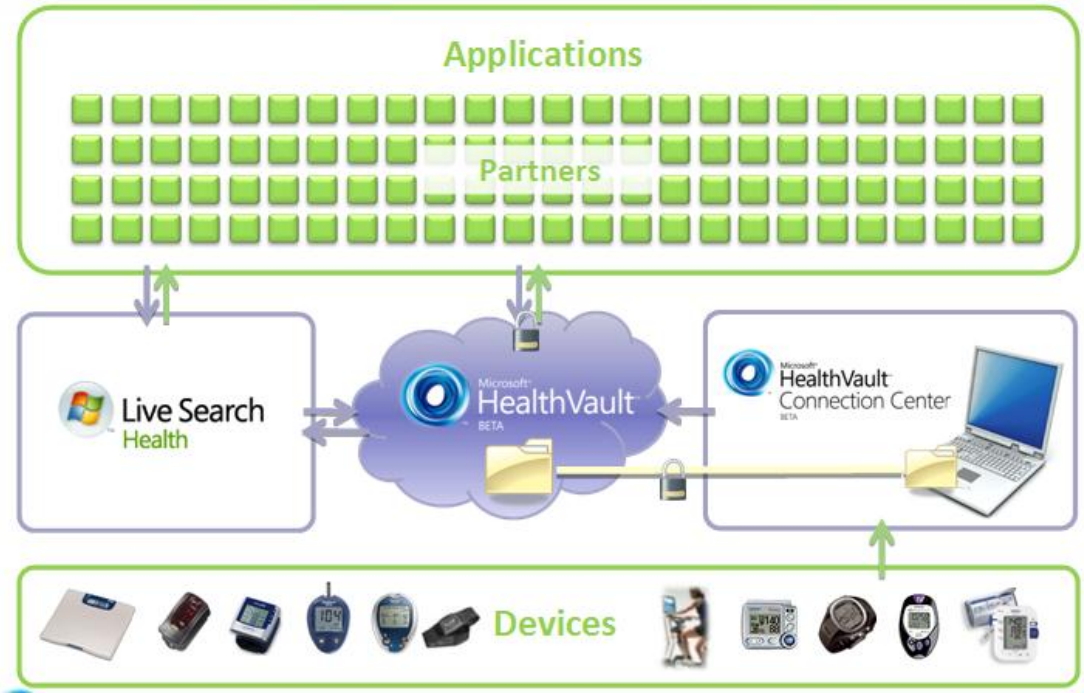
- Υπάρχει ιδιωτική και ασφαλή φύλαξη δεδομένων. Διευκολύνει τους καταναλωτές να συλλέξουν τις σχετικές προσωπικές πληροφορίες υγείας τους από μια ευρεία ποικιλία των πηγών (που αποφεύγουν τη χειρωνακτική εισαγωγή δεδομένων όσο το δυνατόν περισσότερο), να τις αποθηκεύσουν σε μια ασφαλή θέση και να μοιραστούν επιλεκτικά όπως απαιτείται.
- Επικυρώνει τους χρήστες. Μπορείς να ασφαλίσεις τη σελίδα σου με την ταυτοποίηση που χρησιμοποιεί το HealthVault, κάνοντας χρήση του Windows Live ID, ή κάποιων άλλων ανοιχτών (Open ID's). Ακόμα διαχειρίζεται τις καταγραφές για τα διάφορα μέλη μιας οικογένειας (παιδιά, συζύγους, ηλικιωμένους γονείς).
- Ασφαλίζει τον διαμοιρασμό αρχείων και ταυτοποιεί την πρόσβαση σε πληροφορίες. Διευκολύνει το διαμοιρασμό αρχείων που περιέχουν καταγραφές ή ιατρικό ιστορικό και το κάνει με τρόπο που παρέχει ασφάλεια. Υπάρχει πλήρης έλεγχος από τον χρήστη των δεδομένων που έχει στο λογαριασμό του και καμιά πληροφορία δεν μπορεί να εγκαταλείψει το λογαριασμό του χωρίς τη δική του συγκατάθεση.
- Διαλειτουργικότητα εφαρμογής. Τα σχετικά προσωπικά στοιχεία υγείας που παράγονται ή που συλλέγονται από άλλη εφαρμογή του HealthVault, μπορούν να τεθούν στην διάθεση της αίτησής σας επίσης (και αντίστροφα). Δεδομένου ότι ο χρήστης σας αυξάνει τον αριθμό εφαρμογών χρησιμοποιεί, η γενική συλλογή δεδομένων υγείας τους γίνεται πληρέστερη και οι προστιθεμένης αξίας υπηρεσίες που μπορείτε να προσφέρετε την αυξάνεται εντυπωσιακά.

- Συνδετικότητα συσκευών - σύλληψη και χρησιμοποίηση των στοιχείων συσκευών υγείας . Με την ενσωμάτωση στο HealthVault η αίτησή σας μπορεί εύκολα να ζητήσει την πρόσβαση στις πληροφορίες που φορτώνονται από ένα ευρύ φάσμα των healthVault-συμβατών συσκευών. Καμία ανάγκη να ανησυχήσει για τις παραγόμενες επί παραγγελία προσπάθειες ολοκλήρωσης συσκευών, τα πρωτόκολλα συσκευών ή τις διεπαφές. Όλες οι σημαντικές κατηγορίες συσκευών καλύπτονται σήμερα.



Σχήμα 3. 21 Αλυσίδα παροχής Ιατρικής πληροφορίας.

Σχήμα 3. 22 Αρχές σχεδιασμού health Vault



Σχήμα 3. 23 Αρχιτεκτονική Microsoft HealthVault

3.2 Σύγκριση υπηρεσιών Cloud Computing.

Το cloud αναγνωρίζεται ως μια από τις 10 καλύτερες τεχνολογίες και ακόμα έχει δημιουργήσει αρκετό ενδιαφέρον αλλά και ανταγωνισμό στη βιομηχανία. Με την εμφάνιση νέων παρόχων cloud computing, ο προσδιορισμός της καλύτερης περίπτωσης που ταιριάζει στις ανάγκες μιας επιχείρησης, είναι μια πρόκληση αλλά και ένα δύσκολο κεφάλαιο.
Η υιοθέτηση ενός παρόχου cloud, απαιτεί λεπτομερή εξέταση των παραμέτρων όπως ασφάλεια δεδομένων, SLA's αλλά και μείωση δαπανών κεφαλαίου. Παρακάτω γίνεται μια εξέταση και σύγκριση των πιο σημαντικών χαρακτηριστικών που παρέχονται από παρόχους στην βιομηχανία αλλά και εκτιμήσεις που κάνουν οι εταιρίες πριν εισαχθούν στον κόσμο του cloud.
Ενώ υπάρχουν πολλά οφέλη από την υιοθέτηση της υποδομής, της πλατφόρμας, και των υπηρεσιών που παρέχονται από ένα πάροχο Cloud. Η εφαρμοσιμότητα αυτών θα εξαρτάται από τη φύση και το μέγεθος μιας επιχείρησης. Σε μια συνεχώς αναπτυσσόμενη λίστα παρόχων cloud, η απόφαση για μια επιχείρηση στο πόσο να δυναμώσει τις υπολογιστικές πλατφόρμες και με ποιον, είναι μια περίπλοκη απόφαση. Κάθε πάροχος έχει τα δικά του πακέτα τιμών, πληρωμών, ευελιξίας και υποστήριξης αλλά και άλλων σημαντικών παραμέτρων για τις δικές του υπολογιστικές υπηρεσίες.

<u>Επιλογή cloud παρόχου.</u>

Σχήμα 3. 24 Πάροχοι cloud.

Η προσέγγιση της επιλογής ενός cloud παρόχου πρέπει να είναι πολύ προσεκτικά και στρατηγικά υπολογισμένη, διότι πρέπει να γίνει ανάλυση των παροχών του κάθε παρόχου. Κάποιες από τις πιο σημαντικές ερωτήσεις που πρέπει να απαντηθούν είναι οι παρακάτω:

- Πως είναι καθορισμένη η παροχή υπηρεσιών
- Πως εξασφαλίζεται ο πελάτης ή αντισταθμίζεται η ζημιά του σε περίπτωση διακοπής της ζητούμενης υπηρεσίας;
- Υπάρχει σύστημα ενημέρωσης συμβάντων.
- Είναι διαθέσιμες αναφορές πρόσβασης και χρήσης υπηρεσιών από τους χρήστες;
- Υπάρχουν αντίγραφα ασφαλείας των πληροφοριών και αν ναι, που βρίσκονται αυτά τα αντίγραφα αποθηκευμένα;
- Τι γίνονται αυτά τα αντίγραφα των πληροφοριών όταν διακόπτεται η συνεργασία ανάμεσα στην επιχείρηση και τον πάροχο;
- Πως μπορείτε να απεγκλωβίσετε τον εαυτό σας από μια συμφωνία αν υπάρξει μια διαφωνία;
- Πόσο ασφαλή είναι οι τα δεδομένα που αποθηκεύονται;
- Τι επίπεδα λογαριασμών πρόσβασης υπάρχουν και πως ελέγχεται η πρόσβαση στην πληροφορία;
- Πως γίνεται η πληρωμή;
- Ποια είναι τα επιπρόσθετα κόστη για την υποστήριξη της υπηρεσίας;
- Οι χρεώσεις είναι ανάλογες του όγκου των δεδομένων που αποθηκεύονται;

Τα είδη των υπηρεσιών που αξιολογήθηκαν για αυτή τη σύγκριση είναι:

IaaS (Infrastructure as a Service): Υπηρεσίες που εστιάζονται στο Hardware, όπως αποθήκευση δεδομένων, δίκτυα, και εύρος φάσματος υπηρεσιών (bandwidth).

PaaS (Platform as a Service): Υπηρεσίες που εστιάζονται στο λογισμικό και εργαλεία ανάπτυξης λογισμικού.

Πίνακας σύγκρισης παρόχων Cloud.

	Amazon AWS	Google App Engine	Windows Azure	Force.com	Rackspace	GoGrid
Cloud Services	*Paas* *Iaas*	*Paas*	*Paas* *Iaas*	*Paas*	*Iaas*	*Iaas*
Features						
Platforms supported	**Operating systems** • Red Hat Enterprise Linux • Windows Server 2003/2008 • Oracle Enterprise Linux • OpenSolaris • OpenSUSE Linux • Ubuntu Linux • Fedora Gentoo Linux • Debian • Software • IBM DB2 • IBM Informix Dynamic Server • Microsoft SQL Server Standard 2005 • MySQL Enterprise • Oracle Database 11g • Hadoop	**Runtime** • Java Runtime Environment • Python Runtime Environment **Features** • Integration with Google Accounts • URL Fetch • Mail • Memcache • Image Manipulation • Scheduled Tasks and Task Queues • XMPP • Blobstore (which supports objects upto 50MB in size) **Software** External software like AppServers Databases cannot be installed	**Operating systems** • Windows 7 • Windows Server 2008 • Windows Vista	**Software** • Unlimited real-time database customizations • Programmable user interface • Programmable cloud logic • Real-time workflow and approvals • Real-time web sites • Real-time mobile deployment • Integrated content library • Real-time analytics • Granular security and sharing	**Operating systems** • Linux • Mac OS X • Windows	**Operating systems** • Windows server 2008 • Windows server 2003 • CentOS 5.1 • CentOS 5.3 • Redhat Linux 5.1 • Redhat Linux 5.4

	Amazon AWS	Google App Engine	Windows Azure	Force.com	Rackspace	GoGrid
	• Condor • Open MPI • Apache HTTP • IIS/Asp.Net • IBM Lotus Web Content Management • IBM WebSphere Portal Server • IBM sMash • JBoss Enterprise Application Platform • Ruby on Rails • IBM WebSphere Application Server • Java Application Server • Oracle WebLogic • Wowza Media Server Pro • Windows Media Server • Zeus software					
Languages Supported	Any	• Java • Python	• VB.NET • C# • PHP	• Apex • Java • VB.Net • Perl • PHP • Python • Ruby • Windows language including VBA	• .Net • Python • PHP • Java • Ruby	• Java • PHP • Perl • C# • Python • Ruby

	Amazon AWS	Google App Engine	Windows Azure	Force.com	Rackspace	GoGrid
				• s-controls and the AJAX Toolkit		
Cloud services and tools	• Amazon CloudWatch API Tools • Auto Scaling API Tools • Elastic Load Balancing API Tools • AWS Toolkit for Eclipse • AWS Management Console • Amazon EC2 API Tools • Amazon EC2 AMI Tools • Elasticfox Firefox Extension for Amazon EC2 • Javascript Scratchpad for Amazon EC2 • Amazon S3 Authentication Tool for Curl • CloudBerry Explorer for Amazon S3 and CloudFront • Manager for Amazon CloudFront • Firefox Organizer for Amazon S3 and Amazon CloudFront (S3Fox) • AWSzone.com • Javascript Scratchpad for Amazon SQS • Amazon Mechanical Turk Developer Sandbox • Amazon Mechanical Turk Command Line Tools	• Google Secure Data Connector • Private gadgets • Google Visualization API • Google Apps APIs • Google web toolkit • IDE support	• Windows Azure Platform Training Kit • Windows Azure Software Development Kit • Microsoft Visual Studio 2008 Service Pack 1 • Windows Azure platform AppFabric SDK V1.0 • Windows 7 Training Kit For Developers	• Apex Language Code Editor • Enhanced Metadata Support • Upgrade Wizard	• Beanstalk – Hassle-free Subversion Hosting • Attachment fu in Ruby • Cloudvox • Nautilus Cloud Files Plugin by Chmouel Boudjnah • Paperclip-Cloudfiles • Olark Live Website Chat • Vanilla – Free Forum Hosting	• GoGrid's Cloudcontrol Command Line Tool • Cloud Wizard's Open Source Cross Cloud Scripting Language • Mitch Denny's Windows PowerShell Snap-in

	Amazon AWS	Google App Engine	Windows Azure	Force.com	Rackspace	GoGrid
	• LogAnalyzer for Amazon CloudFront • CloudBerry Explorer for Amazon S3 and CloudFront • Amazon CloudFront Authentication Tool for Curl • Firefox Organizer for Amazon S3 and Amazon CloudFront (S3Fox) • Manager for Amazon CloudFront • Amazon Elastic MapReduce Ruby Client • Amazon RDS Command Line Toolkit • Javascript Scratchpad for Amazon FWS Outbound • Javascript Scratchpad for Amazon FWS Inbound					

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
			Iaas			
Integrated DB supported	• MySql	• GAE doesn't support external databases; it provides a data store of its own which can be accessed through standard JDO and JPA APIs.	• Sql azure	• Not applicable	• MySQL, Microsoft SQL Oracle	• MSSQL 2008 Workgroup (64-bit) - Microsoft SQL Server Workgroup Edition 2008 • MSSQL 2008 Standard (64-bit) - Microsoft SQL Server Standard 2008 • MSSQL 2005 Standard (32-bit) - Microsoft SQL Server 2005 Standard Edition • MSSQL 2005 Workgroup (32-bit) - Microsoft SQL Server 2005 Workgroup Edition
Maximum limits	• Amazon S3 - Store object up to 5 GB • Amazon EC2 [Elastic Block storage] - Volume sizes ranging from 1GB to 1TB • (20 TB/account limit while in beta)	• Automatic scaling is built in with App Engine • No matter how many users you have or how much data your application stores, App Engine can scale to meet your needs	• Azure has a 64MB limit on individual blobs and also allows you to split a blob into blocks of 4MB each	In the unlimited edition, • Number of sites - 25 [Features available more for additional fee] • 2,000 Database objects total • storage - 120MB/user • API calls/day - 5,000/user, 5 million total • Page views/month - 1,000,000 [Features with rolling 24-hour time period] • Sites bandwidth/day - 40GB • Sites page generation time/day [Rolling 24-hour time period] -	• Infinite scalability	• Horizontal server scaling—use a GSI to rapidly deploy new servers to meet sudden spikes in demand. Delete the servers when demand drops, paying only for the resources used. • Vertical server scaling—scale RAM by deploying a GSI to a new server with a higher RAM allotment and then deleting the old server with insufficient RAM. • Server parking—bundle and park a server in

				60 server hours		GoGrid's Cloud Storage for only $0.15 -- $3.00/month. This is ideal for users that don't want to pay for an entire month of service for a server used only a few days per month.
Support for human-only tasks	Amazon Mechanical Turk	Not available	Not available	Not available	Not available	Not available
	Amazon AWS	**Google App Engine**	**Window Azure**	**Force.com**	**Rack Space**	**Go Grid**
Support						
Service Level Agreements availability	• Amazon S3 - available with a Monthly Uptime Percentage of at least 99.9% during any monthly billing cycle • Amazon EC2 - available with an Annual Uptime Percentage of at least 99.95% during the Service Year	• 100% Uptime	• 99.9% uptime	• 99.9+ percent uptime	• 100% Network Uptime Guarantee • 1-Hour Hardware Replacement Guarantee • 2-Hour Commencement of Onsite Data Restores	• 100% Uptime , which means • Network Outage: None • Packet loss < 0.1% • Latency < 5ms • Jitter < 0.5ms • Maximum Jitter: 10 milliseconds within any 15-minute period.
Support Pricing Policy	• Premium Support - Silver and Gold support available and are charged accordingly	• Free Support is available 24x7x365 from on-site cloud hosting experts	• Developer support is charged on a per incident basis. However, you are able to utilize support incidents that you already have from existing programs such as the Microsoft Developer Network (MSDN) and the Microsoft Partner Network (MPN).	• Basic Support, Premier Support, Premier Support with Administration. Developer Support is only available for a fee, on a per-case basis.	• 24x7x365 Live Support & Expertise [Pricing details not mentioned in the website]	• FREE 24/7 Phone Support • Free 24/7 Premium Support

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
Support response time	**Severity level vs response time** • Urgent - 1 hour (available for Gold subscribers only) • High - 4 business hours • Normal - 1 business day • Low - 2 business days	Not available	Not available	**Support type vs response time** • Basic Support - 2 business days • Premier Support - 2 hours • Premier Support with Administration - 2 hours	24 x 7 x 365 online live chat and toll free phone support backed by Fanatical Support	EMERGENCY Cases - 30 minutes The following are the EMERGENCY categories: • Server down • Packet loss • Routing issue All other Cases - 120 minutes
Service credit for an outage	**Monthly uptime percentage vs Service credit percentage** **Amazon S3** Equal to or greater than 99% but less than 99.9% - 10% less than 99% - 25% **Amazon EC2** If the Annual Uptime Percentage for a customer drops below 99.95% for the Service Year, that customer is eligible to receive a Service Credit equal to 10% of their bill (excluding one-time payments made for Reserved Instances) for the Eligible Credit Period	Not available	Microsoft will provide a 10 percent credit if compute connectivity falls below 99.95 percent uptime; a 10 percent credit if role-instance uptime or storage falls below 99.9 percent uptime. If it falls below 99 percent availability across anything, 25 percent credit will be provided	Not available	Not available	A "10,000% Service Credit" is a credit equivalent to one hundred (100) times Customer's fees for the impacted Service feature for the duration of the Failure

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
Incidence notification approach	Amazon Web Services publishes the most up-to-the-minute information on service availability in Service Health Dashboard Amazon Web Services keeps a running log of all service interruptions	The user should subscribe to this announcement-only list to receive updates on system outages, maintenance periods, and other service disruptions. Go to the group: google-appengine-downtime-notify Subscribe via email: google-appengine-downtime-notify-subscribe@googlegroups.com Apart from the above,when there is a scheduled down time, GAE puts the data store in read-only mode. During that time any attempt to write data to the data store will throw an exception which can be caught in the application to show a user friendly message to the user	Microsoft may send periodic e-mails informing you of technical service issues related to a product or service you requested	Trust Site -trust.Salesforce.Com-for Incident Communications	Incident reports are mostly proprietary information between us and Rackspace customers	Not available
Access/usage reports	Amazon Cloud watch	The Administrative console provides the following details, view access data and error logs, and analyze traffic browse the application's datastore and manage indexes view the status of the application's scheduled tasks	"Dallas" Features allows users to get detailed access report containing the services/datasets that were accessed, grouped by date and by account key	Force.com Sites Usage Reporting Package gives you reports and a dashboard to analyze usage of the Force.com Sites Portal health check reports show sensitive administrative and user permissions, object permissions,field-level security, organization-wide default settings, and custom sharing rules	The Rackspace Cloud Control Panel provides specific usage metrics	GoGrid CDN (Content Delivery Network) provides, • Basic Reporting • Advanced Reporting and Analytics • Real-Time Reporting Dashboard
Community News/Blogs	http://aws.typepad.com	http://code.google.com/appengine/community.html http://googleappengine.blogspot.com	http://blogs.technet.com/microsoft_blog/archive/tags/Azure/default.aspx	http://sites.force.com/blogs/ideaHome?c=09a30000000D9xo	http://www.rackspace.com/blog/	http://blog.gogrid.com/

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
Pricing						
Service/Resource pricing	**Amazon S3** - Storage Used / Data Transfer In or Data Transfer Out/PUT, COPY, POST, LIST or GET request (No charge for delete requests) **Amazon SimpleDB** - measures the machine utilization of each request and charges based on the amount of machine capacity used to complete the particular request (SELECT, GET, PUT, etc.), normalized to the hourly capacity of a circa 2007 1.7 GHz Xeon processor **Amazon CloudFront** - Charged based on the amount of data transfer out and the number of GET requests **Amazon Elastic MapReduce** – Charged per instance-hour consumed for each instance type, from the time job flow began processing until it is terminated. Each partial instance-hour consumed will be billed as a full hour **Amazon SQS** - Based on data transferred "in" and "out" of Amazon SQS/based on Amazon SQS requests which includes CreateQueue, ListQueues, DeleteQueue, SendMessage, ReceiveMessage, ChangeMessageVisibility, DeleteMessage, SetQueueAttributes, GetQueueAttributes,	An efficient application on a free account can use up to 500MB of storage and up to 5 million page views a month. When you are ready for more, you can enable billing, set a maximum daily budget, and allocate your budget for each resource according to your needs. Billing is based on the following parameters - • Outgoing Bandwidth • Incoming Bandwidth • CPU Time CPU • Stored Data • Recipients Emailed	Billing is based on Compute, Storage, Storage transactions and Data transfers	Force.com Free, Force.com Enterprise, Force.com Unlimited	Cloud Server (virtual instance) by the hour,Bandwidth In and Bandwidth Out,Amount of data backed up,Additional public IP addresses	Resources that are charged are for the RAM usage and data transfer from the server to the internet. Each account has the ability to deploy up to 200 servers. Cloud Storage billing begins after you exceed the initial 10GB storage quota

	AddPermision, and RemovePermission **Amazon RDS** - Based on per DB Instance-hour consumed, from the time a DB Instance is launched until it is terminated. Each partial DB Instance-hour consumed will be billed as a full hour/based on provisioned storage and number of I/O requests /After the DB Instance is terminated, backup storage/ data transferred "in" and "out" of Amazon RDS **Amazon EC2** - Pricing is per instance-hour consumed for each instance type, from the time an instance is launched until it is terminated. Each partial instance-hour consumed will be billed as a full hour. **Amazon FWS** - No charge					
Prepaid plan availability	Available	Available	Available	Available	Available	Available
Special Payment Services	Amazon Flexible Payments Service (Amazon FPS) and Amazon DevPay. AWS also provides consolidated Billing feature which lets you designate one AWS account as a paying account and a set of other accounts as linked accounts to form a simple one-level hierarchy	No special service available	No special service available	No special service available	No special service available	No special service available

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
Data						
Choices of data hosting location	• US – N. Virginia, • US – N. California, • EU – Ireland	• Not available	• USA - Anywhere • USA – NorthWest • USA – SouthWest • [Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities]	• Not available	• Not available	• San Francisco
Data backup	Amazon RDS automatically patches the database software and backs up the database, storing the backups for a user-defined retention period Amazon AWS may delete, without liability of any kind, any of the Amazon SQS Content that sits in a queue or any queue that remains inactive for more than the number of days specified in the user documentation. Amazon SimpleDB, in during the previous six (6) months you if there are no incurred fees for SimpleDB and have registered no usage of the Amazon SimpleDB Content, Amazon AWS may delete, without liability of any kind, the Amazon SimpleDB Content upon thirty (30) days prior notice to you. Amazon S3 versioning provides an additional layer of protection for your S3 objects. You can	The user is solely responsible for securing and backing up the Application and any Content. Google has no responsibility or liability for the deletion or failure to store any Content and other communications maintained or transmitted through use of the Service.	The user is solely responsible for securing and backing up the data.	• All networking components, SSL accelerators, load balancers, Web servers, and application servers are configured in a redundant configuration. • All customer data is stored on a primary database server that is clustered with a backup database server for redundancy • All customer data is stored on disk storage that is mirrored across different storage cabinets and controllers • All customer data, up to the last committed transaction, is automatically backed up to a primary tape library on a nightly basis • Backup tapes are immediately cloned to a second tape library to verify their integrity, and the clones are moved to secure, fire-resistant, off-site storage on	Although the Rackspace Cloud service may be used as a backup service, you agree that you will maintain at least one additional current copy of your programs and data stored on the Rackspace Cloud system somewhere other than on the Rackspace Cloud system.	Whether or not Customer's Signup calls on GoGrid to maintain back-ups, Customer will have to keep a back-up copy of all data hosted by GoGrid.

	easily recover from unintended user errors or application failures. You can also use Versioning for data retention and archiving. Once you have enabled Versioning for a particular S3 bucket, any operation that would have overwritten an S3 object (PUT, POST, COPY, and DELETE) retains the old version of the object.			a regular basis. • Disaster recovery plans are in place.		
Data after termination	Amazon will not take any action to intentionally erase any of the data stored on the Services for a period of thirty (30) days after the effective date of termination Post termination retrieval of data stored on the Services will be conditioned on the payment of Service data storage charges for the period following termination, payment in full of any other amounts due Amazon, and the compliance with terms and conditions Amazon may establish with respect to such data retrieval	If Google suspends or terminates the use of the Service with cause (or if the user voluntarily discontinues the use of the Service), the user will have access to, and the ability to export, the Content for a period of ninety (90) days following such suspension or termination. Fees will continue to be assessed for usage of the Service in excess of any portion of the Fee Threshold during the 90 day period	Upon expiration or termination of your online service subscription, you must contact Microsoft and tell whether to: (1)disable your account and then delete your subscriber data; or (2) Retain your subscriber data in a limited function account for at least 90 days after expiration or termination of your subscription (the "retention period") so that you may extract the data. If you indicate (1), you will not be able to extract your subscriber data from your account. If you indicate (2), you will reimburse Microsoft for any applicable costs. If you do not indicate (1) or (2), Microsoft will retain your subscriber data in accordance with (2). Following the expiration of the retention period, Microsoft will disable your account and then delete your subscriber data.	Upon a request made by you within 30 days after the effective date of termination of Your Force.com Free Edition service, Force.com will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format 30-days after termination, Force.com shall have no obligation to maintain or provide any of Your Data and shall thereafter, unless legally prohibited, delete all of Your Data in the systems or otherwise in Force.com's possession or under its control.	You will not have access to your data stored on the Rackspace Cloud system during a suspension or following termination.	Not available

	Amazon AWS	Google App Engine	Window Azure	Force.com	Rack Space	Go Grid
Account						
Notice period before termination	Free Services - Notice period will be provided to via the email address provided to during registration for the Services Paid Services (other than Amazon FPS and Amazon DevPay) - sixty (60) days' advance notice Amazon FPS and Amazon DevPay - Notice period will be provided to via the email address provided to during registration for the Services	You may discontinue your use of the Service at any time. Google may, at any time, terminate your use of the Service if (A) you have breached any provision of the Terms (or have acted in manner that clearly shows that you do not intend to, or are unable to comply with the provisions of the Terms); or (B) Google is required to do so by law (for example, due to a change to the law governing the provision of the Service); or (C) the Service relies on data or services provided by a third party partner and the relationship with such partner (i) has expired or been terminated or (ii) requires Google to change the way Google provides the data or services through the Service; or (D) providing the Service could create a substantial economic burden as determined by Google in its reasonable good faith judgment; or (E) providing the Service could create a security risk or material technical burden as determined by Google in its reasonable good faith judgment.	There is no notice Period before termination or suspension, but upon expiration or termination of your online service subscription, you can contact Microsoft and tell whether to: (1)disable your account and then delete your subscriber data; or (2)retain your subscriber data in a limited function account for at least 90 days after expiration or termination of your subscription	Salesforce may terminate Your Force.com service at any time without cause upon 60 days' written notice to You, or (b) upon 7 days' written notice to You of a material breach of the Agreement if such breach remains uncured at the expiration of such period	Rackspace may terminate the Agreement for breach on written notice You may terminate the Agreement for breach on written notice if: (i) Rackspace materially fails to provide the Services as agreed and do not remedy that failure within five (5) days of your written notice describing the failure, or (ii) Rackspace materially fails to meet any other obligation stated in the Agreement and do not remedy that failure within thirty (30) days of your written notice describing the failure.	GoGrid will provide 30 days advanced written notice of any termination for convenience. Upon termination for convenience, GoGrid will refund any amounts prepaid for Service not yet provided.
New user trail credentials	Amazon SimpleDB users pay no charges on the first 25 Machine Hours, 1 GB of Storage, and 1 GB of Data Transfer Out consumed every month	An efficient application on a free account can use up to 500MB of storage and up to 5 million page views a month	During Community Technology Preview (CTP), services included in Windows Azure will be available without charge - subject to certain limits. Once Windows Azure is launched for commercial use, it will be priced and licensed through both packaged	Force.com free edition	Not available	• Included free with every account, • f5 Hardware Load Balancing • 10GB of Cloud Storage per month

			offers, and the consumption			• Unlimited inbound Data Transfer • 24/7 Premium Support
	Amazon AWS	**Google App Engine**	**Window Azure**	**Force.com**	**Rack Space**	**Go Grid**
			Security			
Data security	Amazon Elastic Compute Cloud (EC2) provides Host Operating System,Guest operating system and a complete firewall solution. It also provides a way to encrypt the API calls in transit with SSL to maintain confidentiality.AWS network provides significant protection and also enables customer to implement futher protection Amazon Simple Storage Service (Amazon S3):Amazon S3 is accessible via SSL encrypted endpoints. Data stored within Amazon S3 is not encrypted at rest by AWS. However, users can encrypt their data before it is uploaded to Amazon S3 so that the data cannot be accessed or tampered with by unauthorized parties. SimpleDB APIs provide domain-level controls that only permit authenticated access by domain creator, therefore the customer maintains full control over who has access to their data.SimpleDB access can be granted based on an AWS Account ID.SimpleDB is accessible via SSL-encrypted endpoints.	App Engine runs Java applications using the Java 6 virtual machine (JVM). The JVM runs in a secured "sandbox" environment to isolate your application for service and security. The JVM can execute any Java bytecode that operates within the sandbox restrictions The Python interpreter also runs in a secured "sandbox" environment to isolate your application for service and security	• Filtering Routers • Firewalls • Cryptographic Protection of Messages • Software Security Patch Management • centralized monitoring, correlation, and analysis systems • Network Segmentation • Service Administration Access • Physical Security • limited number of Microsoft personnel may access customer information to respond to support requests and as part of incident response • Windows Azure compute provides optional sandboxing technology and mandatory sandboxing features that attempts to limit the harm to the infrastructure and all other customers from such bugs. • Windows Azure provides virtual machines to customers, giving them access to most of the same security options available in Windows Server. Updates to the software and configuration are	User authentication features such as SAML through to IP range restrictions on logons, session security and auditing. Security Addresses all layers, Physical Security Logical Network Security Host Security Transmission Level Security Database Security	Enterprise firewalls,email accounts include antivirus and spam protection. SSL capabilities available as an add on service	Provided via ServePath's secure infrastructure and telecom facility

			controlled by SSL client certificates and protected by 128 bit encryption. • All Microsoft administrative operations are audited			
Industry regulatory compliance	• SAS70 Type II • HIPAA • SOX	• US Safe Harbor	• US Safe Harbor	• US Safe Harbor • SAS 70 Type II and SysTrust Certified • ISO 27001 Certified	• US Safe Harbor	• SAS Type II • Safe Harbor Policy
	Amazon AWS	**Google App Engine**	**Window Azure**	**Force.com**	**Rack Space**	**Go Grid**
Others						
Virtualizat-ion platform	EC2 uses modified Xen virtualization	Not available	Modified Hyper-V hypervisor	Not available	Xen virtualization	Xen virtualization
Control Panel	Web based Interface	Web based Interface	Web based Interface	Web based Interface	Control panel is custom built by and for the Rackspace Cloud service.management interfaces for the Cloud Sites, Cloud Servers and Cloud Files services as well as a web based file manager.	Multiserver hosting control panel to manage servers,scale Web applications and networks
Age of Service	Since early 2006	Since July 2008	Since October 2008	Since 2007	Since 2006	March 2008

Ο πίνακας σύγκρισης δημιουργήθηκε με βάση τις τελευταίες διαθέσιμες πληροφορίες από το διαδίκτυο αλλά και τους παρόχους cloud. Τα περιεχόμενα των πινάκων δύναται να αλλάξουν καθώς και οι πάροχοι να προσθέσουν νέες υπηρεσίες και χαρακτηριστικά.

Κεφάλαιο 4.

Ασφάλεια

Εισαγωγή

Πρωταρχική σημασία έχει η αναγνώριση εκ μέρους ενός οργανισμού των πραγματικών απαιτήσεών του σε θέματα ασφάλειας. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό:

● Η αποτίμηση των κινδύνων (risk assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον, εκτιμάται η ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους, καθώς και το κόστος που θα έχουν για τον οργανισμό.

● Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

● Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία του. Το βασικότερο εργαλείο που χρησιμοποιείται στον ορισμό αυτών των απαιτήσεων είναι η πολιτική ασφαλείας που θα αναλυθεί παρακάτω.

Ασφάλεια

Όταν λειτουργούμε σε ένα περιβάλλον που υπάρχει ανταλλαγή πληροφορίας από ένα σημείο (πελάτη-client), σε ένα άλλο (διακομιστή-server), και ανάμεσα σε αυτά τα δύο παρεμβάλλεται το διαδίκτυο (“σύννεφο”), θα πρέπει να σκεφτούμε και να ελέγξουμε αν αυτή η ανταλλαγή γίνεται με ασφαλή τρόπο. Όταν γίνεται αποστολή πληροφορίας που περιέχει ευαίσθητα δεδομένα όπως πληροφορίες ιατρικού φακέλου ασθενούς, ή και προσωπικά δεδομένα όπως ημερομηνία γέννησης, Α.Φ.Μ. κλπ, είναι πολύ σημαντικό να διασφαλίσουμε πως η πληροφορία αυτή δε θα υποκλαπεί.

Εκτός από την ασφάλεια μεταφοράς των δεδομένων, πρέπει ακόμα να ελέγξουμε αν είναι ασφαλής ο τόπος που θα αποθηκευτούν οι πληροφορίες που αποστέλλουμε. Αν δηλαδή ο αποθηκευτικός χώρος που θα καταλήξουν σε ένα data center, παρέχει συνθήκες ασφάλειας και αξιοπιστίας. Πρέπει να γνωρίζουμε δηλαδή αν αποθηκεύονται με κάποιο τρόπο κρυπτογράφησης ή συμπίεσης και ακόμα αν υπάρχει δυνατότητα χρήσης αυτών των πληροφοριών από το διαχειριστή του data center.

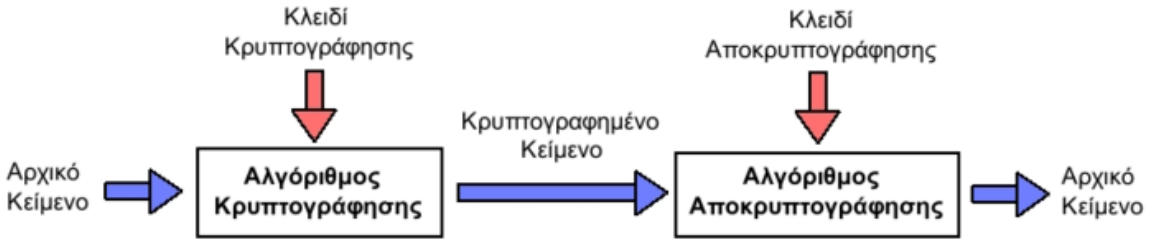
Ένα ασφαλές “σύννεφο” είναι απόλυτα απαραίτητο να πληροί όλες τις ομοσπονδιακές απαιτήσεις ασφάλειας, και να μπορεί να ενσταλάξει εμπιστοσύνη και εμπιστευτικότητα. Υπάρχουν ανασφάλειες ασφάλειας και αυτό γίνεται ορθώς. Όταν οι εφαρμογές μας εκτελούνται από το “σύννεφο”, όταν οι πληροφορίες μας

αποθηκεύονται στο "σύννεφο" και όταν δεν γνωρίζουμε ποιοι άλλοι μοιράζονται τους πόρους του "σύννεφου" όπως και εμείς, αυτό μπορεί να μας κάνει λίγο δειλούς αλλά και απρόθυμους να χρησιμοποιήσουμε το "σύννεφο" για τον οργανισμό μας. Σκεφτόμαστε ότι εγκαταλείπουμε τον έλεγχο αλλά και την ασφάλεια από τις πληροφορίες μας.

Μετατοπίζοντας τη δημόσια πληροφορία, σε ένα εξωτερικό "σύννεφο", μειώνουμε την έκθεση των εσωτερικών ευαίσθητων δεδομένων, και η ομοιογένεια του "σύννεφου" κάνει τον έλεγχο/δοκιμή της ασφάλειας του "σύννεφου" ποιο εύκολη.

Στα δημόσια "σύννεφα" οι χρήστες τείνουν να μην έχουν τον έλεγχο για το ποιος βλέπει και "αγγίζει" τα δεδομένα τους.

Η ταυτοποίηση των στοιχείων χρήστη για την είσοδο σε μια ψηφιακή υπηρεσία είναι ένα είδος ασφάλειας της πληροφορίας μας. Μόλις γίνει η εισαγωγή των στοιχείων για την είσοδο σε ένα σύστημα, ξεκινάει η πρόσβαση στους φακέλους, τα αρχεία και τις εφαρμογές που βρίσκονται στο διακομιστή (server). Τώρα ανακύπτει ένα θέμα που έχει να κάνει με την ασφαλή μεταφορά μέσω του internet, στο σύννεφο, των στοιχείων του συνδρομητή. Πρέπει δηλαδή να υπάρχει ένα είδος κρυπτογράφησης στα δεδομένα που αποστέλλονται. Δηλαδή μια διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Συγκεκριμένα να μπορούν να φτάσουν με ασφαλή τρόπο τα στοιχεία του από το χώρο του πελάτη (client) στο διακομιστή (server).



Σχήμα 4. 1 Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

4.1 Απαιτήσεις Ασφάλειας

Οι βασικές απαιτήσεις για την ασφάλεια των web εφαρμογών είναι οι εξής:

4.1.1 Αυθεντικοποίηση (Authentication): Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας, την οποία ισχυρίζεται ότι έχει ένας πελάτης της εφαρμογής. Ο πελάτης μπορεί να είναι κάποιος

τελικός χρήστης, κάποια υπηρεσία, διαδικασία ή υπολογιστής. Στο ηλεκτρονικό εμπόριο η πιστοποίηση της ταυτότητας των μερών που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να είναι σίγουρο για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται συνήθως μέσω ψηφιακών υπογραφών.

4.1.2 Εμπιστευτικότητα (Confidentiality): Είναι έννοια στενά συνδεδεμένη με την ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Αφορά τη μη αποκάλυψη των ευαίσθητων πληροφοριών σε άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση. Για το ηλεκτρονικό εμπόριο η εμπιστευτικότητα αποτελεί υψίστης σημασίας συστατικό στην προστασία των οικονομικών δεδομένων του οργανισμού, καθώς και στην προστασία των προσωπικών δεδομένων των πελατών. Τεχνικές κρυπτογράφησης χρησιμοποιούνται για να εξασφαλίσουν την εμπιστευτικότητα.

4.1.3 Εξουσιοδότηση (Authorization): Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτούμενα μέλη μπορούν να πραγματοποιήσουν, όπως για παράδειγμα εκτέλεση συναλλαγών, μεταφορά χρημάτων από ένα λογαριασμό σε άλλο ή αύξηση του πιστωτικού ορίου κάποιου πελάτη.

4.1.4 Ακεραιότητα (Integrity): Η ακεραιότητα είναι η εγγύηση ότι τα δεδομένα προστατεύονται από τυχαία ή σκόπιμη (κακόβουλη) τροποποίηση. Διασφαλίζει την εγκυρότητα, την ορθότητα και την πληρότητα των δεδομένων κατά τη φάση της εισαγωγής τους, της αποθήκευσης και της μεταφοράς τους. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς στάλθηκαν.

4.1.5 Μη αποποίηση ευθύνης (Non- repudiation): Μη αποποίηση ευθύνης σημαίνει ότι ένας χρήστης δεν μπορεί να αρνηθεί την εκτέλεση μιας λειτουργίας, και κανένα από τα συναλλασσόμενα μέρη δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, σε περίπτωση που χρειαστεί, να μπορούν να αποδείξουν την προέλευση, μεταφορά και παραλαβή των δεδομένων.

4.1.6 Διαθεσιμότητα (Availability): Αφορά την άμεση πρόσβαση στις υπηρεσίες του συστήματος για τους νόμιμους χρήστες του. Πολλοί επιτιθέμενοι, χρησιμοποιώντας επιθέσεις τύπου άρνησης υπηρεσίας (denial of service), έχουν σαν στόχο να συντρίψουν την εφαρμογή, ώστε οι υπόλοιποι χρήστες να μην μπορούν να έχουν πρόσβαση στην συγκεκριμένη εφαρμογή.

4.2 Ασφάλεια Εφαρμογών Ηλεκτρονικού Εμπορίου

Οι εφαρμογές ηλεκτρονικού εμπορίου αποτελούν αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων και της πλαστοπροσωπίας. Τα προβλήματα αυτά αντιμετωπίζονται με τη χρήση κρυπτογραφίας, η οποία επιτρέπει τη μετάδοση εμπιστευτικών πληροφοριών μέσα από ένα δίκτυο χωρίς να υπάρχει κίνδυνος υποκλοπής ή ανεπιθύμητων παρεμβάσεων. Παράλληλα επιτρέπει στις δύο πλευρές που επικοινωνούν, δηλαδή στον έμπορα και στον πελάτη, να προβαίνουν σε αμοιβαία πιστοποίηση ταυτότητας.

Στην πράξη, οι κρυπτογραφικές αρχές πρέπει να ενσωματωθούν σε εργάσιμα πρωτόκολλα επικοινωνίας και λογισμικό. Υπάρχει μια ποικιλία κρυπτογραφικών πρωτοκόλλων στο διαδίκτυο, καθένα από τα οποία είναι ειδικευμένο για διαφορετική λειτουργία. Το πρωτόκολλο SSL (Secure Sockets Layer), το οποίο παρέχει κρυπτογραφημένη επικοινωνία μεταξύ ενός προγράμματος πλοήγησης (web browser) και ενός εξυπηρετητή web (web server), αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Το πρωτόκολλο SSL παρέχει απόρρητη επικοινωνία μεταξύ πελατών και εμπόρων, υποστηρίζοντας πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών, προσφέροντας έτσι ένα ικανοποιητικό επίπεδο ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου.

Για να υπάρχει όμως ασφάλεια στις εφαρμογές ηλεκτρονικού εμπορίου απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου (web server). Ο εξυπηρετητής διαδικτύου πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης του πελάτη στον εξυπηρετητή του καταστήματος. Οι εξυπηρετητές διαδικτύου διαχειρίζονται και διανέμουν τις πληροφορίες στο διαδίκτυο.

4.3 Πρωτόκολλο Ασφάλειας SSL

Το SSL (Secure Socket Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου Ιστού, το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server). Δηλαδή το πρωτόκολλο αυτό μπορεί να παρέχει απόρρητη επικοινωνία μεταξύ εμπόρου και πελάτη σε μια συναλλαγή πληρωμής και για το λόγο αυτό το SSL αποτελεί το κύριο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Συγκεκριμένα, το πρωτόκολλο SSL παρέχει κρυπτογράφηση της μεταδιδόμενης πληροφορίας (data encryption), υποχρεωτική πιστοποίηση της ταυτότητας του

εξυπηρετητή (server authentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (client authentication) μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Επιπλέον εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity), εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Για κάθε κρυπτογραφημένη συναλλαγή δημιουργείται ένα κλειδί συνόδου (session key) το μήκος του οποίου μπορεί να είναι 40 bits ή 128 bits. Είναι γνωστό ότι όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογραφημένη επικοινωνία.

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Έχουν υπάρξει τρεις εκδόσεις του SSL. Η ιστορία της εξέλιξης του SSL έχει ως εξής:

Ιούλιος 1994: Κυκλοφόρησε η πρώτη έκδοση v.1.0 του πρωτοκόλλου SSL από τη Netscape, η οποία χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της εταιρείας.

Δεκέμβριος 1994: Κυκλοφόρησε η δεύτερη έκδοση v.2.0 του πρωτοκόλλου, η οποία ενσωματώθηκε στο web browser της Netscape, τον Netscape Navigator.

Ιούλιος 1995: Εκδόθηκε ο αντίστοιχος web browser της Microsoft, ο Internet Explorer, ο οποίος υποστηρίζει και αυτός την έκδοση v.2.0 του SSL, με κάποιες όμως επεκτάσεις της Microsoft.

Το SSL πρωτόκολλο, στην έκδοση v.2.0, καθιερώθηκε ως de facto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων. Το HTTP (Hyper Text Transfer Protocol) είναι ένα πρωτόκολλο που φροντίζει τη μεταφορά και τον τρόπο μετάδοσης δεδομένων στο διαδίκτυο. Ωστόσο το SSL v.2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του. Για το λόγο αυτό υπήρχε η ανάγκη για βελτίωση της έκδοσης v.2.0. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία.

Νοέμβριος 1995: Κυκλοφόρησε επισήμως η έκδοση v.3.0 του SSL, ενώ λίγους μήνες πιο πριν εφαρμοζόταν σε προϊόντα της εταιρείας, όπως τον Netscape Navigator.

Μάιος 1996: Το SSL περνά στη δικαιοδοσία του Internet Engineering Task Force - IETF, ο οποίος δημιουργεί την ειδική ομάδα εργασίας TLS group και μετονομάζει την νέα έκδοση του SSL, σε TLS (Transport Layer Security).

Η ομάδα εργασίας TLS group καθιερώθηκε το 1996 για να τυποποιήσει το πρωτόκολλο Transport Layer Security. Η TLS group εργάστηκε πάνω SSL v.3.0

πρωτόκολλο. Η ομάδα αυτή έχει ολοκληρώσει μια σειρά από προδιαγραφές που περιγράφουν τις εκδόσεις 1.0 και 1.1 του TLS πρωτοκόλλου, και ετοιμάζει την έκδοση 1.2.

Ιανουάριος 1999: Εκδίδεται η πρώτη έκδοση του πρωτοκόλλου TLS, η οποία μπορεί να θεωρείται και ως η έκδοση v.3.1 του SSL.

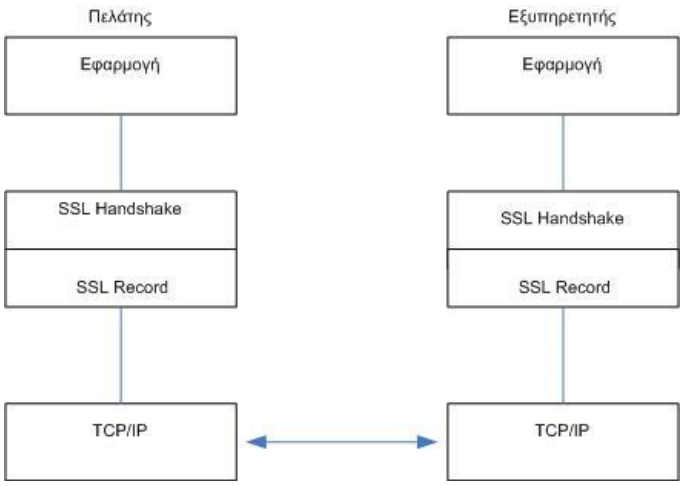
Δεκέμβριος 2005: Δημοσιεύεται η έκδοση 1.1 του TLS πρωτοκόλλου από την TLS group.

Η τρίτη έκδοση του πρωτοκόλλου SSL κάλυψε πολλές αδυναμίες της δεύτερης έκδοσης. Οι σημαντικότερες αλλαγές αφορούν: α) στη μείωση των απαραίτητων μηνυμάτων κατά το στάδιο εγκαθίδρυσης της σύνδεσης («χειραψία», «handshake»), β) στην επιλογή των αλγορίθμων συμπίεσης και κρυπτογράφησης από τον εξυπηρετητή και γ) στην εκ νέου διαπραγμάτευση του κυρίως κλειδιού (master-key) και του «αναγνωριστικού» συνόδου (session-id). Ακόμη αυξάνονται οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης και προστίθενται νέες τεχνικές για τη διαχείριση των κλειδιών. Γενικά, η τρίτη έκδοση του SSL (v.3.0) είναι πιο ολοκληρωμένη σχεδιαστικά από τη δεύτερη, με μεγαλύτερο εύρος υποστήριξης και λιγότερες ατέλειες.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου SSL, γεγονός που ερχόταν σε σύγκρουση με την τότε νομοθεσία των Η.Π.Α περί εξαγωγής κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει τη χρήση αλγορίθμων κρυπτογράφησης με κλειδί των 40 bits στις προς εξαγωγή εφαρμογές SSL, τη στιγμή που η κανονική έκδοση χρησιμοποιεί κλειδί των 128 bits. Γενικές πληροφορίες για την κρυπτογραφία και τους αλγόριθμους κρυπτογράφησης υπάρχουν στο Παράρτημα.

4.3.1 Αρχιτεκτονική του SSL

Η αρχιτεκτονική τοποθέτηση του SSL απεικονίζεται στο Σχήμα.



Σχήμα 4. 2 Αρχιτεκτονική Τοποθέτηση του SSL

Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Το TCP/IP (Transmission Control Protocol/Internet Protocol) είναι το πρωτόκολλο επικοινωνίας (communication protocol) για την επικοινωνία ανάμεσα σε υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο. Τα αρχικά TCP/IP αναφέρονται σε δύο από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, δηλ. στο TCP και στο IP. Το FTP (File Transfer Protocol) είναι ένα πρωτόκολλο μεταφοράς αρχείων, το οποίο φροντίζει για τη διακίνηση αρχείων μέσα στο διαδίκτυο, και το TELNET είναι ουσιαστικά μια υπηρεσία του διαδικτύου με την οποία οι χρήστες αποκτούν απευθείας πρόσβαση σε άλλους υπολογιστές στο διαδίκτυο.

Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο διασύνδεσης ανοικτών συστημάτων (Open System Interconnection, OSI), έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επιπλέον η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL. Το S/HTTP (Secure HTTP) πρωτόκολλο φροντίζει για την ασφαλή μεταφορά δεδομένων στο διαδίκτυο.

Ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείτε στην κορυφή του.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού. Οι αρχές τις κρυπτογραφίας περιγράφονται στο Παράρτημα.

Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου. Πληροφορίες για τα κλειδιά συνόδου υπάρχουν στο κεφάλαιο

Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

Για τη γενική λειτουργία του πρωτοκόλλου SSL υπάρχουν δύο βασικές οντότητες: σύνοδος SSL και σύνδεση SSL.

Η σύνοδος SSL αποτελεί τη δημιουργία μιας σχέσης μεταξύ ενός πελάτη και ενός εξυπηρετητή. Οι σύνοδοι δημιουργούνται από το SSL Handshake protocol και είναι ομάδες παραμέτρων ασφάλειας, οι οποίες μπορούν να διαμοιραστούν ταυτόχρονα σε πολλές συνδέσεις. Ο κύριος λόγος για αυτό είναι η αποφυγή χρονοβόρων διαπραγματεύσεων νέων παραμέτρων ασφάλειας για κάθε νέα σύνδεση.

Οι παράμετροι που περιέχονται και μοιράζονται σε μια σύνοδο είναι οι ακόλουθοι:

Αναγνωριστικό συνόδου: επιλέγεται από τον εξυπηρετητή για αναγνώριση μιας ενεργούς ή επαναληπτικής κατάστασης συνόδου.

Ψηφιακό πιστοποιητικό (μεταξύ ομότιμων οντοτήτων).

Μέθοδος συμπίεσης των δεδομένων: Αλγόριθμος που χρησιμοποιείται για συμπίεση δεδομένων πριν την κρυπτογράφηση.

Αλγόριθμος κρυπτογράφησης των δεδομένων.

Κύριο μυστικό (master secret): Μοναδικός αριθμός μήκους 48-byte, κοινό μυστικό μεταξύ εξυπηρετητή και πελάτη.

Δυνατότητα επανεκκίνησης της συνόδου.

Σύνδεση SSL είναι η μεταφορά των πληροφοριών μεταξύ δύο οντοτήτων. Στο SSL οι συνδέσεις αυτές είναι σχέσεις μεταξύ ομότιμων οντοτήτων και είναι παροδικές.

Οι παράμετροι που περιέχονται σε μια σύνδεση είναι οι ακόλουθοι:

Τυχαίοι αριθμοί μεταξύ πελάτη και εξυπηρετητή, οι οποίοι είναι διαφορετικοί για κάθε σύνδεση.

Μυστικό MAC εξυπηρετητή: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον εξυπηρετητή.

Μυστικό MAC πελάτη: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον πελάτη.

Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον εξυπηρετητή και αποκρυπτογράφηση από τον πελάτη.

Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον πελάτη και αποκρυπτογράφηση από τον εξυπηρετητή.

Διανύσματα αρχικοποίησης της σύνδεσης

Αριθμοί ακολουθίας: Κάθε μέλος (εξυπηρετητής, πελάτης) διατηρεί ξεχωριστούς αριθμούς ακολουθίας για αποστολή και λήψη μηνυμάτων σε κάθε σύνδεση.

το πρωτόκολλο SSL αποτελείται από δύο επιμέρους πρωτόκολλα, το SSL record protocol και το SSL handshake protocol. Το SSL record protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Συγκεκριμένα το πρωτόκολλο αυτό τοποθετεί τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει. Επίσης εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το SSL handshake protocol είναι ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το οποίο επίσης διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας. Συγκεκριμένα το πρωτόκολλο αυτό διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του εξυπηρετητή και του πελάτη αν αυτό ζητηθεί. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας. Τα SSL record protocol και SSL handshake protocol περιγράφονται αναλυτικά παρακάτω.

4.3.2 SSL Record Protocol

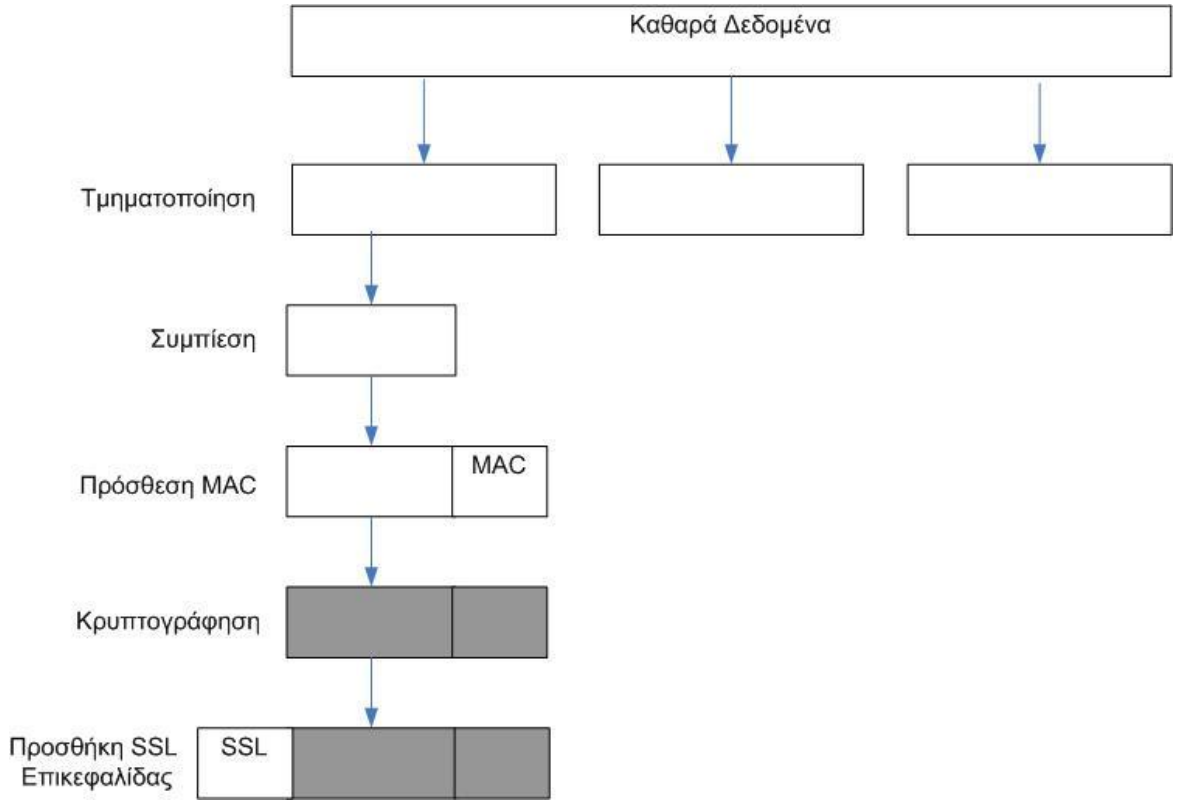
Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις:

Εμπιστευτικότητα: Το Handshake Protocol ορίζει ένα κοινό μυστικό κλειδί, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων του SSL.

Ακεραιότητα: Το Handshake Protocol επίσης ορίζει ένα κοινό μυστικό κλειδί που χρησιμοποιείται για τη δημιουργία MAC όλων των μηνυμάτων που ανταλλάσσονται.

Το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό (fragmentation), τη συμπίεση, την αυθεντικοποίηση και την κρυπτογράφηση δεδομένων. Ουσιαστικά το πρωτόκολλο αυτό μετατρέπει τα προς μετάδοση δεδομένα σε SSL πακέτα.

Το **Error! Reference source not found.** φανερώνει τη λειτουργία του SSL Record rotocol. Συγκεκριμένα το Record Protocol παίρνει το μήνυμα της εφαρμογής που θα μεταδοθεί, τμηματοποιεί τα δεδομένα σε εύχρηστα blocks, προαιρετικά συμπιέζει τα δεδομένα με κατάλληλους μηχανισμούς που επιλέγονται κατά τη «χειραψία» και μετά εφαρμόζει ένα MAC πάνω από τα συμπιεσμένα δεδομένα. Στη συνέχεια κρυπτογραφεί το αποτέλεσμα χρησιμοποιώντας συμμετρική κρυπτογράφηση, προσθέτει μια επικεφαλίδα SSL και στο τέλος μεταδίδει το πακέτο. Η μέθοδος συμπίεσης και ο αλγόριθμος κρυπτογράφησης καθορίζονται κατά τη διάρκεια εκτέλεσης του SSL Handshake Protocol.



Σχήμα 4. 3 Λειτουργία του SSL Record Protocol

Το SSL Record Protocol εκτελεί και την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Συγκεκριμένα τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων.

Διάφορα πρωτόκολλα SSL μπορούν να στρωματοποιούνται στην κορυφή του SSL Record Protocol. Οι προδιαγραφές του SSL 3.0 καθορίζουν τα ακόλουθα τρία πρωτόκολλα SSL:

Πρωτόκολλο προειδοποίησης (SSL Alert Protocol)

Πρωτόκολλο χειραψίας (SSL Handshake Protocol)

Πρωτόκολλο Αλλαγής Προδιαγραφών Κρυπτογραφίας (SSL Change Cipher Spec Protocol)

Το SSL Alert Protocol χρησιμοποιείται για να μεταφέρει προειδοποιήσεις (alerts) μέσω του SSL Record Protocol. Οι προειδοποιήσεις είναι συνήθως μηνύματα προβλημάτων και λαθών (π.χ. "λάθος MAC", "μη αναμενόμενο μήνυμα" κλπ.) που αφορούν τόσο τη

σύνδεση όσο και τη μετάδοση των μηνυμάτων μεταξύ δύο ομότιμων οντοτήτων. Με τον τρόπο αυτό ειδοποιεί το SSL να διακόψει τη σύνδεση ή να προβεί σε όποιες άλλες ενέργειες έχουν καθοριστεί.

Το SSL Handshake Protocol είναι το κύριο πρωτόκολλο SSL και περιγράφεται στην επόμενη ενότητα.

Το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας είναι το απλούστερο από τα πιο πάνω πρωτόκολλα. Χρησιμοποιείται για την αλλαγή μιας προδιαγραφής κρυπτογραφίας με μια άλλη. Κανονικά μια προδιαγραφή κρυπτογραφίας αλλάζει στο τέλος μιας SSL χειραψίας. Μπορεί όμως να τροποποιηθεί και σε οποιαδήποτε άλλη στιγμή.

4.3.3 Αντοχή του SSL σε Γνωστές Επιθέσεις

Επίθεση Λεξικού (Dictionary Attack)

Κατά την επίθεση αυτή, ένα τμήμα του μη κρυπτογραφημένου κειμένου βρίσκεται στην κατοχή κακόβουλων προσώπων. Το τμήμα αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί ένα κομμάτι που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του κειμένου έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα (128 bits). Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bits κλειδιά και παρ' όλο που τα 88 bits αυτών μεταδίδονται χωρίς κρυπτογράφηση, ο υπολογισμός 240 διαφορετικών ακολουθιών καθιστά την επίθεση εξαιρετικά δύσκολη.

Βίαιη Επίθεση (Brute Force Attack)

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι ατελέσφορη.

Επίθεση Επανάληψης (Replay Attack)

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ πελάτη - εξυπηρετητή και προσπαθεί να χρησιμοποιήσει ξανά τα μηνύματα του πελάτη για να αποκτήσει πρόσβαση στον εξυπηρετητή, έχουμε επίθεση τύπου replay attack. Όμως το SSL κάνει χρήση του αναγνωριστικού συνόδου (connection-ID), το οποίο παράγεται από τον εξυπηρετητή με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια αναγνωριστικά σύνδεσης.

Επίθεση Παρεμβολής (Man-In-The-Middle-Attack)

Η επίθεση Man-In-The-Middle-Attack συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του εξυπηρετητή και του πελάτη. Αφού επεξεργαστεί τα μηνύματα του πελάτη και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον εξυπηρετητή. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον εξυπηρετητή. Δηλαδή, προσποιείται στον πελάτη ότι είναι ο εξυπηρετητής και αντίστροφα.

Το SSL υποχρεώνει τον εξυπηρετητή να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη.

Το SSL στις Ηλεκτρονικές συναλλαγές.

Το πρωτόκολλο SSL μπορεί να χρησιμοποιείται για την εγκαθίδρυση ασφαλών συνδέσεων μεταξύ εξυπηρετουμένων (πελάτης) και εξυπηρετητών (έμπορας). Συγκεκριμένα μπορεί να χρησιμοποιείται για να αυθεντικοποιεί έναν εξυπηρετητή και προαιρετικά τον εξυπηρετούμενο, να εκτελεί ανταλλαγή κλειδιών και να παρέχει αυθεντικοποίηση και ακεραιότητα μηνυμάτων σε εφαρμογές ηλεκτρονικού εμπορίου και γενικά σε εφαρμογές διαδικτύου. Για τους λόγους αυτούς το πρωτόκολλο SSL αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο.

Η μη διασφάλιση αυθεντικοποίησης εξυπηρετούμενου βοήθησε το πρωτόκολλο SSL να διαδοθεί σε περιβάλλοντα ηλεκτρονικού εμπορίου. Η υποστήριξη της αυθεντικοποίησης εξυπηρετούμενου απαιτεί ξεχωριστά δημόσια κλειδιά και πιστοποιητικά για κάθε εξυπηρετούμενο. Είναι λοιπόν φανερό ότι η αυθεντικοποίηση κάθε πελάτη στο ηλεκτρονικό εμπόριο είναι πρακτικά αδύνατη. Επίσης είναι πιο σημαντικό οι τελικοί καταναλωτές να μπορούν να ενημερώνονται σχετικά με την ταυτότητα των εμπόρων με τους οποίους συναλλάσσονται, παρά να απαιτείται ίδιος βαθμός ασφάλειας και από τους εμπόρους για τους καταναλωτές. Επιπλέον αφού ο αριθμός των εμπόρων-εξυπηρετητών διαδικτύου είναι πολύ μικρότερος από τον αριθμό των καταναλωτών-χρηστών, είναι ευκολότερο και πιο πρακτικό να εφοδιάζονται οι εξυπηρετητές με τα απαραίτητα δημόσια κλειδιά και πιστοποιητικά.

Σήμερα το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για Διαδίκτυο γενικά και το ηλεκτρονικό εμπόριο συγκεκριμένα. Αξίζει να σημειωθεί ότι αν όχι όλες, οι περισσότερες τράπεζες που προσφέρουν τις υπηρεσίες τους διαμέσου του διαδικτύου έχουν αναπτύξει την ασφάλεια των εφαρμογών ηλεκτρονικής τραπεζικής με βάση το πρωτόκολλο SSL.

Το πρωτόκολλο SSL χρησιμοποιείται συνήθως σε HTTP προϊόντα εξυπηρετητών και εξυπηρετούμενων. Για παράδειγμα, υπάρχουν αρκετοί HTTP εξυπηρετητές διαθέσιμοι οι οποίοι υποστηρίζουν το SSL. Από την πλευρά του εξυπηρετούμενου, σήμερα, οι περισσότεροι browsers ιστού υποστηρίζουν το SSL. Τα περισσότερα από αυτά τα προϊόντα υποστηρίζουν τον αλγόριθμο RC4 για κρυπτογράφηση και τα MD2 και MD5 για σύνοψη.

Μειονέκτημα της χρήσης του SSL αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του browser του εξυπηρετούμενου με τον HTTPS εξυπηρετητή. Η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίηση της SSL συνόδου. Πρακτικά οι χρήστες αντιλαμβάνονται λίγα δευτερόλεπτα καθυστέρηση μεταξύ της έναρξης σύνδεσης με τον HTTPS εξυπηρετητή και της ανάκτησης της πρώτης HTML σελίδας από αυτόν.

4.4 Transport Layer Security Protocol, TLS

Το Μάιο του 1996 το IETF δημιούργησε το πρωτόκολλο Transport Layer Security TLS WG για την ασφάλεια του επιπέδου μεταφοράς. Το Δεκέμβριο του 1996 ένα πρώτο έγγραφο TLS 1.0 κυκλοφόρησε ως Internet Draft. Το έγγραφο ήταν ουσιαστικά το ίδιο με τις προδιαγραφές του SSL 3.0. Γενικά η ομάδα εργασίας για τη δημιουργία του TLS είχε σαν στρατηγική της οι προδιαγραφές του TLS 1.0 να βασίζονται κυρίως στο SSL 3.0, παρά σε άλλα πρωτόκολλα ασφάλειας επιπέδου μεταφοράς όπως SSL 2.0. Πρόσφατα, το Δεκέμβριο του 2005, η ομάδα εργασίας TLS group δημοσίευσε την έκδοση 1.1 του TLS.

Στο TLS 1.0 ενσωματώθηκε το SSL 3.0 με κάποιες μικρές τροποποιήσεις. Οι τροποποιήσεις αυτές αφορούσαν περισσότερο σημεία αποσαφήνισης. Η κύρια τροποποίηση που υποδείχθηκε για το SSL 3.0 ώστε να ενσωματωθεί στο TLS 1.0 είναι:

Το TLS record protocol και το TLS handshake protocol θα έπρεπε να διαχωρίζονται εντελώς και να καθορίζονται σαφώς σε σχετικά έγγραφα.

Οι διαφορές μεταξύ του TLS 1.0 και του SSL 3.0 δεν είναι ιδιαίτερα σημαντικές, αλλά είναι αρκετά κρίσιμες ώστε τα TLS 1.0 και SSL 3.0 να μη συνεργάζονται

εύκολα. Ωστόσο το TLS 1.0 ενσωματώνει ένα μηχανισμό μέσω του οποίου μια υλοποίηση TLS μπορεί να γίνει συμβατή με το SSL 3.0.

Το πρωτόκολλο TLS είναι από μόνο του ένα στρωματοποιημένο πρωτόκολλο. Στο χαμηλότερο επίπεδο, το TLS record protocol λαμβάνει τα προς μετάδοση μηνύματα, κατακερματίζει τα δεδομένα σε διαχειρίσιμα τμήματα, προαιρετικά τα συμπιέζει, υπολογίζει και προσαρτά ένα MAC σε κάθε τμήμα, κρυπτογραφεί το αποτέλεσμα και το αποστέλλει. Επιπλέον το πρωτόκολλο αυτό εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το TLS record protocol όταν λάβει ένα πακέτο το αποκρυπτογραφεί, το επιβεβαιώνει, το αποσυμπιέζει, και το επανασυναρμολογεί πριν το μεταδώσει. Μια κατάσταση TLS σύνδεσης αποτελεί το λειτουργικό περιβάλλον του TLS record protocol. Αυτή καθορίζει τους αλγόριθμους συμπίεσης, κρυπτογράφησης και αυθεντικοποίησης μηνυμάτων, καθώς και τα κλειδιά που χρησιμοποιούνται για κρυπτογράφηση και αυθεντικοποίηση. Η σύνδεση αυτή (σύνδεση TLS), δημιουργείται κατά την εκτέλεση του TLS handshake protocol.

Στο υψηλότερο επίπεδο, το TLS handshake protocol χρησιμοποιείται για να συμφωνηθεί μια κατάσταση συνόδου μεταξύ του εξυπηρετητή και του εξυπηρετούμενου (πελάτη). Συγκεκριμένα προσδιορίζεται μια ταυτότητα συνόδου, μια προδιαγραφή κρυπτογραφίας, μια μέθοδος συμπίεσης και ένα κύριο κλειδί. Τα στοιχεία αυτά χρησιμοποιούνται για τη δημιουργία παραμέτρων ασφάλειας που θα χρησιμοποιηθούν από το TLS record protocol κατά την προστασία δεδομένων εφαρμογών. Συγκεκριμένα το TLS handshake protocol αποτελείται από τρία υποπρωτόκολλα:

Το TLS change cipher spec protocol αποτελείται από ένα απλό μήνυμα Change_Cipher_Spec, το οποίο αποστέλλεται από τον πελάτη στον εξυπηρετητή κατά τη διάρκεια της χειραψίας, αφού έχουν συμφωνηθεί οι παράμετροι ασφάλειας.

Το TLS alert protocol χρησιμοποιείται για να αποστέλλει μηνύματα προειδοποίησης, τα οποία μεταβιβάζουν τη σημαντικότητα ενός μηνύματος προειδοποίησης και μια περιγραφή της προειδοποίησης αυτής. Οι προειδοποιήσεις είναι συνήθως μηνύματα προβλημάτων και λαθών που αφορούν κυρίως τη μετάδοση των μηνυμάτων.

Το TLS handshake protocol χρησιμοποιείται για να συμφωνηθεί μια κατάσταση συνόδου. Όταν ένας πελάτης και ένας εξυπηρετητής αρχίζουν για πρώτη φορά να επικοινωνούν επιλέγουν αλγόριθμους κρυπτογράφησης, προαιρετικά αυθεντικοποιούνται αμοιβαία και χρησιμοποιούν κρυπτογραφία δημοσίου κλειδιού για να παράγουν ένα κύριο μυστικό και τα αντίστοιχα κλειδιά συνόδου. Η ροή των μηνυμάτων που ο πελάτης και ο εξυπηρετητής ανταλλάσσουν μεταξύ τους είναι ουσιαστικά η ίδια, όπως του SSL handshake protocol.

Μετά την εκτέλεση του TLS handshake protocol ο πελάτης και ο εξυπηρετητής μπορούν να ανταλλάσσουν μηνύματα δεδομένων εφαρμογών με ασφάλεια. Τα μηνύματα αυτά μεταφέρονται μέσω του SSL Record protocol, αφού πρώτα κατακερματιστούν, συμπιεστούν, αυθεντικοποιηθούν και κρυπτογραφηθούν.

4.5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Για την αντιμετώπιση των πιθανών κινδύνων κάθε εταιρία ή οργανισμός θα πρέπει να καταρτίσει μια πολιτική ασφαλείας.

Με τον όρο πολιτική ασφαλείας εννοούμε ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μια εταιρεία ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του.

4.5.1 Περιεχόμενα πολιτικής ασφαλείας:

Το κείμενο της πολιτικής ασφαλείας θα πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμό που επιτρέπει την ανταλλαγή πληροφοριών.

Τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια.

Την επεξήγηση της πολιτικής ασφαλείας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει η εταιρεία ή οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.

Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.

Αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφαλείας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

4.5.2 Ζητήματα που αντιμετωπίζει:

Παρ'ότι οι πολιτικές ασφαλείας είναι γενικά υποκειμενικές και προσαρμόσιμες στις συγκεκριμένες ανάγκες και τους στόχους κάθε εταιρίας ή οργανισμού, υπάρχουν ορισμένα ζητήματα τα οποία είναι τόσο σημαντικά που θα πρέπει να αντιμετωπίζονται σε όλες τις πολιτικές ασφαλείας. Αυτά είναι:

Φυσική ασφάλεια:

Το μέγεθος της δικτυακής οντότητας μιας εταιρίας μπορεί να εκτείνεται από ένα κτίριο ή κτιριακό συγκρότημα μέχρι μια χώρα ή ολόκληρο τον κόσμο. Αυτό σημαίνει ότι η ασφάλεια του δικτύου έχει άμεση συνάρτηση με τη φυσική ασφάλεια. Χωρίς την εξασφάλιση της φυσικής ασφάλειας, οι βασικές απαιτήσεις για την ασφάλεια των πληροφοριών, δηλαδή η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα θα διατρέχουν σοβαρότατο κίνδυνο. Η ενότητα της πολιτικής ασφαλείας που αφορά τη φυσική ασφάλεια δηλώνει ρητά πώς θα προστατευθούν οι εγκαταστάσεις και ο υλικός εξοπλισμός της εταιρίας. Καθορίζει, επίσης, ποιοι εργαζόμενοι έχουν δικαίωμα πρόσβασης σε απαγορευμένες περιοχές, όπως είναι τα δωμάτια των servers ή οι αποθήκες των καλωδίων.

- Ασφάλεια δικτύου

Η ενότητα της ασφάλειας δικτύου δηλώνει τον τρόπο προστασίας των στοιχείων που αποθηκεύονται στο δίκτυο. Μπορεί επίσης να περιλαμβάνει μέτρα ασφάλειας σχετικά με τις τεχνολογίες προστασίας του δικτύου, όπως είναι τα firewalls και τα intrusion detection systems (συστήματα ανίχνευσης επιθέσεων).

- Έλεγχος πρόσβασης

Η ενότητα του ελέγχου πρόσβασης καθορίζει ποιος έχει πρόσβαση σε τι. Πρέπει να υπάρχει μια κατάλληλη διαδικασία που να εξασφαλίζει ότι μόνο οι αρμόδιοι για κάθε υπηρεσία ή πηγή πληροφοριών θα έχουν πρόσβαση σε αυτή. Ο έλεγχος πρόσβασης θα πρέπει να διευκολύνει τους διαχειριστές στη δουλειά τους και να είναι σχετικά εύκολος και κατανοητός ώστε να αποφεύγονται τα λάθη.

- Πιστοποίηση

Εκφράζει τον τρόπο που οι χρήστες πιστοποιούν την ταυτότητά τους στο δίκτυο. Ο τύπος της πιστοποίησης που χρησιμοποιείται ποικίλλει ανάλογα με τον τρόπο πρόσβασης των χρηστών στο δίκτυο. Για πρόσβαση από το γραφείο τους, ένα απλό όνομα χρήστη και ένας κωδικός είναι αρκετοί αφού ο έλεγχος πιστοποίησης

ενισχύεται από τη φυσική ασφάλεια. Για πρόσβαση όμως στο δίκτυο της εταιρίας μέσω του Internet μπορεί να χρειαστεί μια πιο περίπλοκη και ασφαλής πιστοποίηση.

- Συμμόρφωση

Η ενότητα της συμμόρφωσης επεξηγεί τον τρόπο εφαρμογής της πολιτικής ασφαλείας. Μπορεί επίσης να καθορίζει τις μεθόδους διερεύνησης τυχόν παραβιάσεων της πολιτικής καθώς επίσης και την επιβολή τιμών.

Σχέδιο για την αντιμετώπιση περιστατικών και εκτάκτων αναγκών:

Το σχέδιο αυτό εξηγεί τον τρόπο αντιμετώπισης κάθε είδους περιστατικού, από την επίθεση κακόβουλων χρηστών μέχρι μια φυσική καταστροφή. Μπορεί επίσης να απαριθμεί τα μέλη μιας ομάδας αντιμετώπισης έκτακτων περιστατικών που θα διαχειριστούν τέτοια περιστατικά.

Ασφάλεια λογισμικού:

Η ενότητα της ασφάλειας λογισμικού επεξηγεί τον τρόπο χρήσης του λογισμικού. Καθορίζει ποιοι έχουν το δικαίωμα να αγοράζουν και να εγκαθιστούν πακέτα λογισμικού στον υλικό εξοπλισμό της εταιρίας, καθώς επίσης και τα μέτρα ασφάλειας όσον αφορά τη λήψη λογισμικού από το Internet.

Προϋποθέσεις:

Εκτός από τα ζητήματα που αντιμετωπίζει, η πολιτική ασφαλείας έχει και κάποιες βασικές προϋποθέσεις που θα πρέπει να εκπληρώνονται ώστε να έχει το επιθυμητό αποτέλεσμα:

Απαιτεί συμμόρφωση από το προσωπικό του οργανισμού. Το έγγραφο της πολιτικής ασφαλείας θα πρέπει να είναι στη διάθεση όλου του προσωπικού.

Εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού.

Είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και εφαρμόσιμη από άποψη κόστους.

Είναι γενικεύσιμη ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού.

Είναι απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και εξειδικευμένες αναφορές ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές, καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στα εξής:

Στην οργανωτική δομή και στην κουλτούρα του οργανισμού

Στις απαιτήσεις ασφαλείας

Στις τεχνολογικές εξελίξεις

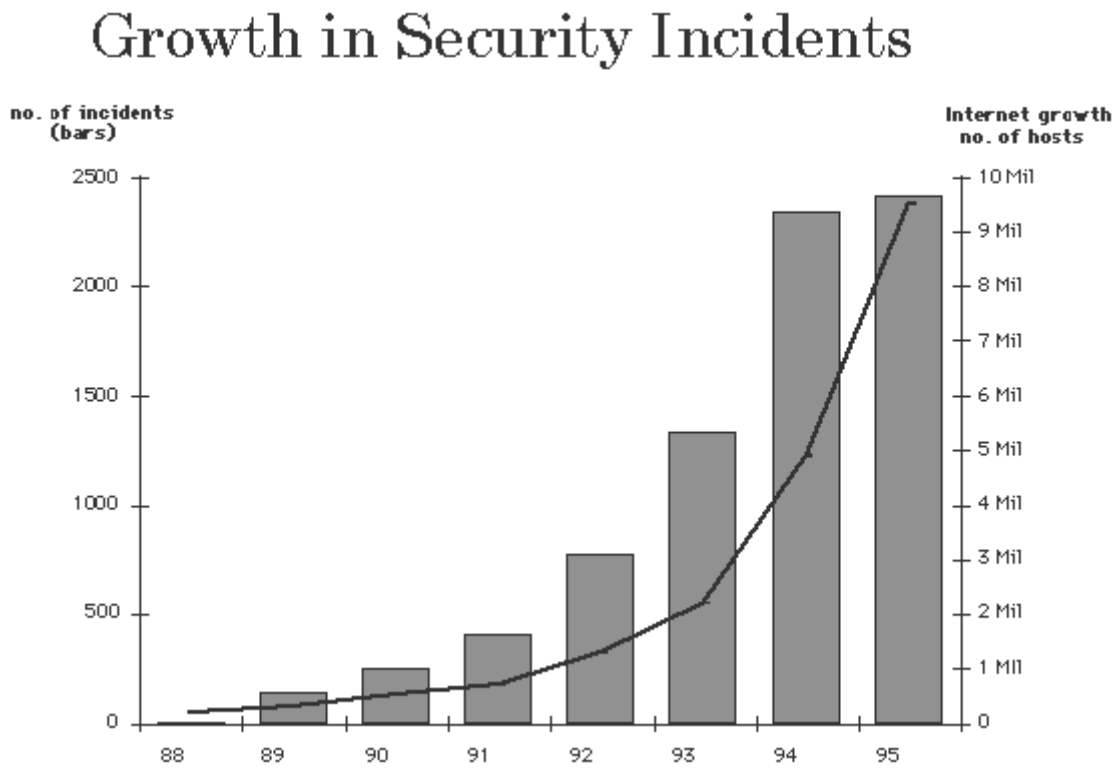
4.5.3 ΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΣΤΗ ΣΥΝΤΑΞΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ποίοι είναι αυτοί οι οποίοι εμπλέκονται στο δύσκολο έργο της σύνταξης της πολιτικής ασφαλείας μιας επιχείρησης; Ο υπεύθυνος ασφαλείας της επιχείρησης, οι υπεύθυνοι και οι διαχειριστές του δικτύου της εταιρίας, οι υπεύθυνοι των τμημάτων που επηρεάζονται άμεσα ή έμμεσα από την εφαρμογή της συγκεκριμένης πολιτικής ασφαλείας, οι υπεύθυνοι εφαρμογής αντιμέτρων σε περιπτώσεις παραβιάσεων, αντιπρόσωποι από την διοίκηση της επιχείρησης και φυσικά οι νομικοί σύμβουλοι.

ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΖΗΤΗΜΑΤΟΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Ειδικότερα στις Η.Π.Α., το ζήτημα της ασφάλειας έχει λάβει πολύ μεγάλες διαστάσεις τα τελευταία χρόνια. Από τη στιγμή μάλιστα που σχεδόν όλες οι μεγάλες εταιρείες και οργανισμοί δραστηριοποιούνται εμπορικά στο Internet είναι αναπόφευκτο το ζήτημα της ασφάλειας να αποτελεί μία από τις σημαντικότερες προτεραιότητές τους. Για το λόγο αυτό, όλες οι μεγάλες εταιρίες διαθέτουν ειδικό τμήμα ασφάλειας και προστασίας των δεδομένων στο οποίο επενδύουν ένα σεβαστό μέρος του προϋπολογισμού τους. Παράλληλα με τις κρατικές υπηρεσίες δραστηριοποιούνται και ανεξάρτητοι οργανισμοί όπως το Computer Security Institute

(CSI). Το ινστιτούτο αυτό, μάλιστα, διεξάγει από το 1995 μία ετήσια, εκτεταμένη έρευνα για την ασφάλεια και την αντιμετώπιση του ηλεκτρονικού εγκλήματος (Computer Crime and Security Survey) στην οποία παίρνουν μέρος πολλές από τις μεγαλύτερες επιχειρήσεις και οργανισμούς των Η.Π.Α.. Η έρευνα αυτή δείχνει την ολοένα αυξανόμενη χρήση του Internet για διαφημιστικούς σκοπούς και εμπορικές συναλλαγές, αλλά και την παράλληλη αύξηση των κρουσμάτων ηλεκτρονικών επιθέσεων που εκδηλώνονται με διάφορους τρόπους, από την παραποίηση ή καταστροφή του Web site της εταιρίας μέχρι την υποκλοπή προσωπικών δεδομένων και την οικονομική απάτη.



Σχήμα 4. 4 Ανάπτυξη περιστατικών ασφάλειας.

Το διάγραμμα περιγράφει την κατάσταση μέχρι και το 1995. Η κατάσταση δεν άλλαξε και πολύ τα επόμενα χρόνια, με τον αριθμό των περιστατικών παραβίασης ασφαλείας να αυξάνεται περίπου ανάλογα προς την αύξηση του μεγέθους των δικτύων υπολογιστών και κυρίως του Internet. Μάλιστα, η αύξηση των κρουσμάτων ήταν ιδιαίτερα σημαντική κατά το 2001 παρά τα γεγονότα της 11 Σεπτεμβρίου και τα πολύ αυστηρά μέτρα που τα ακολούθησαν (π.χ. Patriot Act). Το γεγονός αυτό καταδεικνύει την ανάγκη μεγαλύτερης συνειδητοποίησης σχετικά με τους κινδύνους που ελλοχεύουν στην ηλεκτρονική δραστηριότητα των εταιριών και της λήψης ουσιαστικότερων και αποτελεσματικότερων μέτρων για την αντιμετώπιση.

4.5.4 ΣΧΕΤΙΚΗ ΝΟΜΟΘΕΣΙΑ ΣΤΟΝ ΕΛΛΗΝΙΚΟ ΧΩΡΟ

Από όσα έχουν αναφερθεί γίνεται προφανές ότι η αναμενόμενη έκρηξη στη χρήση του Internet για την πραγματοποίηση εμπορικών συναλλαγών, που αναπόφευκτα θα συμβεί και στη χώρα μας, καθιστά το ζήτημα της ασφάλειας πολύ σημαντικό. Θα μπορούσαμε να πούμε ότι μόνο τα τελευταία χρόνια έχει αρχίσει μια προσπάθεια ενημέρωσης και ευαισθητοποίησης των πολιτών και των εταιριών σχετικά με ζητήματα ασφάλειας. Επιπλέον, έχει γίνει μια σημαντική εκστρατεία ενημέρωσης του κοινού σχετικά με ζητήματα προστασίας προσωπικών δεδομένων.

Πολύ σημαντικό ρόλο στο σημείο αυτό έχει παίξει ένας ανεξάρτητος διοικητικός φορέας, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr) που δραστηριοποιείται τα τελευταία χρόνια. Βασική αρμοδιότητα της Αρχής είναι η εποπτεία του νόμου 2472/1997 και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε ό,τι αφορά την ασφάλεια, η Αρχή έχει δημοσιεύσει ένα άρθρο σχετικά με το Ηλεκτρονικό Επιχειρείν και την προστασία των προσωπικών δεδομένων του πολίτη (www.dpa.gr/Documents/Gre/Com/article.doc , Κ. Μουλινός, Κ. Καμπουράκη, "E-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή", Αρχή Δεδομένων Προσωπικού Χαρακτήρα). Στο άρθρο αυτό καθορίζονται οι διακριτές περιπτώσεις στις οποίες καταγράφονται προσωπικά δεδομένα ενός χρήστη στο Διαδίκτυο, καθώς επίσης και τα μέτρα προστασίας που θα πρέπει να λαμβάνουν οι παροχείς Υπηρεσιών Διαδικτύου, οι παροχείς Τελικών Υπηρεσιών, δηλαδή οι φορείς που παρέχουν τη ζητούμενη από το χρήστη υπηρεσία στο Διαδίκτυο, και οι Έμπιστες Τρίτες Οντότητες.

Επιπλέον, πρωτοβουλίες σχετικά με την ασφάλεια λαμβάνονται και από το e-business forum (www.e-businessforum.gr). Πρόκειται για μια πρωτοβουλία της Γενικής Γραμματείας Βιομηχανίας του Υπουργείου Ανάπτυξης και αποτελεί έναν διαρκή μηχανισμό διαβούλευσης της Πολιτείας με τον επιχειρηματικό και ακαδημαϊκό κόσμο καθώς και τους κοινωνικούς και επαγγελματικούς φορείς, για την παραγωγή θέσεων και προτάσεων προς όλα τα ενδιαφερόμενα μέρη, με αντικείμενο την ανταγωνιστικότητα των επιχειρήσεων στη νέα ψηφιακή οικονομία και την ηλεκτρονική επιχειρηματικότητα.

Όσον αφορά το ζήτημα της ασφάλειας ιδιαίτερο ενδιαφέρον παρουσιάζει η ομάδα εργασίας Β1 του e-business forum, η οποία ασχολήθηκε με την ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων με στόχο την περιγραφή της σημερινής κατάστασης και την εξειδίκευση των αναγκαίων πρωτοβουλιών για την οικοδόμηση μέτρων εμπιστοσύνης και ασφάλειας σε περιβάλλον ηλεκτρονικού επιχειρείν (βλ. Τελικό Παραδοτέο Ομάδας Β1 του E-Business Forum, «Ασφάλεια

πληροφοριακών και επικοινωνιακών συστημάτων στο χώρο του ηλεκτρονικού επιχειρείν», Ιούλιος 2002, Αθήνα).

Εκτός από τον Ν. 2472/1997, άλλοι σημαντικοί νόμοι που ενισχύουν το νομοθετικό πλαίσιο που σχετίζεται με ζητήματα τηλεπικοινωνιακών δικτύων και της ασφάλειας που παρέχεται σε αυτά, είναι:

Ο νόμος 2867/19-12-2000, που σχετίζεται με την οργάνωση και λειτουργία των τηλεπικοινωνιακών φορέων.

Ο νόμος 2225/20-07-1994 περί προστασίας του απορρήτου των τηλεπικοινωνιών, ο οποίος όμως καθορίζει και τις περιπτώσεις άρσης του απορρήτου αυτού.

Ο νόμος 2774/22-12-1999, σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο συμμόρφωσης με την κοινοτική οδηγία 97/66. Σχετικά με την ασφάλεια, στο άρθρο 10 του παρόντος νόμου επισημαίνεται ότι ο φορέας παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του και εφόσον χρειάζεται από κοινού με το φορέα παροχής του δημοσίου δικτύου τηλεπικοινωνιών, καθώς και η ασφάλεια του δημόσιου τηλεπικοινωνιακού δικτύου.

Ο νόμος 2672/1998, σχετικά με τη διακίνηση εγγράφων με ηλεκτρονικά μέσα, ο οποίος καθορίζει τις προϋποθέσεις χρήσης και αποδοχής της διακίνησης εγγράφων μεταξύ υπηρεσιών του δημοσίου είτε μεταξύ αυτών και ιδιωτικών φορέων ή φυσικών προσώπων με τα παραπάνω μέσα (άρθρο 14). Επιπλέον στον νόμο 2672 είναι σημαντικό ότι γίνεται για πρώτη φορά αναφορά στις ψηφιακές υπογραφές και προβλέπεται ότι οι προϋποθέσεις και η διαδικασία έκδοσης, διακίνησης, διαχείρισης και διασφάλισής τους καθορίζονται με προεδρικό διάταγμα.

Το προεδρικό διάταγμα 150/2001, σχετικά με τις ηλεκτρονικές υπογραφές το οποίο προσαρμόζει την ελληνική νομοθεσία στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης στις 13/12/1999 "Σχετικά με το Κοινοτικό Πλαίσιο για τις Ηλεκτρονικές Υπογραφές". Στην οδηγία 99/93/ΕΚ διαμορφώνεται ένα ενιαίο για τον Κοινοτικό χώρο πλαίσιο αντιμετώπισης νομικών ζητημάτων, που προκύπτουν από τη χρήση της ηλεκτρονικής υπογραφής ως μεθόδου ηλεκτρονικής πιστοποίησης στοιχείων.

Το σχέδιο νόμου για την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών που ψηφίστηκε κατά τη συνεδρίαση της ολομέλειας της Βουλής στις 5 Φεβρουαρίου 2003 και αφορά τη θέσπιση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.). Η ισχύς του παρόντος νόμου θα αρχίσει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως.

Το γεγονός ότι οι νόμοι αυτοί ψηφίσθηκαν τα τελευταία χρόνια δείχνει πόσο ραγδαίες είναι οι εξελίξεις και η ανάγκη προσαρμογής της νομοθεσίας σε αυτές.

Εκτός από την ενίσχυση του νομοθετικού πλαισίου, το γεγονός ότι στο ζήτημα της ασφάλειας των δικτύων και των προσωπικών δεδομένων έχει υπάρξει τα τελευταία χρόνια μια σημαντική πρόοδος γίνεται εμφανές και από τη δραστηριοποίηση πολλών Ελληνικών εταιριών που παρέχουν σε εταιρίες και οργανισμούς υπηρεσίες και προϊόντα για την ασφάλεια των δικτύων τους και των δικτυακών τους τόπων στο Internet. Η ανάπτυξη των εταιριών αυτών τα τελευταία χρόνια είναι ραγδαία, κάτι που δείχνει τη συνεχή αύξηση εταιριών και οργανισμών για θέματα ασφάλειας.

Παράγοντες που επηρεάζουν την υποδομή ασφαλείας:

Προφανώς η συγκεκριμένη κατηγοριοποίηση δεν είναι απόλυτη και δεν μπορεί να περιγράψει το σύνολο των περιπτώσεων αφού υπάρχει ένα πλήθος παραμέτρων που επηρεάζουν την πολυπλοκότητα της υποδομής ασφαλείας μιας εταιρείας και κατά συνέπεια το συνολικό κόστος ενός περιστατικού παραβίασής της. Προσπαθώντας να συγκεκριμενοποιήσουμε αυτές τις παραμέτρους καταλήγουμε στα ακόλουθα:

Μέγεθος εταιρείας: Όπως είναι προφανές οι εταιρείες με μεγάλο αριθμό προσωπικού και σημαντικό κύκλο εργασιών είναι υποχρεωμένες να διαθέτουν πιο πολύπλοκα συστήματα ασφαλείας από ότι οι μικρές και μικρομεσαίες επιχειρήσεις καθώς ένα περιστατικό παραβίασης της ασφάλειας των συστημάτων τους θα έχει πολύ μεγαλύτερες επιπτώσεις τόσο στην υποδομή τους όσο και στο γόητρό τους.

Ύπαρξη ηλεκτρονικών συναλλαγών: Η επένδυση σε υποδομή ασφάλειας για μια εταιρεία που χρησιμοποιεί το Internet για την πραγματοποίηση ηλεκτρονικών συναλλαγών θα είναι πολύ μεγαλύτερη από ότι αν το χρησιμοποιούσε απλώς για διαφημιστικούς λόγους (π.χ. Web site). Αντίστοιχα και ο οικονομικός αντίκτυπος ενός περιστατικού παραβίασης της ασφάλειας θα είναι σημαντικά μεγαλύτερος.

Τομέας δραστηριοποίησης της εταιρείας: Όπως γίνεται αντιληπτό η σημασία της ασφάλειας είναι ιδιαίτερα αυξημένη για εταιρείες που δραστηριοποιούνται σε κρίσιμους τομείς, όπως είναι ο κλάδος της υγείας και ο τραπεζικός κλάδος.

Ποσοστοποίηση κόστους:

Το επόμενο βήμα μετά την κατηγοριοποίηση του κόστους είναι μία προσπάθεια ποσοστοποίησης των επιμέρους συνιστωσών του. Βέβαια, απόλυτη ποσοστοποίηση δεν μπορεί να γίνει, παρά μόνον μία ανάλυση που να προσεγγίζει την πραγματικότητα στην πλειοψηφία των περιπτώσεων. Με βάση τα στοιχεία που συλλέξαμε από τις απαντήσεις των ερωτηματολογίων και τη μελέτη της σχετικής

βιβλιογραφίας, καταλήξαμε στην παρακάτω ποσοστοποίηση των επιμέρους κλάδων του κόστους:

ΥΛΙΚΟ	30%
ΛΟΓΙΣΜΙΚΟ	10%
ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ	60%

Οι όροι Υλικό και Λογισμικό αναφέρονται τόσο στην υποδομή που θα πρέπει να υπάρχει προληπτικά στο δίκτυο της εταιρείας όσο και στο κόστος που προκύπτει από την αποκατάσταση του δικτύου και την αγορά νέου εξοπλισμού μετά την εκδήλωση μιας επίθεσης. Στο ανθρώπινο δυναμικό περιλαμβάνονται οι αμοιβές των εργαζομένων στο τμήμα της ασφάλειας, οι επιπλέον αμοιβές που μπορεί να χρειαστεί να καταβληθούν σε περίπτωση ενός περιστατικού καθώς και τα ενδεχόμενα έξοδα σε περίπτωση που για την επίλυση ενός προβλήματος επιλεγεί η λύση του outsourcing. Παρατηρούμε κατά συνέπεια ότι το ανθρώπινο δυναμικό αποτελεί τη μεγαλύτερη συνιστώσα του συνολικού κόστους.

Χρήση Κωδικών Ασφάλειας (Passwords):

Οι κωδικοί ασφάλειας αποτελούν ένα από τα σημαντικότερα πεδία της ασφάλειας των επικοινωνιών. Αποτελούν την τελευταία γραμμή άμυνας ενάντια σε εισβολείς.

Κάθε πάροχος διαδικτύου θα πρέπει να διαθέτει και να επιβάλλει κανόνες αναφορικά με τους κωδικούς ασφάλειας ούτως ώστε να δημιουργούνται συμπαγείς κωδικοί, οι οποίοι να προστατεύονται και να μεταβάλλονται συχνά.

Δημιουργία και Διαχείριση Κωδικών Ασφάλειας:

Προκειμένου οι χρήστες και οι χρήστες παρόχου να χρησιμοποιήσουν ένα εταιρικό δίκτυο ή υπολογιστικό σύστημα το οποίο προστατεύεται, θα πρέπει να διαθέτουν όνομα χρήστη (login name) και κατάλληλο κωδικό πρόσβασης (password).

Η πολιτική δημιουργίας και διαχείρισης κωδικών ασφάλειας θα πρέπει να πληροί τα ακόλουθα:

Ύπαρξη συμπαγών κωδικών ασφάλειας: οι χρησιμοποιούμενοι κωδικοί ασφάλειας πρέπει να είναι συμπαγείς και με ένα ικανό ελάχιστο μήκος, ώστε να μην μπορεί να τους «μαντέψει» κάποιος εισβολέας.

Περιορισμένη πρόσβαση στο αρχείο φύλαξης των κωδικών ασφάλειας: η πρόσβαση στο αρχείο που φυλάσσονται οι κωδικοί πρόσβασης πρέπει να είναι περιορισμένη.

Περιοδική αλλαγή των κωδικών ασφάλειας: η πολιτική πρέπει να μην ευνοεί την συνεχή χρήση του ιδίου κωδικού ασφάλειας. Πρέπει να επιβάλλεται στους χρήστες και στους χρήστες παρόχου να αλλάζουν σε τακτά χρονικά διαστήματα τους κωδικούς πρόσβασης τους.

Προστασία Κωδικών Ασφάλειας:

Οι υπεύθυνοι ασφάλειας του δικτύου ή του συστήματος θα πρέπει να δίνουν έμφαση στην ενημέρωση των χρηστών αναφορικά με την πολιτική προστασίας των κωδικών ασφάλειας.

Η πολιτική προστασίας των κωδικών ασφάλειας θα πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

Ο χρήστης και ο χρήστης παρόχου δε θα πρέπει να μοιράζεται τον κωδικό ασφαλείας του με άλλους χρήστες και χρήστες παρόχου, και δε θα πρέπει να αποκαλύπτει σε κανένα τον κωδικό ασφάλειας που του έχει δοθεί.

Ο χρήστης και ο χρήστης παρόχου δε θα πρέπει να αναφέρει τους κωδικούς ασφάλειας του σε τηλεφωνικές συνομιλίες, ούτε να τους περιλαμβάνει σε μηνύματα ηλεκτρονικού ταχυδρομείου.

Ο χρήστης και ο χρήστης παρόχου οφείλει να απομνημονεύει τον κωδικό ασφάλειας του, και σε περίπτωση που αυτό είναι αδύνατο, το μέσο καταγραφής του κωδικού ασφάλειας θα πρέπει να τοποθετείται σε προστατευμένο χώρο (π.χ. κλειδωμένα ντουλάπια).

Πολιτική Ασφάλειας Παρόχου Υπηρεσίας Εφαρμογής (Application Service Provider):

Η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής ορίζει το σύνολο των εγγυήσεων που οφείλει να λαμβάνει ο πάροχος διαδικτύου από τον πάροχο υπηρεσίας εφαρμογής, προκειμένου να εξασφαλιστεί το απόρρητο των επικοινωνιών των χρηστών.

Ο πάροχος διαδικτύου οφείλει να ελέγχει διεξοδικά κατά πόσο ο πάροχος υπηρεσίας εφαρμογής δύναται να εφαρμόσει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής πριν την ανάθεση της υπηρεσίας και κατά τη διάρκεια λειτουργίας της υπηρεσίας.

Ο πάροχος υπηρεσίας εφαρμογής οφείλει να καταθέσει στον πάροχο διαδικτύου το πλήρες διάγραμμα δικτύου που χρησιμοποιεί για την υποστήριξη της εν λόγω υπηρεσίας. Επίσης οφείλει να διακόπτει άμεσα τη λειτουργία της υπηρεσίας σε περίπτωση που εντοπιστεί οποιοδήποτε θέμα ασφάλειας των απόρρητων δεδομένων επικοινωνίας.

Ο πάροχος υπηρεσίας εφαρμογής υποχρεούται να χρησιμοποιεί διαδικασίες και μεθόδους κρυπτογράφησης των απόρρητων δεδομένων επικοινωνίας, και να εφαρμόζει την πολιτική κωδικών του παρόχου διαδικτύου ως προς τα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

4.5.5 Έλεγχος και Εποπτεία:

Οι πολιτικές και οι διαδικασίες που ορίστηκαν στον κανονισμό αυτό αποτελούν μέρος της γενικότερης Πολιτικής Ασφάλειας που ορίστηκε σε προηγούμενο Κανονισμό. Κατά συνέπεια η ΑΔΑΕ μπορεί ανά πάσα στιγμή να προβεί σε έλεγχο του καθορισμού, επιβολής και σωστής λειτουργίας των πολιτικών που ορίστηκαν στον παρόντα κανονισμό.

Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει:

Τεχνικές κρυπτογράφησης όπως αυτές δηλώνονται από τους παρόχους διαδικτύου. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να ζητήσει πλήρη ενημέρωση σχετικά με τις τεχνικές κρυπτογράφησης που χρησιμοποιεί ο πάροχος διαδικτύου στα συστήματα μετάδοσης.

Πολιτική προστασίας κωδικών.

Πολιτική προστασίας από ιούς και διαθέτει απαραίτητα συστήματα προστασίας από ιούς (ειδικό λογισμικό και δικτυακό εξοπλισμό).

Πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής.

Αρχές Πιστοποίησης:

Σκοπός των Αρχών Πιστοποίησης είναι να επαληθεύσουν την αντιστοιχία μιας οντότητας (π.χ. ενός φυσικού προσώπου) με το δημόσιο κλειδί της. Η επαλήθευση γίνεται με την έκδοση των ψηφιακών πιστοποιητικών.

Οι οργανισμοί που μπορούν να δραστηριοποιηθούν στη Ελλάδα ως Αρχές Πιστοποίησης είναι υπό τον έλεγχο της ΑΔΑΕ. Η ΑΔΑΕ θα επιβλέψει ότι η Αρχή Πιστοποίησης είναι σύμφωνη με την υπάρχουσα νομοθεσία.

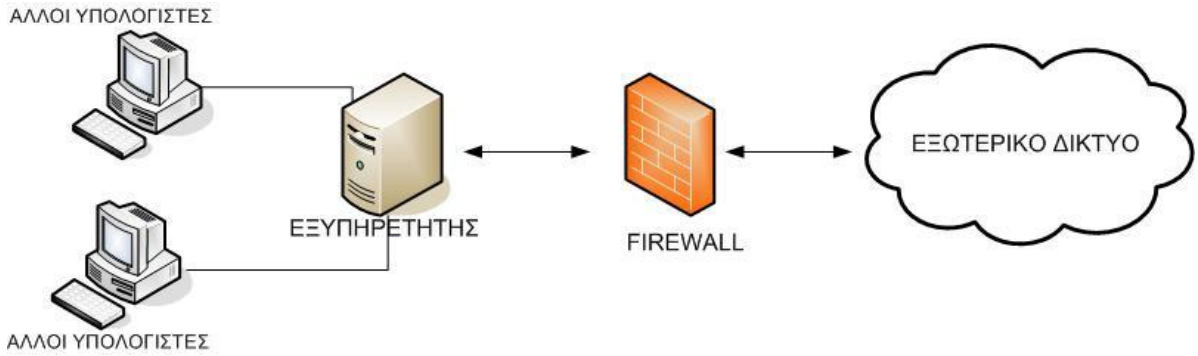
Στις συναλλαγές ηλεκτρονικού εμπορίου οι Αρχές Πιστοποίησης έχουν σημαντικό ρόλο, αφού πιστοποιούν την αυθεντικότητα των πελατών, όπως αναφέρεται στο κεφάλαιο 5. Συνεπώς η ΑΔΑΕ επιβλέπει έμμεσα τις ηλεκτρονικές συναλλαγές που πραγματοποιούνται, αφού ελέγχει τις Αρχές Πιστοποίησης, αλλά και άμεσα, αφού είναι στη δικαιοδοσία της ο έλεγχος κάθε οργανισμού ηλεκτρονικού εμπορίου.

Όλοι οι οργανισμοί που ασχολούνται με το ηλεκτρονικό εμπόριο στην Ελλάδα είναι υποχρεωμένοι να εφαρμόζουν τους κανόνες που ανακοινώνει η ΑΔΑΕ για τη διασφάλιση του απορρήτου των επικοινωνιών και των προσωπικών δεδομένων των πελατών τους.

4.6 Συστήματα Firewalls

Πολλά δίκτυα για να αυξήσουν την ασφάλεια των ιστοσελίδων τους χρησιμοποιούν firewalls. Τα firewalls είναι ισχυρά εργαλεία τα οποία όμως δεν υποκαθιστούν σε καμιά περίπτωση άλλα μέτρα ασφαλείας και για το λόγο αυτό χρησιμοποιούνται ως συμπληρωματικά αυτών. Συνήθως τοποθετούνται ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο ενός οργανισμού και παρέχουν έναν απλό τρόπο για να ελέγχουν την ποσότητα και το είδος των δεδομένων που διακινούνται μεταξύ των δύο δικτύων.

Αν το ζητούμενο αποτέλεσμα είναι η δημιουργία ενός εσωτερικού δικτυακού τόπου στο οποίο θα έχουν πρόσβαση μόνο οι χρήστες του τοπικού δικτύου, τότε ο εξυπηρετητής τοποθετείται μέσα στο firewall όπως φαίνεται στο **Error! Reference source not found.**.

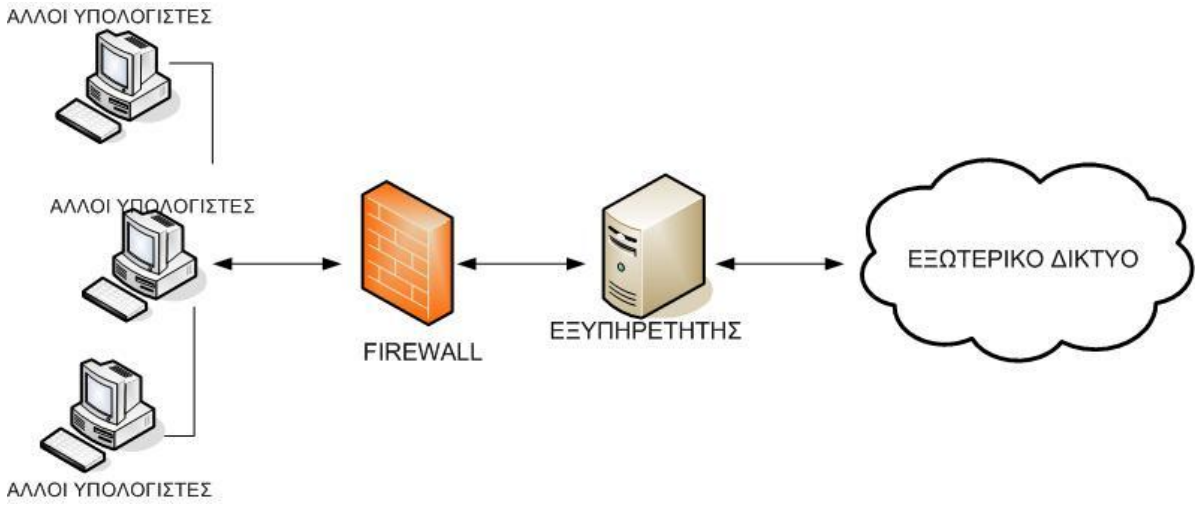


Σχήμα 4. 5 Εξυπηρετητής τοποθετημένος μέσα από το firewall.

Αν πάλι το ζητούμενο αποτέλεσμα είναι να είναι ο εξυπηρετητής διαθέσιμος στον έξω κόσμο, τότε θα πρέπει να τοποθετηθεί κάπου έξω από το firewall. Για την ασφάλεια και του τοπικού δικτύου θα πρέπει να τοποθετηθεί έξω και από την περιοχή του τοπικού δικτύου όπως φαίνεται στο **Error! Reference source not found.** .

Η τεχνική αυτή ονομάζεται "διαμόρφωση εξιλαστήριου θύματος" (sacrificial lamb configuration) διότι ο εξυπηρετητής πάντα κινδυνεύει να καταρρεύσει από επιθέσεις, αλλά με αυτόν τον τρόπο δε θα κινδυνεύει το εσωτερικό δίκτυο ακόμα και αν ο εξυπηρετητής καταρρεύσει. Βέβαια υπάρχουν αρχιτεκτονικές όπου χρησιμοποιούνται ζεύγη εξυπηρετητών (εσωτερικοί και εξωτερικοί) ώστε και στον έξω κόσμο να παρέχουν πληροφορίες και να επιτρέπουν μόνο στους εσωτερικούς χρήστες την πρόσβαση σε ιδιωτικά έγγραφα.

Εάν ο εξυπηρετητής βρίσκεται πίσω από το firewall, υπάρχει τρόπος ώστε να εξασφαλιστεί πρόσβαση στον έξω κόσμο. Με τον τρόπο αυτό, όμως, δημιουργούνται οπές στο φράγμα ασφάλειας. Είναι πολύ καλύτερα να χρησιμοποιηθεί ο εξυπηρετητής ως εξιλαστήριο θύμα. Υπάρχουν βέβαια και αρκετές αρχιτεκτονικές firewalls που δεν επιτρέπουν την τοποθέτηση εξυπηρετητών έξω από αυτούς. Σε αυτή την περίπτωση θα πρέπει αναγκαστικά ο εξυπηρετητής να βρίσκεται πίσω από το φράγμα ασφάλειας με δεδομένο πάντα το μειονέκτημα της πιθανής δημιουργίας οπών ασφάλειας.

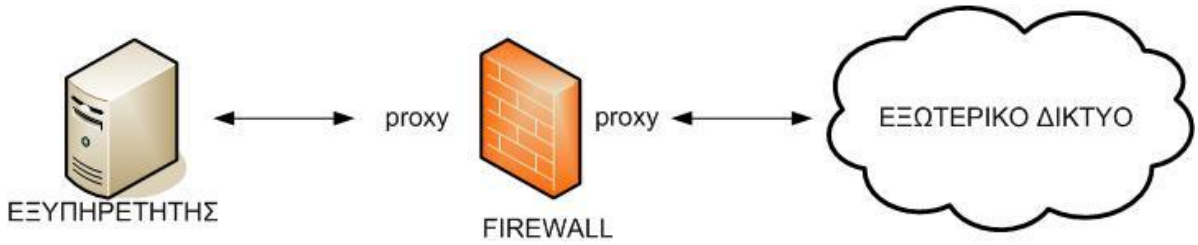


Σχήμα 4. 6 Εξυπηρετητής τοποθετημένος έξω από το firewall

Υπάρχουν δύο τρόποι για να επιτευχθεί η πρόσβαση του εξυπηρετητή, που βρίσκεται πίσω από το φράγμα ασφάλειας, με τον έξω κόσμο:

Στην περίπτωση που χρησιμοποιείται ο τύπος firewall υπολογιστή διαλογής (screened host), μπορεί να επιτραπεί η είσοδος για αιτήσεις (requests) από τη θύρα 80 (http service) η οποία επικοινωνεί με τον web εξυπηρετητή. Έτσι δημιουργείται μια μικρή οπή ασφάλειας απ' όπου ο έξω κόσμος επικοινωνεί με τον εξυπηρετητή.

Στην περίπτωση που χρησιμοποιείται ο τύπος διπλοσυνδεδεμένο firewall (dual homed gateway), χρειάζεται η εγκατάσταση proxy στο firewall. Ο proxy μπορεί να δει και από τις δύο πλευρές του φράγματος ασφάλειας, όπως φαίνεται στο **Error! Reference source not found.**. Έτσι, οι αιτήσεις για πληροφορίες σταματούν πάνω στον proxy ο οποίος τις προωθεί στον εξυπηρετητή και οι απαντήσεις από τον εξυπηρετητή σταματούν στον proxy ο οποίος τις προωθεί στον αιτούντα.



Σχήμα 4. 7 Πρόσβαση του εξυπηρετητή με τον έξω κόσμο.

4.6.1 Η Αναγκαιότητα Χρήσης των Firewalls

Σε ένα περιβάλλον χωρίς firewalls η δικτυακή ασφάλεια αποτελεί αποκλειστικά μέριμνα του κάθε σταθμού ξεχωριστά και όλοι οι σταθμοί πρέπει να συνεργάζονται ώστε να παρέχουν ένα ομοιόμορφα υψηλό επίπεδο ασφάλειας. Όσο πιο μεγάλο είναι το δίκτυο, τόσο πιο δύσκολα επιτυγχάνεται η διατήρηση όλων των σταθμών σε υψηλά επίπεδα ασφάλειας. Εξαιτίας της πολυπλοκότητας του δικτύου, τα λάθη και οι παραλήψεις στην ασφάλεια είναι συχνό φαινόμενο, με αποτέλεσμα να δημιουργούνται «οπές» ασφάλειας τις οποίες μπορούν να ανακαλύψουν και να εκμεταλλευτούν οι εισβολείς. Τα firewalls έχουν σχεδιαστεί έτσι ώστε να παρέχουν προηγμένες λειτουργίες παρακολούθησης και καταγραφής και η διαχείριση τους να είναι σχετικά εύκολή.

4.6.2 Επιθέσεις

Η πραγματοποίηση οποιασδήποτε από τις παραπάνω θεμελιώδεις απειλές, μπορεί να γίνει με μια από τις παρακάτω τεχνικές επίθεσης:

Denial of service attacks: Μια από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι με στόχο τη διακοπή παροχής υπηρεσιών από ένα δικτυακό κόμβο ή πληροφοριακό σύστημα είναι οι επιθέσεις τύπου Denial of service. Τα προγράμματα που συνήθως χρησιμοποιούν οι επιτιθέμενοι ακολουθούν την τακτική μαζικής αποστολής μηνυμάτων-αιτημάτων στο στόχο ώστε να προκαλέσουν την αποτυχία ανταπόκρισης του και την κατάρρευση του συστήματος.

Επιθέσεις μεταμφίεσης (Spoofing): Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» σε κάποιο νόμιμο χρήστη, ώστε να αποκτήσει πρόσβαση σε μια εφαρμογή. Δηλαδή ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι αποτέλεσμα των εξής: α) οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, β) οι κωδικοί πρόσβασης είτε διακινούνται

μέσω του δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση, και γ) οι χρήστες χρησιμοποιούν εύκολους κωδικούς.

E-mail Spoofing: Το e-mail spoofing αποτελεί πρακτική παραποίησης ή απόκρυψης της πραγματικής πηγής από την οποία προήρθε το μήνυμα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται συνήθως για να παραπλανήσει το χρήστη ώστε να συλλεχθούν από αυτόν χρήσιμα δεδομένα. Ενδεικτικά αποστέλλονται μηνύματα με υποτιθέμενο αποστολέα τον διαχειριστή του συστήματος, ζητώντας από το χρήστη να επιβεβαιώσει το password που χρησιμοποιεί.

Επιθέσεις παρακολούθησης (Sniffing): Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά συστημάτων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «προγράμματα sniffing». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Οι συσκευές με δυνατότητες sniffing μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών IDS (Intrusion Detection System). Συνεπώς τέτοιου είδους συσκευές είναι χρήσιμες και απαραίτητες. Ωστόσο, είναι προφανές ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις υπηρεσίες που προσφέρουν τα προγράμματα sniffing για την υλοποίηση των παράνομων δραστηριοτήτων τους. Υπάρχουν ειδικά προγράμματα sniffing, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση: α) password, β) στοιχείων οικονομικών συναλλαγών (π.χ. κωδικοί πιστωτικών καρτών), γ) εμπιστευτικών δεδομένων (π.χ. προσωπικά στοιχεία χρηστών, e-mail).

Ιοί (viruses) - σκουλήκια (worms): Οι ιοί είναι προγράμματα ή εντολές που προσαρτώνται σε προγράμματα ή δεδομένα και εκτελούνται παράλληλα με αυτά. Μπορούν να προκαλέσουν την αλλοίωση ή καταστροφή δεδομένων. Τα σκουλήκια αντίστοιχα, είναι προγράμματα που κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Και οι δύο κατηγορίες προγραμμάτων έχουν ως στόχο να πλήξουν το σύστημα στο οποίο εκτελούνται, προκαλώντας ζημιές όπως διαγραφή δεδομένων.

Buffer overflow attacks (υπερχείλιση καταχωρητή): Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο να πλήξουν τις εφαρμογές που αποθηκεύουν δεδομένα σε προσωρινό χώρο μνήμης (buffer) μέχρι να έρθει η ώρα τους για επεξεργασία. Οι επιτιθέμενοι βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της εφαρμογής με τις δικές τους εντολές. Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών, οι επιτιθέμενοι αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.

Cookie Poisoning: Τα Cookies είναι αρχεία υπολογιστών που αποθηκεύονται στον σκληρό δίσκο του υπολογιστή του πελάτη ή στην μνήμη cache, κατά την πρόσβαση του σε μια εφαρμογή διαδικτύου μέσω ενός browser. Αυτά τα αρχεία περιέχουν πληροφορίες όπως όνομα χρήστη, κωδικός πρόσβασης και στοιχεία συνόδου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες με σκοπό τη χρήση του υπολογιστή του πελάτη για κακόβουλες πράξεις. Τα Cookies χωρίζονται σε δύο κατηγορίες: αυτά που μένουν στον υπολογιστή του χρήστη μόνο κατά τη διάρκεια της επίσκεψης του χρήστη στην εφαρμογή διαδικτύου, και αυτά που έχουν ημερομηνία λήξης και παραμένουν στον σκληρό δίσκο του πελάτη μέχρι την ημερομηνία λήξης τους οπότε και διαγράφονται.

4.6.3 Μέσα Προστασίας

Ασφάλεια Δικτύου, Host και Εφαρμογής:

Ο σχεδιασμός και η ανάπτυξη ασφαλών web εφαρμογών προϋποθέτει ότι πρέπει να εφαρμοστεί ασφάλεια και στα τρία στρώματα: Δικτύου (Network), Host και Εφαρμογής (Application).

Ασφάλεια Δικτύου (Network)

Η ασφάλεια μιας web εφαρμογής στηρίζεται πάνω στην ασφαλή υποδομή του δικτύου. Η υποδομή του δικτύου αποτελείται από δρομολογητές (rooters), firewalls και διακόπτες (switches). Ο ρόλος της ασφάλειας δικτύου δεν είναι μόνο για την προστασία του από επιθέσεις βασισμένες στο πρωτόκολλο TCP/IP, αλλά και για την εφαρμογή αντίμετρων όπως ασφαλείς διεπαφές και ισχυροί κωδικοί πρόσβασης. Το ασφαλές δίκτυο είναι επίσης υπεύθυνο για τη διασφάλιση της ακεραιότητας των δεδομένων που διακινούνται μέσα από αυτό.

Τα firewalls μπλοκάρουν τα πρωτόκολλα και τις θύρες που δεν χρησιμοποιεί η εφαρμογή. Επιπλέον εξετάζουν τις επικοινωνίες και παρέχουν υψηλή ασφάλεια στο δίκτυο. Συγκεκριμένα με την εφαρμογή φιλτραρίσματος εμποδίζουν τις κακόβουλες επικοινωνίες. Τα firewalls αποτελούν αναπόσπαστο τμήμα της ασφάλειας, αλλά δεν αποτελούν πλήρη λύση από μόνα τους..

Ασφάλεια Host:

Η ασφάλεια web εφαρμογών προϋποθέτει πρώτα από όλα την ασφάλεια του εξυπηρετητή (server), είτε αυτός είναι εξυπηρετητής διαδικτύου (web server),

εξυπηρετητής εφαρμογής (application server) ή εξυπηρετητής βάσεων δεδομένων (database server).

Ακολούθως παρατίθενται τα μέτρα προστασίας που πρέπει να λαμβάνονται για την προστασία του εξυπηρετητή, και κατ'επέκταση των web εφαρμογών:

Patches and Updates: Πολλοί κίνδυνοι ασφάλειας υπάρχουν λόγω του ότι οι ευπάθειες είναι ευρέως γνωστές και διαδεδομένες. Όταν ανακαλύπτονται νέες ευπάθειες, συχνά ο εκμεταλλευόμενος κώδικας δημοσιεύεται στους πίνακες δελτίων του διαδικτύου μέσα σε λίγες ώρες από την πρώτη επιτυχημένη επίθεση. Η συχνή επιδιόρθωση (patching) και ενημέρωση (updating) του λογισμικού του εξυπηρετητή είναι το πρώτο βήμα για την εξασφάλιση της ασφάλειας στον εξυπηρετητή. Η χρήση των patches και updates στον εξυπηρετητή μειώνει τις ευκαιρίες για επίθεση τόσο των επιτιθέμενων όσο και του κακόβουλου κώδικα (malicious code).

Υπηρεσίες: Η απενεργοποίηση των περιττών και αχρησιμοποίητων υπηρεσιών μειώνει εύκολα και γρήγορα τη διαθέσιμη περιοχή για επιθέσεις (attach surface area).

Πρωτόκολλα: Η απενεργοποίηση των περιττών και αχρησιμοποίητων πρωτοκόλλων μειώνει επίσης τη διαθέσιμη περιοχή για επιθέσεις και τους ανοικτούς «δρόμους» που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να εισβάλουν στο σύστημα.

Accounts (Λογαριασμοί): Ο αριθμός των λογαριασμών που έχουν πρόσβαση στον εξυπηρετητή πρέπει να περιοριστεί στον ελάχιστο δυνατό. Επιπλέον θα πρέπει να επιβάλλονται κατάλληλες πολιτικές ασφάλειας των λογαριασμών όπως είναι η εξουσιοδότηση με ισχυρούς κωδικούς πρόσβασης.

Ports (Θύρες): Οι υπηρεσίες που τρέχουν σε έναν εξυπηρετητή ακούνε συγκεκριμένες θύρες προκειμένου να εξυπηρετήσουν τις εισερχόμενες αιτήσεις. Οι ανοικτές θύρες σε έναν εξυπηρετητή πρέπει να είναι γνωστές και να ελέγχονται συχνά ώστε καμιά επισφαλής υπηρεσία να μην ακούει.

Auditing and Logging (Έλεγχος και Καταγραφή): Ο έλεγχος είναι ζωτικής σημασίας στον προσδιορισμό εισβολέων ή επιθέσεων που βρίσκονται σε εξέλιξη. Η καταγραφή αποδεικνύεται ιδιαίτερα χρήσιμη, καθώς αποθηκεύονται πληροφορίες για τον τρόπο που εκτελέστηκε μια επίθεση οι οποίες μπορούν να χρησιμοποιηθούν για ενίσχυση των μέτρων προστασίας ενάντια σε παρόμοιου είδους επιθέσεις.

Ασφάλεια Εφαρμογής

Προκειμένου να εξασφαλιστεί η ασφάλεια των web εφαρμογών ακολουθούνται κάποιες βασικές διαδικασίες οι οποίες είναι οι εξής:

Επικύρωση δεδομένων εισόδου (Input Validation): Η επικύρωση δεδομένων εισόδου ασχολείται με το πως τα φίλτρα της εφαρμογής δέχονται κάποια δεδομένα εισόδου ως έγκυρα και ασφαλή και κάποια άλλα τα απορρίπτουν ως μη ασφαλή.

Αυθεντικοποίηση: Αυθεντικοποίηση είναι η διαδικασία κατά την οποία κάποια οντότητα αποδεικνύει την ταυτότητα κάποιας άλλης οντότητας, συνήθως με τη χρήση πιστοποιητικών.

Εξουσιοδότηση: Η εξουσιοδότηση αναφέρεται στον τρόπο με τον οποίο η εφαρμογή παρέχει έλεγχο πρόσβασης στις διαδικασίες.

Διαχείριση Διαμόρφωσης: Η διαχείριση διαμόρφωσης ασχολείται με το πως η εφαρμογή χειρίζεται κάποια λειτουργικά ζητήματα όπως είναι ποιες βάσεις δεδομένων ενώνονται με την εφαρμογή, ή με ποιο τρόπο η εφαρμογή διοικείται.

Ευαίσθητα Δεδομένα: Τα ευαίσθητα δεδομένα αναφέρονται στο πως η εφαρμογή χειρίζεται τα δεδομένα που πρέπει να προστατευτούν.

Διαχείριση Συνόδου: Μια σύνοδος αναφέρεται σε μια σειρά σχετικών αλληλεπιδράσεων μεταξύ του χρήστη και της web εφαρμογής. Η διαχείριση συνόδου ασχολείται με το πως η εφαρμογή χειρίζεται και προστατεύει αυτές τις αλληλεπιδράσεις.

Κρυπτογράφηση: Η κρυπτογράφηση αναφέρεται στο πως η εφαρμογή παρέχει εμπιστευτικότητα και ακεραιότητα.

Διαχείριση εξαιρέσεων: Η διαχείριση εξαιρέσεων ασχολείται με το τι κάνει η εφαρμογή σε περίπτωση που αποτύχει μια κλήση, δηλαδή αν επιστρέφει φιλικά μηνύματα προς τον χρήστη κλπ.

Έλεγχος και Καταγραφή: Ο έλεγχος και η καταγραφή αναφέρονται στο πως η εφαρμογή καταγράφει τα σχετικά με την ασφάλεια γεγονότα.

4.6.4 Αρχές Ασφάλειας

Οι βασικές αρχές ασφάλειας πρέπει να εφαρμόζονται σε κάθε είδους εφαρμογές, ανεξάρτητα από την τεχνολογία της κάθε εφαρμογής. Οποιοσδήποτε ασχολείται με την ασφάλεια των web εφαρμογών πρέπει να τηρεί τις παρακάτω βασικές αρχές ασφάλειας:

Ελάχιστα δυνατά προνόμια: Θα πρέπει να παραχωρούνται στους χρήστες ελάχιστα προνόμια και δικαιώματα πρόσβασης, ούτως ώστε οι επιτιθέμενοι να έχουν περιορισμένες ικανότητες σε περίπτωση που καταφέρουν να παραβιάσουν την ασφάλεια της εφαρμογής.

Έλεγχος εγκυρότητας εισαγόμενων δεδομένων: Τα δεδομένα τα οποία εισάγονται στην εφαρμογή από τους χρήστες αποτελούν δίοδο εχθρικού λογισμικού προς την εφαρμογή. Τα δεδομένα αυτά αποτελούν το αρχικό όπλο του επιτιθέμενου στην προσπάθεια του να εισβάλει στην εφαρμογή. Τα εισερχόμενα προς την εφαρμογή δεδομένα θα πρέπει να ελέγχονται. Η πιο ασφαλής τακτική ελέγχου είναι να θεωρούνται όλα τα δεδομένα εισαγωγής κακόβουλα μέχρι να αποδειχθεί το αντίθετο και να γίνεται έλεγχος επικύρωσης όλων των δεδομένων, ώστε η εφαρμογή να αποδέχεται μόνο ασφαλή δεδομένα και να απορρίπτει τα υπόλοιπα.

Έλεγχος στην πύλη: Όλοι οι επισκέπτες θα πρέπει να αυθεντικοποιούνται κατά την είσοδο τους στο σύστημα.

Αποτυχία με ασφάλεια: Σε περίπτωση που αποτύχει η εφαρμογή τα ευαίσθητα δεδομένα δεν θα πρέπει να παραμένουν προσιτά σε τρίτους. Θα πρέπει να επιστρέφονται φιλικά μηνύματα σφάλματος στους χρήστες τα οποία να μην εκθέτουν τις εσωτερικές λεπτομέρειες του συστήματος και γενικά να μην περιλαμβάνουν λεπτομέρειες που θα μπορούσαν να βοηθήσουν τους επιτιθέμενους να εκμεταλλευτούν τις ευπάθειες τις εφαρμογής.

Δημιουργία ασφαλών προεπιλογών: Οι λογαριασμοί προεπιλογής (default account) θα πρέπει εξ ορισμού να είναι εκτός λειτουργίας και σε περίπτωση ανάγκης να επιτρέπεται ρητά η χρήση τους. Όταν εμφανίζεται ένα λάθος θα πρέπει τα ευαίσθητα δεδομένα να μην διαρρέουν πίσω στον χρήστη ο οποίος ενδεχομένως θα μπορεί να τα χρησιμοποιήσει ενάντια στο σύστημα.

Μείωση περιοχής επιθέσεων: Θα πρέπει να μειώνεται η διαθέσιμη περιοχή για επιθέσεις. Αυτό μπορεί να γίνει θέτοντας εκτός λειτουργίας ή αφαιρώντας αχρησιμοποίητες συσκευές και πρωτόκολλα.

4.6.5 Πλάνο Ασφάλειας

Οι υπεύθυνοι για την ασφάλεια web εφαρμογών θα πρέπει να συντάσσουν ένα αναλυτικό πλάνο ασφάλειας το οποίο να ικανοποιεί όλες τις απαιτήσεις ασφάλειας. Κάθε οργανισμός ηλεκτρονικού εμπορίου θα πρέπει να ακολουθεί ένα πλάνο ασφάλειας για την ορθή και ασφαλή λειτουργία του. Σύμφωνα με τους κανονισμούς της ΑΔΑΕ, οι υπεύθυνοι για την δημιουργία ενός πλάνου ασφάλειας θα πρέπει να λαμβάνουν υπόψη τα εξής:

Αναγνώριση και έλεγχος αυθεντικότητας

Αναγνωριστικά χρηστών: Με τη βοήθεια των αναγνωριστικών εξασφαλίζεται η ταυτοποίηση κάθε χρήστη.

Επιλογή κωδικών πρόσβασης: Οι κωδικοί πρόσβασης (passwords) που υιοθετούν οι χρήστες πρέπει να έχουν αρκετό μήκος και να επιλέγονται με τέτοιο τρόπο, ώστε να είναι δύσκολο για κάποιον εισβολέα να τους μαντέψει.

Αποθήκευση κωδικών πρόσβασης: Οι κωδικοί πρόσβασης των χρηστών θα πρέπει να αποθηκεύονται σε κατάλληλη μορφή, ώστε κανείς, ακόμα και ο διαχειριστής του συστήματος να μην μπορεί να τους διαβάσει.

Συχνότητα αλλαγής κωδικών πρόσβασης: Οι κωδικοί πρόσβασης πρέπει να αλλάζουν αρκετά συχνά, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.

Έλεγχος πρόσβασης

Δικαιώματα πρόσβασης: Για κάθε νέο λογαριασμό χρήστη θα πρέπει να καθορίζονται τα δικαιώματα πρόσβασης στους πόρους του συστήματος.

Αδρανής σταθμός εργασίας: Οι σταθμοί εργασίας θα πρέπει να κλειδώνονται όταν μένουν αδρανείς για κάποιο χρονικό διάστημα, ώστε να περιοριστεί η πιθανότητα ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση.

Διαχείριση δικαιωμάτων: Κατάλληλος μηχανισμός επιτρέπει την πρόσβαση σε ιδιαίτερες λειτουργίες του συστήματος μόνο σε χρήστες που πρέπει να έχουν πρόσβαση σε αυτές.

Ασφάλεια του λογισμικού εφαρμογών: Η πρόσβαση στα αρχεία του λογισμικού εφαρμογών θα πρέπει να ελέγχεται με τη βοήθεια κατάλληλων προγραμμάτων.

Απόδοση ευθυνών

Καταγραφή γεγονότων: Πρόκειται για την καταγραφή όλων των περιστατικών που λαμβάνουν χώρα στο σύστημα κάθε χρονική στιγμή, ώστε κάθε επεισόδιο να μπορεί να διερευνηθεί και να αποδοθούν ευθύνες.

Διατήρηση των αρχείων καταγραφής γεγονότων: Θα πρέπει να διατηρείται κατάλληλο αρχείο καταγραφής γεγονότων για αρκετό χρονικό διάστημα.

Διερεύνηση επεισοδίων: Όταν κάποια επεισόδια ανιχνεύονται ή υπάρχουν υποψίες για αυτά, πρέπει να διερευνούνται σε βάθος.

Προστασία από ιούς

Πρόληψη και αποτροπή: Θα πρέπει να ελαχιστοποιηθεί η πιθανότητα να προσβληθεί το σύστημα από ιούς οποιασδήποτε μορφής.

Ανίχνευση: Το σύστημα θα πρέπει να περιλαμβάνει μηχανισμούς περιοδικού ελέγχου για ιούς.

Αντιμετώπιση: Θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί απομόνωσης και καταστροφής ιών.

Διαχείριση ασφάλειας δικτύου

Παρακολούθηση του δικτύου: Η κατάσταση του δικτύου θα πρέπει να παρακολουθείται, ώστε να διευκολύνεται η έγκαιρη ανίχνευση των προβλημάτων.

Εμπιστευτικότητα δεδομένων στο δίκτυο: Η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω δικτύου θα πρέπει να προστατεύεται.

Έλεγχος πρόσβασης μέσω δικτύου

Απομακρυσμένη πρόσβαση σε μη ενεργές θύρες: Μόνο οι θύρες (ports) που χρησιμοποιούνται θα πρέπει να είναι ενεργές και οι υπόλοιπες πρέπει να είναι κλειδωμένες.

Firewalls: Τα δίκτυα πρέπει να προστατεύονται μέσω των φραγμάτων ασφαλείας.

Διαχείριση συστήματος

Διαδικασίες: Δημιουργία εγγράφου στο οποίο θα καθορίζονται αναλυτικά οι διαδικασίες εκτέλεσης των σημαντικότερων εργασιών.

Έλεγχος πρόσβασης στο λογαριασμό του διαχειριστή του συστήματος: Ο λογαριασμός του διαχειριστή συστήματος είναι ο πιο προνομιούχος λογαριασμός στο σύστημα και για αυτό η χρήση του θα πρέπει να ελέγχεται.

Σχέδιο συνέχειας

Αποκατάσταση λειτουργίας: Ο υπεύθυνος ασφάλειας θα πρέπει να καταρτίσει σχέδιο συνέχειας για περιπτώσεις αντιμετώπισης έκτακτων περιστατικών και διαδικασιών ανάνηψης. Οι υπολογιστές του συστήματος και οι υπηρεσίες δικτύου θα πρέπει να είναι διαθέσιμες όταν χρειάζονται.

Εφεδρικά αντίγραφα: Η ύπαρξη εφεδρικών αντιγράφων εξασφαλίζει τη συνεχή διαθεσιμότητα των δεδομένων.

4.7 Πύλες Εφαρμογών (Application Gateways)

Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή να υλοποιήσει μια αυστηρότερη πολιτική ασφάλειας. Στο μοντέλο πελάτη/εξυπηρετητή η πύλη εφαρμογών είναι μια ενδιάμεση διεργασία που τρέχει μεταξύ του πελάτη που ζητάει μια συγκεκριμένη υπηρεσία και του εξυπηρετητή που παρέχει αυτή την υπηρεσία. Δηλαδή η πύλη εφαρμογών λειτουργεί ως εξυπηρετητής από τη σκοπιά του πελάτη και ως πελάτης από τη σκοπιά του εξυπηρετητή. Μια πύλη εφαρμογών μπορεί να λειτουργεί είτε στο επίπεδο εφαρμογής είτε στο επίπεδο μεταφοράς του TCP/IP.

Αν η πύλη λειτουργεί στο επίπεδο εφαρμογής ονομάζεται πύλη επιπέδου εφαρμογής (application-level gateway) ή απλά πύλη εφαρμογών. Αντίστοιχα αν η πύλη λειτουργεί στο επίπεδο μεταφοράς ονομάζεται πύλη επιπέδου κυκλώματος (circuit-level gateway).

Οι περισσότερες πύλες που χρησιμοποιούνται σε διατάξεις firewalls λειτουργούν στο επίπεδο εφαρμογής, είναι δηλαδή πληρεξούσιοι εξυπηρετητές (proxy servers).

Όταν ένας χρήστης που βρίσκεται στο εσωτερικό δίκτυο θέλει να επικοινωνήσει με μια υπηρεσία του εξωτερικού δικτύου, η πύλη εφαρμογών παρεμβάλλεται. Δηλαδή αντί ο χρήστης να επικοινωνήσει άμεσα με την υπηρεσία, επικοινωνεί με την πύλη εφαρμογών η οποία διαχειρίζεται παρασκηνιακά όλη τη μεταξύ τους επικοινωνία. Συγκεκριμένα όταν ένας πελάτης συνδέεται με την πύλη εφαρμογών χρησιμοποιώντας ένα από τα πρωτόκολλα εφαρμογής του TCP/IP, όπως το Telnet ή το FTP, η πύλη του ζητά πληροφορίες όπως ένα όνομα εισόδου (login) και ένα κωδικό πρόσβασης (password) για την πιστοποίηση της ταυτότητας του. Αν η πύλη αναγνωρίσει και δεχτεί το χρήστη, ο χρήστης της δίνει το όνομα του απομακρυσμένου συστήματος (υπηρεσία) που επιθυμεί να προσπελάσει, η πύλη εφαρμογών συνδέεται για λογαριασμό του χρήστη με αυτό το απομακρυσμένο σύστημα και εγκαθιστά μια δευτερεύουσα σύνδεση. Στη συνέχεια μετάγει τα δεδομένα της εφαρμογής μεταξύ των δύο συνδέσεων.

Στην περίπτωση μιας πύλης εφαρμογών μπορεί η κίνηση δεδομένων να παρακολουθείται και επιπλέον να επιβληθούν εξειδικευμένοι περιορισμοί σχετικά με την κίνηση αυτών από και προς το ιδιωτικό δίκτυο με σκοπό να αποτραπεί η υποκλοπή πολύτιμων προγραμμάτων ή δεδομένων.

Σχήμα 4. 8 Τοποθέτηση μιας πύλης εφαρμογών μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου

Η πύλη εφαρμογών φιλοξενείται σε ένα υπολογιστή γενικού σκοπού, ο οποίος ονομάζεται Bastion host (ή υπολογιστής-οχυρό). Ο υπολογιστής-οχυρό απαιτείται να παρέχει μεγάλη ασφάλεια διότι αποτελεί το κύριο σημείο επικοινωνίας για τους χρήστες του εσωτερικού δικτύου. Επιπλέον επειδή ο υπολογιστής-οχυρό εκτίθεται σε άμεσες επιθέσεις από το διαδίκτυο θα πρέπει να είναι ρυθμισμένος με τέτοιο τρόπο ώστε να είναι ιδιαίτερα ασφαλής. Συνήθως το λειτουργικό σύστημα του bastion host είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητες του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται. Έτσι μειώνεται η πιθανότητα ύπαρξης τυχόν «οπών ασφαλείας» και συνεπώς ενισχύεται η ασφάλεια του bastion host.

4.7.1 Πληρεξούσιοι Εξυπηρετητές (Proxy Servers)

Μια πύλη επιπέδου εφαρμογής που τρέχει σε ένα υπολογιστή-οχυρό συνήθως στεγάζει διάφορους proxy servers. Οι proxy servers χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Αν ένας χρήστης του ενδοεπιχειρησιακού δικτύου θέλει να έχει πρόσβαση σε ένα συγκεκριμένο εξυπηρετητή εφαρμογής TCP/IP στο διαδίκτυο, πρέπει η εφαρμογή του εξυπηρετούμενου να εγκαταστήσει μια σύνδεση με τον proxy server που τρέχει για αυτή τη συγκεκριμένη εφαρμογή στον υπολογιστή-οχυρό. Ο proxy server με τη σειρά του πρέπει να πιστοποιήσει την αυθεντικότητα του χρήστη και να τον εξουσιοδοτήσει για πρόσβαση.

Μπορούν να χρησιμοποιηθούν διάφορα σχήματα πιστοποίησης αυθεντικότητας και εξουσιοδότησης. Το απλούστερο σχήμα είναι ο proxy server να κρατά μια λίστα με διευθύνσεις IP που επιτρέπεται να συνδεθούν σε εξωτερικούς εξυπηρετητές εφαρμογών. Αυτό το σχήμα δεν είναι πολύ ασφαλές, αφού οποιοσδήποτε μπορεί να

προσποιηθεί ότι έχει εξουσιοδοτημένη διεύθυνση IP. Ένα πιο ασφαλές σχήμα είναι η χρήση ισχυρών μηχανισμών πιστοποίησης αυθεντικότητας μεταξύ του χρήστη και του proxy server.

Μετά την επιτυχή πιστοποίηση αυθεντικότητας και εξουσιοδότηση του χρήστη, ο proxy server εγκαθιστά μια δεύτερη σύνδεση TCP/IP με τον εξυπηρετητή της εφαρμογής που ζητήθηκε. Ο εξυπηρετητής της εφαρμογής μπορεί να θέλει και αυτός με τη σειρά του να πιστοποιήσει την αυθεντικότητα του χρήστη. Αν και εδώ πιστοποιηθεί επιτυχώς η αυθεντικότητα του χρήστη και εξουσιοδοτηθεί, ο εξυπηρετητής της εφαρμογής αρχίζει να εξυπηρετεί την αίτηση. Από τη στιγμή αυτή και μετά ο proxy server απλά μετάγει δεδομένα εφαρμογής μεταξύ των δύο συνδέσεων. Για κάθε πακέτο που ρέει από τον εσωτερικό εξυπηρετούμενο στον εξωτερικό εξυπηρετητή, ο proxy server συνήθως αντικαθιστά τη διεύθυνση IP του αποστολέα με τη δική του διεύθυνση. Έτσι οι εσωτερικές διευθύνσεις IP που χρησιμοποιούνται στο ενδοεπιχειρησιακό δίκτυο είναι ολοκληρωτικά κρυμμένες και δεν εκτίθενται στο διαδίκτυο.

4.7.2 Πλεονεκτήματα και Μειονεκτήματα Πυλών Εφαρμογών (και Proxy Servers)

Υπάρχουν αρκετά πλεονεκτήματα σχετικά με τη χρήση πυλών επιπέδου εφαρμογής γενικότερα και proxy servers ειδικότερα, μερικά από τα οποία είναι τα εξής:

Παρέχουν μεγαλύτερη ασφάλεια: Τα firewalls αυτού του τύπου έχουν τη δυνατότητα προσθήκης μιας λίστας ελέγχου προσπέλασης για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης προτού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες.

Επιπλέον τα συστήματα αυτού του τύπου παρέχουν μεγαλύτερη ασφάλεια αφού «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxy server εμποδίζοντας έτσι την απευθείας σύνδεση.

Υπάρχουν κάποιοι «έξυπνοι» proxy servers που λέγονται Application Layer Gateways (ALGs), οι οποίοι μπορούν να μπλοκάρουν συγκεκριμένα τμήματα ενός πρωτοκόλλου. Για παράδειγμα ένας (ALGs) για FTP μπορεί να διαχωρίζει την εντολή "put" από την εντολή "get". Έτσι ένας οργανισμός μπορεί να επιτρέπει στους χρήστες του να «κατεβάζουν» αρχεία αλλά να μην αφήνει τους έξω να παίρνουν τα αρχεία των δικών του συστημάτων.

Παρέχουν καλύτερη καταγραφή συμβάντων: Ένα βασικό χαρακτηριστικό των firewalls αυτής της κατηγορίας είναι ο on-line έλεγχος, ο οποίος επιτρέπει την παρακολούθηση της δραστηριότητας και την καταγραφή συγκεκριμένων γεγονότων.

Τα firewalls επιπέδου εφαρμογής έχουν ορισμένα μειονεκτήματα:

Ένα firewall επιπέδου εφαρμογής απαιτεί ένα ξεχωριστό proxy server για κάθε υπηρεσία δικτύου: Οι πύλες επιπέδου εφαρμογής επιτρέπουν μόνο εκείνα τα πρωτόκολλα και υπηρεσίες TCP/IP για τα οποία υπάρχει proxy server. Για παράδειγμα αν ένα firewall φιλοξενεί proxy servers για Telnet και FTP, τότε μόνο η κυκλοφορία Telnet και FTP επιτρέπεται, ενώ όλες οι άλλες υπηρεσίες παρεμποδίζονται. Εάν απαιτείται η υποστήριξη κάποιας άλλης υπηρεσίας από το firewall, είναι αναγκαίο να προστεθεί ένας νέος proxy server. Συνεπώς αν παρουσιαστεί μια νέα υπηρεσία στο Internet και το firewall δεν έχει τον αντίστοιχο proxy server, οι χρήστες του δικτύου δεν θα έχουν τη δυνατότητα πρόσβασης σε αυτή την υπηρεσία.

Δεν είναι πάντοτε διαφανή προς το χρήστη

Είναι δυσκολότερα στην υλοποίηση

Η ταχύτητα και η απόδοση των firewalls επιπέδου εφαρμογής δεν είναι τόσο ικανοποιητική όσο των firewalls επιπέδου δικτύου.

4.7.3 Υβριδικά Συστήματα Ασφάλειας

Συνήθως η κατασκευή ενός firewall δε στηρίζεται μόνο σε μια από τις αρχιτεκτονικές που αναφέρθηκαν πιο πάνω. Για την κατασκευή ενός firewall συνδυάζονται τα firewalls επιπέδου δικτύου (φίλτρα πακέτων, δρομολογητές διαλογής) και τα firewalls επιπέδου εφαρμογής (πύλες εφαρμογών, proxy servers). Τα συνδυασμένα firewalls που προκύπτουν ονομάζονται υβριδικά συστήματα ασφάλειας και οδηγούν στην επίλυση συνδυασμένων προβλημάτων. Τα προς επίλυση προβλήματα εξαρτώνται από τις υπηρεσίες τις οποίες θέλει να προσφέρει ένας οργανισμός στους χρήστες, καθώς και από το επίπεδο του κινδύνου που είναι διατεθειμένος να δεχτεί.

Σε ένα υβριδικό σύστημα ασφάλειας, τα λαμβανόμενα πακέτα υπόκεινται πρώτα στον έλεγχο τον οποίο διενεργεί το firewall επιπέδου δικτύου. Ακολούθως τα πακέτα είτε απορρίπτονται, είτε διέρχονται και κατευθύνονται προς τον προορισμό τους, είτε προωθούνται σε κάποιο proxy server για περαιτέρω επεξεργασία. Όταν το εσωτερικό δίκτυο ενός οργανισμού απαιτεί την ασφάλεια την οποία παρέχει ένα firewall επιπέδου εφαρμογής για ορισμένες υπηρεσίες και την ταχύτητα και ευελιξία ενός

firewall επιπέδου δικτύου για ορισμένες άλλες υπηρεσίες, τότε βέλτιστη λύση αποτελεί ένα υβριδικό σύστημα ασφάλειας.

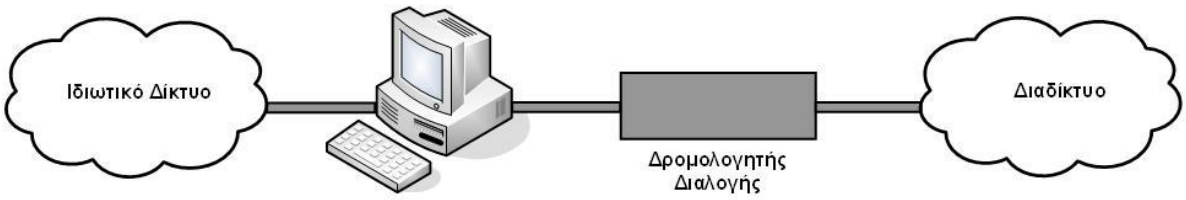
Ένα υβριδικό σύστημα ασφάλειας είναι σαφώς ακριβότερο, καθώς παρέχει μεγαλύτερη λειτουργικότητα και περισσότερα χαρακτηριστικά από ένα απλό firewall επιπέδου δικτύου.

Τα εξής υβριδικά συστήματα ασφάλειας εφαρμόζονται σήμερα ευρέως στο διαδίκτυο: Διπλοσυνδεδεμένα Φράγματα Ασφάλειας (Dual-Homed Firewalls), Φράγματα Ασφάλειας Υπολογιστή Διαλογής (Screened Host Firewalls), και Φράγματα Ασφάλειας Υποδικτύου Διαλογής (Screened Subnet Firewalls).

Διπλοσυνδεδεμένα Φράγματα Ασφαλείας (Dual-Homed Firewalls):

Τα διπλοσυνδεδεμένα firewalls αποτελούν καλύτερη εναλλακτική λύση σε σχέση με τα firewalls επιπέδου δικτύου, καθώς η πρόσβαση στο προστατευόμενο δίκτυο μπορεί να γίνει μόνο μέσω των proxy servers που τρέχουν στον υπολογιστή-οχυρό. Τα διπλοσυνδεδεμένα firewalls συνδυάζουν τόσο τα firewalls επιπέδου δικτύου, όσο και τα firewalls επιπέδου εφαρμογής, όπως κάθε υβριδικό σύστημα.

Ένα διπλοσυνδεδεμένο firewall αποτελείται από ένα υπολογιστή-οχυρό που είναι συνδεδεμένος και με τα δύο δίκτυα (ιδιωτικό δίκτυο και διαδίκτυο) και έχει απενεργοποιημένες τις δυνατότητες για προώθηση και δρομολόγηση IP. Αυτό σημαίνει ότι τα πακέτα IP από το ένα δίκτυο, το Internet, δε μπορούν να δρομολογηθούν άμεσα προς το εσωτερικό προστατευόμενο δίκτυο. Η IP κίνηση είναι πλήρως ελεγχόμενη, αφού τα συστήματα του εσωτερικού δικτύου και τα συστήματα του διαδικτύου δεν επιτρέπεται να επικοινωνήσουν άμεσα μεταξύ τους. Επιπλέον τοποθετείται και ένας δρομολογητής διαλογής μεταξύ του υπολογιστή-οχυρό και του διαδικτύου. Σκοπός του είναι να διασφαλίσει ότι κάθε πακέτο IP που φθάνει από το διαδίκτυο απευθύνεται με σωστό τρόπο στον υπολογιστή-οχυρό. Αν κάποιο πακέτο φθάνει με κάποια άλλη IP διεύθυνση προορισμού πρέπει να απορριφθεί.



Σχήμα 4. 9 Ένα διπλοσυνδεδεμένο firewall.

Για λόγους απόδοσης μπορούν να χρησιμοποιηθούν περισσότεροι του ενός υπολογιστές-οχυρά, όπου όλοι θα είναι συνδεδεμένοι και στο εσωτερικό και στο εξωτερικό δικτυακό τμήμα.

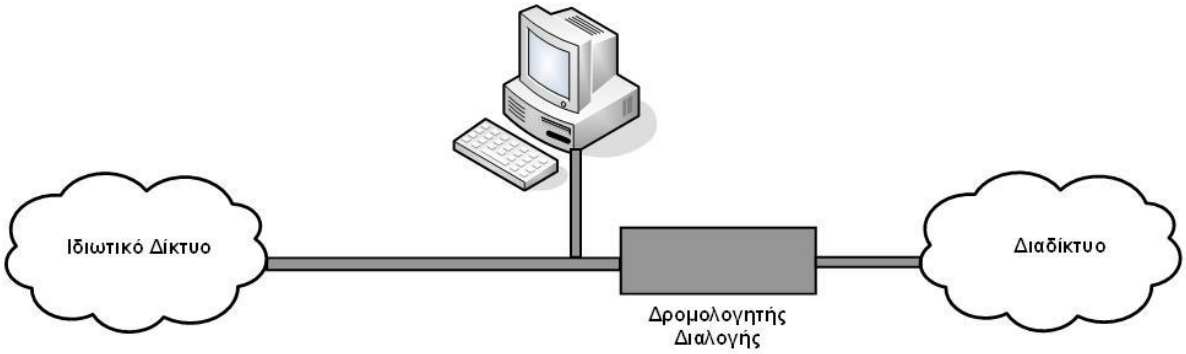
Το διπλοσυνδεδεμένο firewall είναι ένας απλός αλλά ασφαλής σχηματισμός. Η πρόσβαση στο ενδοεπιχειρησιακό δίκτυο μπορεί να περάσει μόνο από proxy servers που τρέχουν στον υπολογιστή-οχυρό. Έτσι καμιά υπηρεσία δεν περνά εκτός από αυτές για τις οποίες υπάρχουν proxy servers. Με τον τρόπο αυτό υλοποιείται η πολιτική σχεδιασμού όπου κάθε υπηρεσία απαγορεύεται εκτός και αν αυτή ρητά επιτρέπεται.

Το διπλοσυνδεδεμένο firewall έχει το μικρότερο κόστος από τις τρεις υβριδικές αρχιτεκτονικές που εξετάζονται, αλλά παρουσιάζει ένα σοβαρότατο μειονέκτημα: Αποτελεί μοναδικό σημείο δυνητικής αποτυχίας στο δίκτυο, συνεπώς αν ένας κακόβουλος επιτιθέμενος εισβάλει σε αυτό, τότε όλο το δίκτυο εκτίθεται σε κίνδυνο. Επιπλέον υπάρχουν και κάποια πρακτικά προβλήματα στη χρήση αυτού του μηχανισμού που σχετίζονται με το ότι δεν υπάρχουν proxy servers για ιδιόκτητα εταιρικά TCP/IP πρωτόκολλα εφαρμογής, όπως τα Lotus Notes, SQLnet και SAP.

Φράγματα Ασφάλειας Υπολογιστή Διαλογής (Screened Host Firewalls):

Ένα firewall υπολογιστή διαλογής παρέχει υπηρεσίες μέσω ενός υπολογιστή που είναι προσαρτημένος μόνο στο εσωτερικό δίκτυο. Στο σχηματισμό αυτό υπάρχει και ένας δρομολογητής διαλογής που συνδέει το εσωτερικό δίκτυο με το διαδίκτυο και πρέπει να είναι ρυθμισμένος έτσι ώστε να στέλνει όλη την κυκλοφορία IP που προέρχεται από το διαδίκτυο στην πύλη εφαρμογών που τρέχει στον υπολογιστή-οχυρό. Πριν όμως προωθήσει την κυκλοφορία IP σε αυτόν τον υπολογιστή, ο δρομολογητής διαλογής πρέπει να εφαρμόσει τους κανόνες φίλτρου πακέτων του. Μόνο η πληροφορία που είναι συμβατή με τους κανόνες διοχετεύεται στον υπολογιστή-οχυρό, ενώ όλη η άλλη πληροφορία απορρίπτεται. Συνεπώς οι πίνακες δρομολόγησης του δρομολογητή διαλογής πρέπει να προστατεύονται ισχυρά από εισβολή, διότι αν μια καταχώρηση στον πίνακα αλλάξει έτσι ώστε η κυκλοφορία να μην προωθείται στον υπολογιστή-οχυρό αλλά να στέλνεται απευθείας στο εσωτερικό δίκτυο, το firewall «αστοχεί».

Στο Σχήμα παρουσιάζεται ο σχηματισμός ενός firewall υπολογιστή διαλογής.



Σχήμα 4. 10 Ένας σχηματισμός firewall υπολογιστή διαλογής.

Ο μηχανισμός firewall υπολογιστή διαλογής είναι πιο ευέλικτος. Επιτρέπει στο δρομολογητή διαλογής να «περνάει» ορισμένες αξιόπιστες υπηρεσίες κατευθείαν στο εσωτερικό δίκτυο. Οπότε έχει τη δυνατότητα να επιτρέπει και στις υπηρεσίες για τις οποίες δεν υπάρχουν proxy servers, να περνάνε στο εσωτερικό δίκτυο, κάτι το οποίο δεν μπορούσε να πραγματοποιήσει αρχιτεκτονική διπλοσυνδεδεμένων firewalls.

Επειδή η αρχιτεκτονική αυτή επιτρέπει και τη μεταφορά πακέτων από το Internet κατευθείαν στο εσωτερικό δίκτυο, ίσως φαίνεται πιο επικίνδυνη από την αρχιτεκτονική διπλοσυνδεδεμένων firewalls, η οποία δεν επιτρέπει σε κανένα πακέτο να περάσει απευθείας από το Internet στο εσωτερικό δίκτυο. Πρακτικά όμως η αρχιτεκτονική διπλοσυνδεδεμένων firewalls είναι επιρρεπής σε ενδεχόμενες αποτυχίες οι οποίες θα έχουν ως αποτέλεσμα τη μεταφορά πακέτων από το εξωτερικό προς το εσωτερικό δίκτυο. Από την άλλη πλευρά είναι ευκολότερο να αμυνθεί κανείς με τη χρήση ενός δρομολογητή ο οποίος παρέχει ένα περιορισμένο σύνολο υπηρεσιών, παρά με τη χρήση ενός υπολογιστή. Στις περισσότερες περιπτώσεις πάντως, η αρχιτεκτονική υπολογιστή διαλογής παρέχει μεγαλύτερη ασφάλεια και χρησιμότητα.

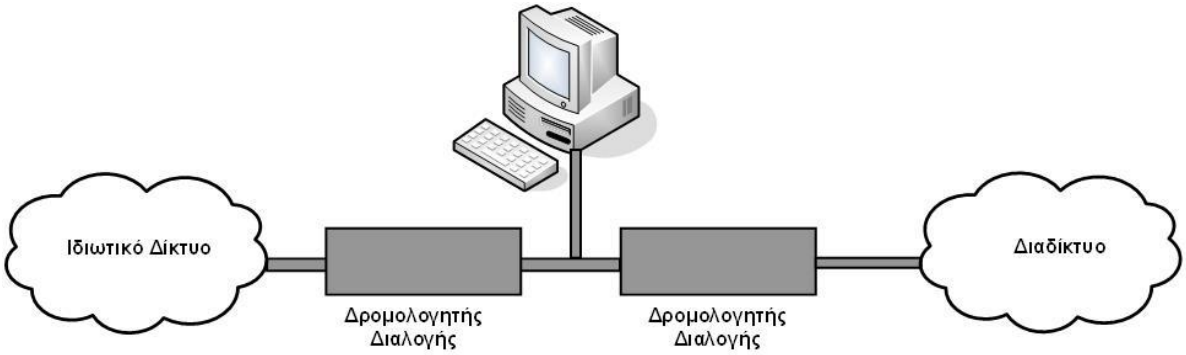
Η αρχιτεκτονική αυτή παρουσιάζει ένα σοβαρότατο μειονέκτημα: Βασίζεται σε δύο ξεχωριστές συσκευές ασφάλειας, το δρομολογητή διαλογής και τον υπολογιστή-οχυρό. Εάν κάποια από τις δύο αυτές συσκευές αποτύχει, τότε το δίκτυο εκτίθεται σε κίνδυνο. Αν για παράδειγμα ένας εισβολέας καταφέρει να παραβιάσει τον υπολογιστή-οχυρό, τότε θα έχει ελεύθερη πρόσβαση στο εσωτερικό δίκτυο. Ομοίως αν ο δρομολογητής εκτεθεί σε κίνδυνο, όλο το δίκτυο είναι πλέον ανασφαλές. Για αυτούς τους λόγους η πιο διαδεδομένη αρχιτεκτονική είναι η επόμενη.

Φράγματα Ασφάλειας Υποδικτύου Διαλογής (Screened Subnet Firewalls):

Ένα firewall υποδικτύου διαλογής αποτελείται από δύο δρομολογητές διαλογής με τον υπολογιστή-οχυρό να βρίσκεται ενδιάμεσα. Έτσι δημιουργείτε ένα εσωτερικό (περιμετρικό) υποδίκτυο διαλογής, ανάμεσα στο εσωτερικό και εξωτερικό δίκτυο. Στο **Error! Reference source not found.** απεικονίζεται ο σχηματισμός firewall υποδικτύου διαλογής.

Αυτή η αρχιτεκτονική εισάγει ένα επιπλέον επίπεδο ασφάλειας σε σχέση με την αρχιτεκτονική υπολογιστή διαλογής, προσθέτοντας το περιμετρικό υποδίκτυο το οποίο απομονώνει περισσότερο το εσωτερικό δίκτυο από το Internet.

Αυτό το περιμετρικό υποδίκτυο αναφέρεται και ως «αποστρατιωτικοποιημένη ζώνη» (DMZ-demilitarized zone). Είναι δυνατό να υπάρχουν περισσότεροι του ενός υπολογιστές-οχυρά στο απομονωμένο αυτό δίκτυο για λόγους απόδοσης.



Σχήμα 4. 11 Ένας σχηματισμός firewall υποδικτύου διαλογής.

Ο λόγος για τον οποίο προστίθεται ένα επιπλέον δίκτυο είναι ότι οι υπολογιστές-οχυρά αποτελούν τις πλέον ευπαθείς συσκευές του δικτύου, καθώς είναι τα συστήματα τα οποία κατεξοχήν μπορούν να δεχτούν επιθέσεις. Στην αρχιτεκτονική υπολογιστή διαλογής, ανάμεσα στον υπολογιστή-οχυρό και στο εσωτερικό δίκτυο δεν υπάρχει κανένας άλλος μηχανισμός άμυνας. Παραβιάζοντας κάποιος τον υπολογιστή-οχυρό μπορεί να έχει πλήρη πρόσβαση στο εσωτερικό δίκτυο. Η αρχιτεκτονική υποδικτύου διαλογής προσφέρει περισσότερη ασφάλεια, απομονώνοντας τον υπολογιστή-οχυρό στο περιμετρικό υποδίκτυο. Έτσι ακόμη και αν κάποιος εισβολέας αποκτήσει κάποια πρόσβαση στον υπολογιστή-οχυρό, θα έχει

να αντιμετωπίσει ακόμη ένα δρομολογητή για μπορέσει να εισβάλει στο εσωτερικό δίκτυο.

Όπως έχει αναφερθεί, στο περιμετρικό υποδίκτυο περιλαμβάνονται δύο δρομολογητές διαλογής. Ο εσωτερικός δρομολογητής βρίσκεται μεταξύ του εσωτερικού δικτύου και του περιμετρικού υποδικτύου, ενώ ο εξωτερικός δρομολογητής βρίσκεται μεταξύ του περιμετρικού υποδικτύου και του εξωτερικού δικτύου, συνήθως του Internet.

Ο εσωτερικός δρομολογητής προστατεύει το εσωτερικό δίκτυο, τόσο από το Internet, όσο και από το περιμετρικό υποδίκτυο. Ο δρομολογητής αυτός αναλαμβάνει το μεγαλύτερο βάρος υλοποίησης του μηχανισμού φιλτραρίσματος πακέτων του firewall. Έτσι επιτρέπει να περάσουν μόνο επιλεγμένες υπηρεσίες από το εσωτερικό δίκτυο προς το Internet. Τέτοιες υπηρεσίες αφορούν εξερχόμενες συνόδους Telnet, FTP, WAIS, Copher και άλλες συνόδους.

Ο εξωτερικός δρομολογητής προστατεύει τόσο το περιμετρικό υποδίκτυο όσο και το εσωτερικό δίκτυο από το Internet. Ο εξωτερικός δρομολογητής τείνει να επιτρέπει οτιδήποτε κατευθύνεται από το περιμετρικό υποδίκτυο προς τον εξωτερικό κόσμο. Σε γενικές γραμμές είναι απαραίτητο οι κανόνες οι οποίοι τίθενται για την προστασία των εσωτερικών μηχανών να συμφωνούν τόσο στον εσωτερικό όσο και στον εξωτερικό δρομολογητή. Οι μοναδικοί κανόνες φιλτραρίσματος πακέτων που εφαρμόζονται αποκλειστικά σε έναν εξωτερικό δρομολογητή, είναι αυτοί οι οποίοι προστατεύουν τον υπολογιστή-οχυρό και το εσωτερικό δίκτυο από το Internet.

Με αυτή την αρχιτεκτονική υποδικτύου διαλογής, το ιδιωτικό δίκτυο προστατεύεται ακόμη περισσότερο, αφού ένας επιτιθέμενος θα πρέπει να υπονομεύσει, όχι μόνο τον υπολογιστή-οχυρό αλλά και τους δρομολογητές για να φτάσει στο εσωτερικό δίκτυο. Έτσι δεν υπάρχει πλέον ένα και μοναδικό σημείο ευπάθειας το οποίο να θέτει σε κίνδυνο όλο το εσωτερικό δίκτυο.

4.7.4 Ψηφιακές Υπογραφές

Για την απόδειξη της γνησιότητας ενός εγγράφου, χρησιμοποιούνται οι συμβατικές υπογραφές. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί. Στις συναλλαγές ηλεκτρονικού εμπορίου καθίσταται αναγκαία η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής. Ο μηχανισμός της ηλεκτρονικής υπογραφής θα πρέπει να παρέχει απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των ανταλλασσομένων μηνυμάτων. Απαιτείται δηλαδή ένα σύστημα μέσω του οποίου κάποιος θα μπορεί να στείλει ένα υπογεγραμμένο μήνυμα σε κάποιον άλλο με τέτοιο τρόπο ώστε:

- Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας.
- Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος.
- Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

Οι ηλεκτρονικές υπογραφές που βασίζονται στην κρυπτογραφία ονομάζονται ψηφιακές υπογραφές. Η ψηφιακή υπογραφή εξαρτάται άμεσα από το μήνυμα το οποίο στέλνεται, είναι γνωστή μόνο στον αποστολέα αλλά μπορεί να επιβεβαιωθεί από τον καθένα. Η ψηφιακή υπογραφή θα πρέπει να είναι εύκολο να υπολογιστεί και να επιβεβαιωθεί από οποιονδήποτε ενδιαφερόμενο. Παράλληλα όμως θα πρέπει να είναι αδύνατο να αντιγραφεί.

Η ψηφιακή υπογραφή είναι άμεσα συσχετιζόμενη με το μήνυμα το οποίο στέλνεται και δεν είναι ποτέ η ίδια. Διαφορετικό μήνυμα σημαίνει άμεσα και διαφορετική ψηφιακή υπογραφή. Η «σύνδεση» της ψηφιακής υπογραφής με το περιεχόμενο του μηνύματος που υπογράφει εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity). Δηλαδή διασφαλίζει ότι από τη στιγμή που ο αποστολέας υπέγραψε τα δεδομένα, αυτά δεν έχουν τροποποιηθεί.

Πρώτο βήμα για τη δημιουργία της ψηφιακή υπογραφής είναι η παραγωγή μιας σύνοψης μηνύματος (message digest). Για το σκοπό αυτό, χρησιμοποιείται μια συνάρτηση κατακερματισμού (hash function). Η συνάρτηση αυτή αντιστοιχεί σε κάθε μήνυμα μια μοναδική ακολουθία χαρακτήρων, που ονομάζεται σύνοψη μηνύματος.

4.8 Η Σημερινή Πραγματικότητα

Το θέμα της διαλειτουργικότητας είναι ένα από τα πιο κρίσιμα ζητήματα που παραμένουν άλυτα ακόμη και σήμερα. Για να μπορεί μια PKI υποδομή να λειτουργεί ομαλά με οποιουδήποτε τύπου πιστοποιητικά και σε ολόκληρο τον κόσμο χρειάζεται να είναι συμφωνημένη με ένα μεγάλο πλήθος προτύπων, όπως π.χ. εκείνα των ISO (International Organization for Standardization), ITU (International Telecommunication Union), ETSI (Electronic Telecommunications Standardization Institute) αλλά και με διάφορα εθνικά πρότυπα, όπως για παράδειγμα το t-Scheme της Μεγάλης Βρετανίας.

Η πραγματικότητα έχει δείξει πως διαλειτουργικότητα υπάρχει μόνο σε απλές εφαρμογές (π.χ. πιστοποίηση ταυτότητας σε ένα δίκτυο υπολογιστών) ή πολύ περιορισμένου τύπου εφαρμογές (π.χ. χρήση του πρωτοκόλλου Secure Sockets Layer, SSL). Τα κατά τόπου πρότυπα δεν εγγυώνται πλήρη διαλειτουργικότητα καθώς χρειάζεται να γίνει εκτενέστατος έλεγχος για όλες τις περιπτώσεις

συμβατότητας μεταξύ τους. Αυτό απαιτεί χιλιάδες εργατοώρες από εξειδικευμένο προσωπικό, κάτι που είναι ιδιαίτερα αποθαρρυντικό.

Ένας παράγοντας που συμβάλλει στην αύξηση της πολυπλοκότητας μιας τέτοιας υποδομής είναι οι διάφορες κατηγορίες πιστοποιητικών καθώς και το μέσο με το οποίο θα προσφέρονται αυτά στο χρήστη. Για παράδειγμα σήμερα υπάρχουν τρεις κύριες κατηγορίες ψηφιακών πιστοποιητικών, για πιστοποίηση ενός λογαριασμού ηλεκτρονικού ταχυδρομείου, για ηλεκτρονικές συναλλαγές και για ηλεκτρονική μεταφορά κεφαλαίων. Κάθε πιστοποιητικό από τα παραπάνω έχει διαφορετικές απαιτήσεις ασφάλειας. Για παράδειγμα ένα πιστοποιητικό της πρώτη κατηγορίας μπορεί να αποθηκευτεί σε μια δισκέτα, της δεύτερης κατηγορίας σε μια έξυπνη κάρτα (smart card) και της τρίτης ίσως σε μια ειδική προστατευόμενη συσκευή (tamper resistant hardware).

Μια υποδομή σαν την PKI είναι ένα τεράστιο και ιδιαίτερα ακριβό έργο, η επιτυχία του οποίου και τα αναμενόμενα κέρδη εμπεριέχουν σημαντικό ρίσκο. Εκτός από τον υλικοτεχνικό εξοπλισμό απαιτεί και μια εκτεταμένη τεχνολογική υποδομή, κυρίως όσον αφορά στα δίκτυα επικοινωνιών τα οποία υπάρχουν.

Η υλοποίηση και συντήρηση μιας τέτοιας υποδομής στηρίζεται κατά πολύ σε ανθρώπινες ενέργειες. Είναι δηλαδή απαραίτητο ένα εξειδικευμένο προσωπικό. Όμως το εξειδικευμένο προσωπικό, εκτός από το ότι είναι δύσκολο να βρεθεί στην σημερινή αγορά, κοστίζει ιδιαίτερα.

Είναι γεγονός ότι καθυστερεί η ανάπτυξη μιας πραγματικά παγκόσμιας υποδομής δημοσίου κλειδιού, η οποία θα προσφέρει όλα τα πλεονεκτήματα της χρήσης της κρυπτογραφίας δημοσίου κλειδιού. Η υφιστάμενη έλλειψη διαλειτουργικότητας στις εφαρμογές ηλεκτρονικών υπογραφών, το μεγάλο κόστος δημιουργίας και διατήρησης μιας ασφαλούς Υποδομής Δημοσίου Κλειδιού και ο μεγάλος επιχειρηματικός κίνδυνος της ανάπτυξης μιας τέτοιας υποδομής την στιγμή που δεν έχουν προσδιοριστεί σαφώς οι τελικές προδιαγραφές που θα επικρατήσουν, οδηγούν σε συγκράτηση και περιορισμό των σχετικών επενδύσεων και των πρωτοβουλιών για την ανάπτυξη συναφών εφαρμογών. Παράλληλα διατηρείται ένα κλίμα σύγχυσης και πλημμελούς ενημέρωσης των δυνητικών χρηστών των εφαρμογών ηλεκτρονικής υπογραφής, το οποίο δυσχεραίνει την ανάπτυξη της απαραίτητης σχετικής εμπιστοσύνης.

4.9 Διαχείριση της Πρόσβασης των Χρηστών

Στόχος είναι η προστασία του συστήματος από μη εξουσιοδοτημένη προσπέλαση. Θα πρέπει να υπάρχουν επίσημες διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα τμήματα του συστήματος. Ιδιαίτερη προσοχή απαιτείται στον καθορισμό των δικαιωμάτων των χρηστών, ώστε να μην είναι δυνατό να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος.

4.9.1 Δήλωση χρηστών

Θα πρέπει να υπάρχει μια συγκεκριμένη διαδικασία για την αρχική δήλωση (εγγραφή) των χρηστών στο σύστημα και τη διαγραφή τους από αυτό. Η διαδικασία αυτή πρέπει να περιλαμβάνει τα ακόλουθα:

Χρήση μοναδικών ID χρηστών για τη σύνδεση κάθε χρήστη με τις ενέργειες του στο σύστημα.

Έλεγχο της εξουσιοδότησης του χρήστη από τον ιδιοκτήτη του συστήματος για τη χρήση των παρεχόμενων υπηρεσιών.

Την γραπτή ενημέρωση των χρηστών για τα δικαιώματα τους στο σύστημα.

Γραπτή δήλωση των χρηστών ότι αποδέχονται τους όρους παροχής υπηρεσιών από το σύστημα.

Εξασφάλιση ότι οι υπηρεσίες δεν παρέχονται πριν ολοκληρωθούν οι διαδικασίες εξουσιοδότησης των χρηστών.

Τήρηση αρχείου όλων των χρηστών του συστήματος.

Άμεση διαγραφή των χρηστών που αποχωρούν από το σύστημα.

Εξασφάλιση ότι περισσότεροι από ένας χρήστες δεν έχουν το ίδιο ID.

4.9.2 Διαχείριση προνομιακών δικαιωμάτων

Προνομιακά δικαιώματα είναι τα δικαιώματα που επιτρέπουν την παράκαμψη των μηχανισμών ελέγχου του συστήματος. Ο καθορισμός και η χρήση τέτοιων δικαιωμάτων θα πρέπει να ελέγχεται και να περιορίζεται.

Θα πρέπει να υπάρχει μια διαδικασία εξουσιοδότησης η οποία θα ελέγχει τα προνομιακά δικαιώματα. Θα πρέπει να εξεταστούν τα ακόλουθα:

Θα πρέπει να καθοριστούν τα προνομιακά δικαιώματα που συνδέονται με κάθε μέρος του συστήματος (εφαρμογές, λειτουργικό σύστημα κλπ.) καθώς και οι χρήστες που μπορούν να τα χρησιμοποιούν.

Τα προνομιακά δικαιώματα πρέπει να παρέχονται μόνο σε όσους χρήστες είναι απολύτως απαραίτητο και μόνο για όσο χρονικό διάστημα χρειάζεται.

Θα πρέπει να ακολουθείται μια διαδικασία έγκρισης και καταγραφής των προνομιακών χρηστών του συστήματος.

4.9.3 Διαχείριση κωδικών πρόσβασης (password)

Οι κωδικοί πρόσβασης είναι ο πλέον συνηθισμένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη του συστήματος. Οι χρήστες θα πρέπει να υποχρεώνονται σε έγγραφη βεβαίωση για την τήρηση της μυστικότητας των κωδικών πρόσβασης τους.

Οι κωδικοί πρόσβασης δεν πρέπει ποτέ να αποθηκεύονται σε κάποιο υπολογιστικό σύστημα σε μη προστατευμένη μορφή. Αν είναι απαραίτητο μπορούν να χρησιμοποιηθούν βιομετρικοί μηχανισμοί αυθεντικοποίησης χρηστών ή και ειδικά στοιχεία ασφάλειας, όπως έξυπνες κάρτες.

4.9.4 Ευθύνες Χρηστών

Σκοπός είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Η συνεργασία των εξουσιοδοτημένων χρηστών του συστήματος είναι απαραίτητη για την ασφάλεια του. Οι χρήστες πρέπει να ενημερώνονται σχετικά με τη χρήση κωδικών πρόσβασης και την ασφάλεια του εξοπλισμού.

Οι χρήστες θα πρέπει να ακολουθούν τις συνιστώμενες πρακτικές ασφάλειας για τη χρήση κωδικών πρόσβασης. Οι χρήστες θα πρέπει να είναι ενημερωμένοι ώστε:

- Να κρατούν μυστικούς του κωδικούς πρόσβασης τους.
- Να αποφεύγουν να καταγράφουν τους κωδικούς πρόσβασης τους σε χαρτί, εκτός αν μπορούν να αποθηκευτούν με ασφάλεια.
- Να αλλάζουν τους κωδικούς πρόσβασης τους όποτε υπάρχει κάποια ένδειξη παραβίασης του συστήματος.
- Να επιλέγουν κωδικούς πρόσβασης με μήκος τουλάχιστον έξι χαρακτήρων, που να απομνημονεύονται εύκολα και να μη βασίζονται σε στοιχεία που εύκολα κάποιος τρίτος μπορεί να υποθέσει (π.χ. ονόματα).
- Να αλλάζουν τους κωδικούς πρόσβασης τους σε τακτά χρονικά διαστήματα.

Οι χρήστες θα πρέπει να εξασφαλίζουν την επαρκή προστασία του εξοπλισμού που λειτουργεί χωρίς επίβλεψη. Θα πρέπει να είναι ενημερωμένοι για τις απαιτήσεις ασφάλειας τέτοιου εξοπλισμού, καθώς και για τις προσωπικές τους ευθύνες. Οι χρήστες θα πρέπει να είναι ενημερωμένοι ώστε:

- Να τερματίζουν τις συνδέσεις που δεν είναι απαραίτητες.
- Να αποσυνδέονται από το σύστημα όταν έχουν ολοκληρώσει την εργασία τους.
- Να ασφαλίζουν τους σταθμούς εργασίας με κατάλληλους μηχανισμούς (ειδικές κλειδαριές, κωδικό πρόσβασης) όταν δε χρησιμοποιούνται.

Διαχείριση κωδικών πρόσβασης

Οι κωδικοί πρόσβασης είναι ο πιο διαδεδομένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη. Μερικές εφαρμογές απαιτούν τον ορισμό των κωδικών πρόσβασης των χρηστών από μια ανεξάρτητη αρχή. Στις περισσότερες όμως περιπτώσεις οι κωδικοί αυτοί επιλέγονται από τους ίδιους τους χρήστες. Ένα καλό σύστημα διαχείρισης κωδικών πρόσβασης θα πρέπει να:

- Επιβάλει τη χρήση ατομικών κωδικών πρόσβασης ώστε κάθε χρήστης να συσχετίζεται με τις δικές του ενέργειες στο σύστημα.
- Όπου είναι κατάλληλο, να επιτρέπεται στους χρήστες να επιλέγουν τον προσωπικό τους κωδικό πρόσβασης.
- Επιβάλει την τακτική αλλαγή των κωδικών πρόσβασης.
- Τηρεί αρχείο με τους προηγούμενους κωδικούς πρόσβασης του κάθε χρήστη, για να αποτρέπει την επαναχρησιμοποίηση των κωδικών αυτών.
- Να μην εμφανίζει τους κωδικούς πρόσβασης στην οθόνη κατά την εισαγωγή τους.
- Να αποθηκεύει τους κωδικούς πρόσβασης κρυπτογραφημένους, χρησιμοποιώντας ένα μονόδρομο αλγόριθμο κρυπτογράφησης.

4.10 Ασφάλεια στο Cloud

Οι προσεγγίσεις ως προς την ασφάλεια πρέπει να είναι αντικειμενικές κυρίως όσον αφορά τον έλεγχο του συστήματος και τη λειτουργικότητά του. Αυτό που εννοούμε είναι ότι δεν είναι κατάλληλη η ίδια αρχιτεκτονική και ο ίδιος έλεγχος για διαφορετικές εφαρμογές ασφάλειας. Σε ότι αφορά την cloud τεχνολογία, δεν πρέπει να αναμείξουμε τραπεζικές με εφαρμογές κοινωνικής δικτύωσης, σε ένα δημόσιο σύννεφο (cloud). Από τη φύση τους κάποιες εφαρμογές χαμηλού κινδύνου ασφάλειας, θα μπορούσαν να συνυπάρξουν με άλλες εφαρμογές με ανάλογες ανάγκες ασφάλειας.

Για να μπορέσουμε να ποσοτικοποιήσουμε τον κίνδυνο θα λέγαμε ότι έχει εξάρτηση από τις ευπάθειες του συστήματος, τις απειλές που δέχεται το σύστημα καθώς και από τα μέτρα πρόληψης που λαμβάνουμε για να αντιμετωπίσουμε τις καταστάσεις αυτές.

$$\text{Risk} = \left(\frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Countermeasures}}\right) \times (\text{Asset value})$$

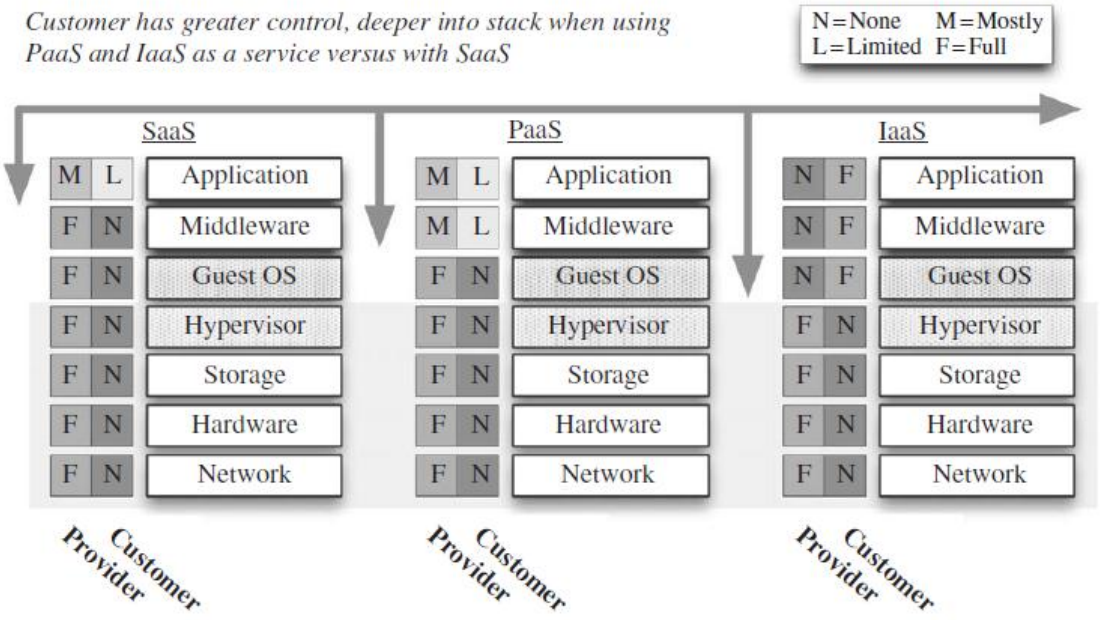
Ο υπολογισμός του κίνδυνου από τον παραπάνω τύπο μας βοηθάει να ποσοτικοποιήσουμε τις ευπάθειες του συστήματος μας, κάτι το οποίο είναι αρκετά δύσκολο να γίνει.

Υπάρχει ένα ευρύ φάσμα μοντέλων και προτύπων που ισχύουν για να παρέχουν ασφάλεια σε Λογισμικό / λύσεις ασγάλειας / σύστηματα Ανάπτυξης Κύκλου Ζωής (System Development Life Cycle - SDLC). Αρκετές από αυτές μπορούν να χρησιμεύσουν ως πρότυπα αναφοράς για την τεχνολογία συστημάτων ασφαλείας, αρχιτεκτονική ασφαλείας, τις διαδικασίες ασφάλειας, και σίγουρα για την ασφάλεια στο cloud. Ορισμένα από αυτά τα μοντέλα είναι:

4.10.1 Πρότυπα ασφαλείας.

- **ISO 27001 through ISO 27006**[F]: Αυτή η σειρά διεθνών προτύπων για την ασφάλεια των πληροφοριών καλύπτει την διαχείριση, τις βέλτιστες πρακτικές, τις απαιτήσεις και τις τεχνικές. Αυτά έχουν σημαντική αξία ως προς τις δυνατότητες εφαρμογής τους στην ασφάλεια του cloud.
- **European Network and Information Security Agency (ENISA)**: Είναι ένας Ευρωπαϊκός οργανισμός ασφάλειας του διαδικτύου.
- **Information Technology Infrastructure Library (ITIL)**[I]: Η διαχείριση ασφάλειας στο ITIL είναι βασισμένη στο ISO/IEC 27002.
- **Control Objectives for Information and related Technology (COBIT):** Πρόκειται για ένα σύνολο από γενικά αποδεκτές καλύτερες πρακτικές και μέτρα ασφάλειας.

Ανάλογα με το είδος της υπηρεσίας που εκτελείται στο cloud (IaaS, PaaS ή IaaS) ο πελάτης έχει και διαφορετικό έλεγχο αυτής της υπηρεσίας.

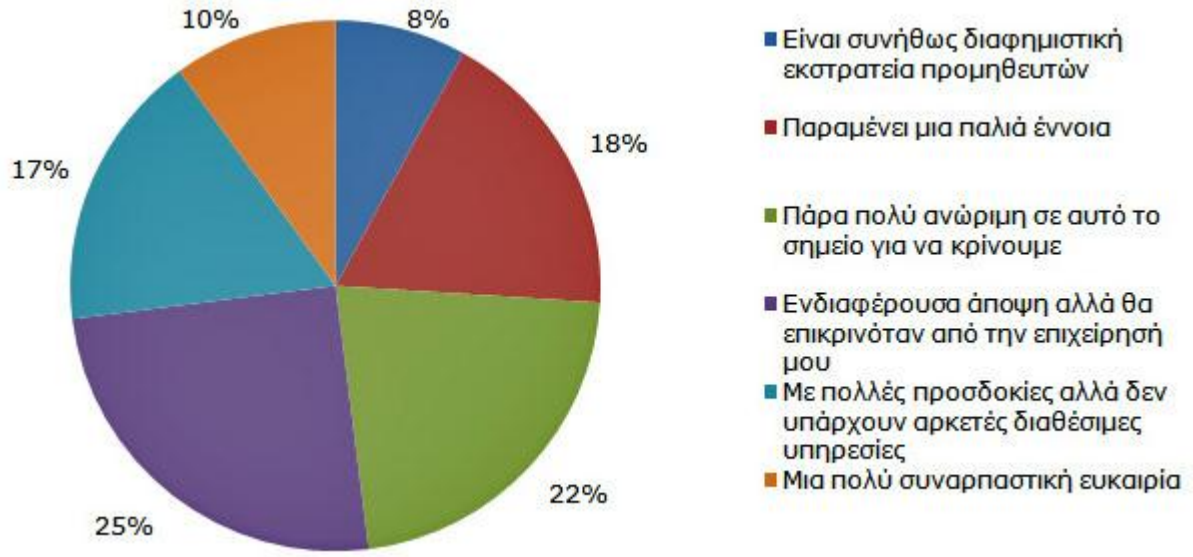


Σχήμα 4. 12 Έκταση του ελέγχου και της προστασίας σε κάθε υπηρεσία.

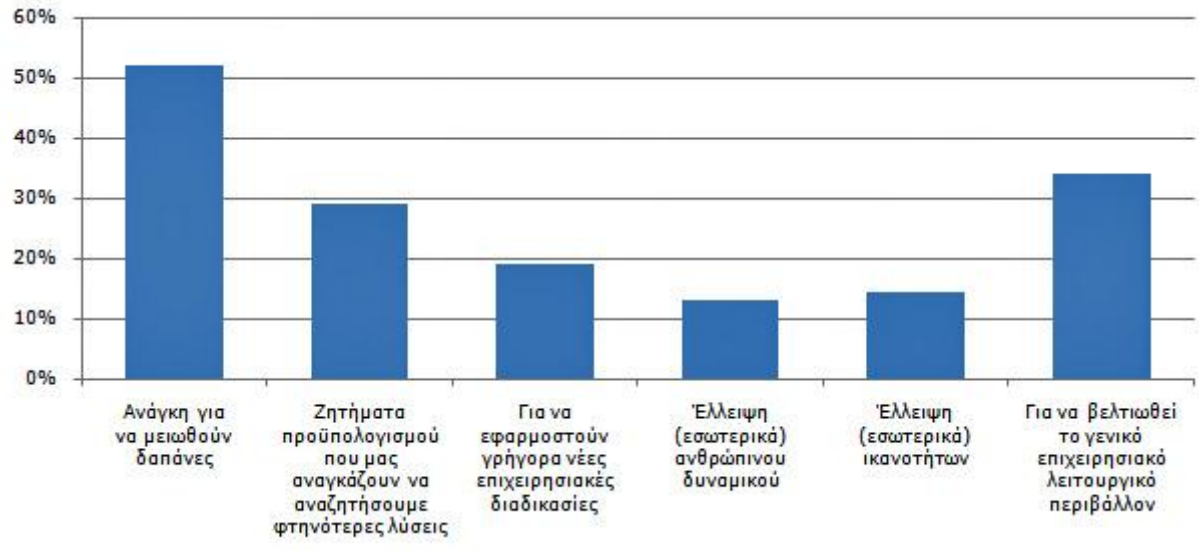
Με το SaaS, η ασφάλεια αναλαμβάνεται από τον πάροχο υπηρεσιών του Cloud. Αντίθετα με το PaaS, προσφέρεται μεγαλύτερη επεκτασιμότητα και έλεγχος από τους πελάτες.

Επίλογος.

Τριπλάσιες αναμένεται να είναι διεθνώς οι δαπάνες για υπηρεσίες cloud computing μέχρι το 2012, χρονιά κατά την οποία η αξία της συγκεκριμένης αγοράς θα φτάσει τα $42 δις, σύμφωνα με τους αναλυτές της IDC. Η IDC υποστηρίζει πως στη σημερινή εποχή που ο περιορισμός του κόστους κυριαρχεί, το cloud computing δεν είναι απλώς μόδα αλλά μια κυρίαρχη τάση.
Σύμφωνα με τα στοιχεία πρόσφατης έρευνας που πραγματοποίησε η διεθνής εταιρία με τη συμμετοχή 696 CIO's και υψηλόβαθμων στελεχών από το χώρο του τμήματος πληροφορικής, το 11% των ερωτηθέντων κάνει ήδη χρήση λύσεων cloud computing. Το 41% δηλώνει έτοιμο να προχωρήσει στην υιοθέτηση τέτοιου είδους υπηρεσιών και αρκετοί έχουν ακολουθήσει πιλοτικές εφαρμογές. Από την άλλη πλευρά το 17% των ερωτηθέντων επισημαίνει, πως δεν υπάρχουν αρκετές εφαρμογές προς χρήση παρόλο που το cloud computing είναι πολλά υποσχόμενο.
Σύμφωνα με τον Dr. Patrick Chan, IDC's Chief Technology Advisor for Emerging Technologies in Asia/ Pacific, το μέλλον του cloud computing φαντάζει λαμπρό. Σε τρία χρόνια από τώρα, οπότε θα έχει επεκταθεί περαιτέρω η συγκεκριμένη τάση, οι μεγάλοι κατασκευαστές θα πρέπει να έχουν ήδη πάρει θέση με τις κατάλληλες εφαρμογές, αν θέλουν να διεκδικήσουν ηγετική θέση σε μια ανερχόμενη αγορά. Μερικοί μεγάλοι κατασκευαστές έχουν ήδη τοποθετηθεί σωστά στη συγκεκριμένη αγορά.



Επίλογος 1. Ποια είναι η άποψή σας για την τρέχουσα κατάσταση του cloud computing; Πηγή: IDC, 2009



Επίλογος 2 Τι οδήγησε τον οργανισμό μας στην επιλογή να επιλέξετε υπηρεσίες cloud computing; Πηγή: IDC, 2009

Επίλογος 3 Πόσο σημαντικό είναι για τον οργανισμό μας, ένας προμηθευτής cloud computing υπηρεσιών να έχει τα παρακάτω χαρακτηριστικά; Πηγή: IDC, 2009

Βιβλιογραφία.

[1]"Cloud Computng- from Wikipedia", http://en.wikipedia.org/wiki/Cloud_computing

[2]"Software as a Service- from Wikipedia", http://en.wikipedia.org/wiki/Software_as_a_service

[3]"Platform as a Service- from Wikipedia", http://en.wikipedia.org/wiki/Platform_as_a_service

[4]"Infrastructure as a Service-from Wikipedia", http://en.wikipedia.org/wiki/Infrastructure_as_a_Service#Infrastructure

[5] Christina Hoffa, Gaurang Mehta, "On the Use of Cloud Computing for Scientific Workflows," *Indiana University, University of Southern California, Argonne National Laboratory, Caltech,*

[6] Torry Harris, "Cloud Computing Services- A comparison," http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

[7] L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner,"A Break in the clouds: Towards a cloud Definition"

[8]"giannakis-summary",http://www.cs.uoi.gr/~pitoura/courses/ir/ir09s/giannakis-summary.pdf

[9]"giannakis-presentation",http://www.cs.uoi.gr/~pitoura/courses/ir/ir09s/giannakis-presentation.pdf

[10] Rachael King," How Cloud Computing Is Changing the World," BusinessWeek, http://businessweek.com

[11] Hamid R Motahari-Nezhad, Bryan Stephenson, Sharad Singhal," Outsourcing Business to Cloud Computing Services: Opportunities and Challenges," Hewlett Packard Labs, Palo Alto, CA, USA

[12] A.Weiss, Computing in the clouds. ACM *netWorker* 11(4):16-25, Dec. 2007

[13] M. Ibrahim, G. Long, Service-Oriented Architecture and Enterprise Architecture, http://www.ibm.com/developerworks/webservices/library/ws-soaenterprise1/?S_TACT=105AGX04&S_CMP=ART

[14] Dr. Maik A. Lindner, Cloud Computing in Research, SAP Research CEC Belfast, SAP UK Ltd., 2009

[15] Borja Sotomayor, Rubén S. Montero and Ignacio M. Llorente, Ian Foster," Virtual Infrastructure Management in Private and Hybrid Clouds," http://www.computer.org/portal/web/internet/home

[16] D. Nurmi et al., "The Eucalyptus Open-Source Cloud- Computing System," *Cloud Computing and Applications 2008* (CCA 08), 2008; www.cca08.org/papers.php

[17] B. Rochwerger et al., "The Reservoir Model and Architecture for Open Federated Cloud Computing," *IBM Systems J.*, Oct. 2008.

[18] B. Sotomayor et al., "Capacity Leasing in Cloud Systems using the OpenNebula Engine," *Proc. Cloud Computing and Applications 2008* (CCA 08), 2008; www. cca08.org/papers.php

[19] S. Lohr, "Google and IBM Join in Cloud Computing Research," *New York Times,* 2007.

[20] Twenty Experts Define Cloud Computing, http://cloudcomputing.syscon.com/read/612375_p.htm.

[21] I. Llorente, OpenNebula Project. http://www.opennebula.org/

[22] Google App Engine, http://appengine.google.com

[23] George Lauer, iHealthBeat, "Health Care Might Be Ripe for Cloud Computing", http://www.ihealthbeat.org/features/2009/health-care-might-be-ripe-for-cloud-computing.aspx

[24] Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper,"Cloud Computing for dummies"

[25] David Chappell," A SHORT INTRODUCTION TO CLOUD PLATFORMS," August 2008

[26] Eucalyptus Public Cloud (EPC). http://eucalyptus.cs.ucsb.edu/wiki/EucalyptusPublicCloud/

[27] Rajkumar Buyya, James Broberg, Andrzej Goscinski," CLOUD COMPUTING-Principles and Paradigms,"

[28] Vic (J.R.) Winkle, "Securing the Cloud",

[29] Hadoop (2006), http://lucene. apache.org/hadoop/