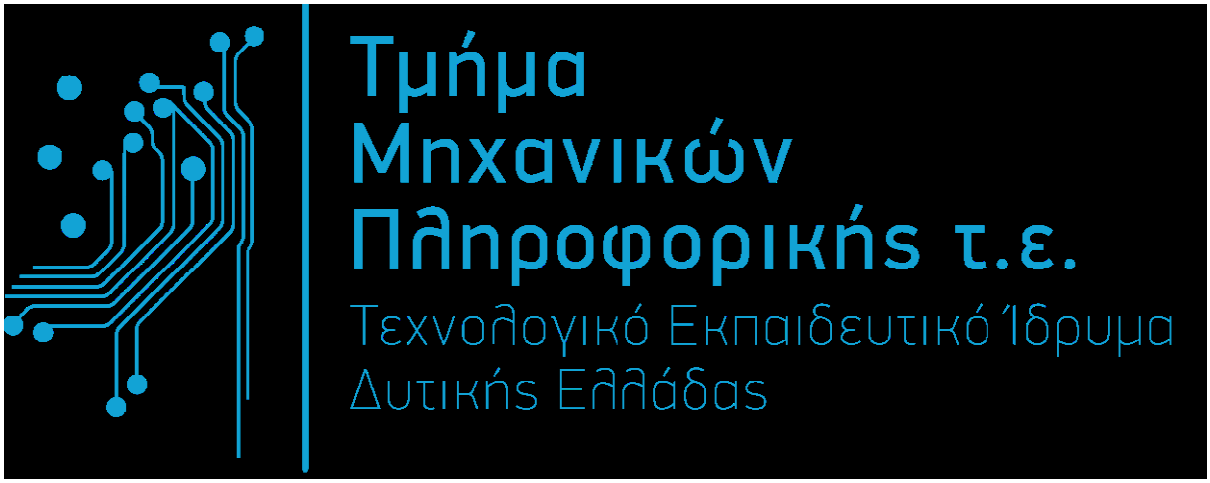


Πτυχιακή εργασία

Ασφάλεια και Ακεραιότητα Δεδομένων σε Cloud Computing Συστήματα

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΩΝ :
Λόης Σωτήριος: ΑΜ 0760
Φραγκουλάκης Χέρτ Νικόλαος: ΑΜ 0888

Επιβλέπων Καθηγητής: Τσακανίκας Βασίλειος

Αντίρριο, 2018

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή Αντίρριο,

Ημερομηνία 22/6/2018

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Τσακανίκας Βασίλειος.

2. Ασαρίδης Ηλείας.

3. Παρασκευάς Μιχάλης.

Ευχαριστίες

Η παρούσα εργασία αναπτύχθηκε στα πλαίσια της πτυχιακής εργασίας για λογαριασμό του τμήματος Μηχανικών Υπολογιστών του ΤΕΙ Δυτικής Ελλάδος.

Υπεύθυνος για την εκπόνηση της πτυχιακής εργασίας ήταν ο καθηγητής Τσακανίκας Βασίλειος τον οποίο ευχαριστούμε πολύ για την καθοδήγηση του και τις καίριες υποδείξεις του κατά την διάρκεια της εκπόνησης της εργασίας μας καθώς και στην επιλογή του θέματος αφού μας δόθηκε η ευκαιρία να ασχοληθούμε με έναν πολύ ενδιαφέροντα τομέα.

Επίσης, θα θέλαμε να ευχαριστήσουμε ιδιαίτερα τις οικογένειες μας και τους φίλους μας που μας στήριξαν σε αυτήν την προσπάθεια μας και που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της πτυχιακής μας εργασίας.

Περίληψη

Τι είναι το cloud computing; Πολλοί χρησιμοποιούν τον όρο νέφος. Ο όρος νέφος χρησιμοποιήθηκε αρχικά για την έννοια του internet. Το cloud computing όμως είναι κάτι συγκεκριμένο που πολλοί σήμερα δεν θα μπορούσαν το περιγράψουν με απλούς όρους είτε να το περιγράψουν με διαφορετικά λόγια.

Το cloud είναι η πραγματοποίηση της ιδέας του ubigiutous computing η οποία αναφέρεται σε μια προηγμένη έννοια ενός υπολογιστικού συστήματος που μπορεί να χρησιμοποιηθεί σε οποιαδήποτε συσκευή, σε οποιαδήποτε θέση, ή σε οποιαδήποτε μορφή.

Πιο αναλυτικά στο κεφάλαιο 1 γίνεται περιγραφή των εισαγωγικών εννοιών για το cloud computing καθώς και στα μοντέλα παροχής υπηρεσιών τα οποία είναι ο τρόπος με τον οποίο μπορεί ο χρήστης να αποκτήσει πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων. Επίσης, στο κεφάλαιο αυτό θα αναφερθούμε στα μοντέλα ανάπτυξης τα οποία είναι το είδος του cloud computing το οποίο θα χρησιμοποιηθεί και στο cloud computing υιοθετώντας τις έννοιες του gridκαι του utilityοι οποίες είναι ένα επιχειρηματικό μοντέλο παροχής υπηρεσιών.

Στο Κεφάλαιο 2 γίνεται μια ιστορική αναδρομή στον όρο «νέφος» και στην προέλευση του. Επιπλέον, γίνεται αναφορά στον καθοριστικό ρόλο της Amazon στην εξέλιξη του νέφους καθώς και στους πρωτοπόρους στην ιστορία της δημιουργίας του cloud computing όπως είναι ο Douglas F.Parkhill, oJohn McCarthy, oJ.C.R. Licklider, oJohn Kemeny, o Thomas Kurtz και o Marc Benioff.

Το Κεφάλαιο 3 αναφέρεται σε θέματα ασφαλείας ενός cloudόπως τα επίπεδα που είναι διαχωρισμένη η ασφάλειαμε σημείο αναφοράς την ειδικότητα της ασφάλειας ή γενικευμένα τα επίπεδα ασφάλειας σαν securitylayer. Επίσης, αναφέρεται σε απειλές σύμφωνα με τον οργανισμό Cloud Security Alliance (CSA) και στα προβλήματα που προκύπτουν στην ασφάλεια ενός cloud.

Στο κεφάλαιο 4 αναφέρονται τα πρωτόκολλα ασφαλείας στα διάφορα επίπεδα δικτύωσης υπολογιστών. Τα πρωτόκολλα ασφαλείας τα οποία αναφέρονται είναι toLayer 2 Tunneling το Protocol, το IPSec, το πρωτόκολλο AHP, το πρωτόκολλο AHP, το πρωτόκολλο IKMP, το πρωτόκολλο SSL.

Στο κεφάλαιο 5 επεξηγείται η ασφάλεια του Cloud Computing μέσα από βιομετρικά χαρακτηρίστηκα όπως τα δαχτυλικά αποτυπώματα, η Ίριδα του ματιού, ο αμφιβληστροειδής κ.α. Αρχικά, αναλύονται τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων που κάνουν κάθε αποτύπωμα μοναδικό και οι αισθητήρες με τους οποίους γίνεται η ανάγνωση τους. Στη συνέχεια, αναλύονται τα βήματα που ακολουθεί ένας αλγόριθμος αναγνώρισης δακτυλικών αποτυπωμάτων και τα μειονεκτήματα ενός τέτοιου συστήματος. Στο τέλος του κεφαλαίου γίνεται αξιολόγηση σε επίπεδο ασφαλείας του συστήματος αναγνώρισης δακτυλικών αποτυπωμάτων.

Στο κεφάλαιο 6παρουσιάζεται η τεχνολογία των QRcode. Γίνεται μια ιστορική ανάδρομη για το πώς ξεκίνησαν να χρησιμοποιούνται και αναλύονται τατεχνικά τους στοιχεία.

Στο κεφάλαιο 7 προτείνεται μια αρχιτεκτονική ασφάλειας και πρόσβασης χρηστών σε υπηρεσίες cloud χρησιμοποιώντας την τεχνολογία της αναγνώρισης των δακτυλικών αποτυπωμάτων και των

QRcode. Συνδυάζοντας αυτές τις δυο τεχνολογίες σε μια αρχιτεκτονική αναλύεται πως αυξάνεται η ασφάλεια σε ένα cloud.

Περιεχόμενα

Ευχαριστίες.....3

Περίληψη.....4

Κεφάλαιο 1: Εισαγωγή στο CloudComputing.....9

1.1 Ο ορισμός του cloudcomputing κατά το NIST.....9

1.2 Μοντέλα παροχής υπηρεσιών.....9

1.2.3 Infrastructure as a Service (IaaS).....10

1.3 Μοντέλα Ανάπτυξης.....10

1.3.3 Κοινοτικό Σύννεφο (Communitycloud).....12

1.4 Ubigiutouscomputing.....12

1.5 GridComputing.....13

1.6 UtilityComputing.....14

1.7 Εικονικοποίηση (Virtualization).....15

1.7.1 Fullvirtualization.....15

1.7.2 Paravirtualization.....16

1.7.3 OS-levelvirtualization.....16

1.8 Εφαρμογές.....16

Κεφάλαιο 2: Ιστορική αναδρομή.....18

2.1 Douglas F.Parkhill.....18

2.2 JohnMcCarthy.....19

2.3 J.C.R. Licklider.....19

2.4 JohnKemenyandThomasKurtz.....19

2.5 MarcBenioff.....19

Κεφάλαιο 3: Ασφάλεια στο CloudComputing.....20

3.1 ΕπίπεδαΑσφαλείας cloud (Security Levels).....20

3.1.1 Level 1: physicallevelofsecurity.....20

3.1.2 Level 2: network level of security.....20

3.1.3 Level 3: OS και Applicationsecurity.....21

3.2 Απειλές κατά CSA.....22

3.2.1 Παραβίαση Δεδομένων (Databreaches).....22

3.3 Προβλήματα στην ασφάλεια.....23

Κεφάλαιο 4: Πρωτόκολλα ασφαλείας.....28

4.1 Layer 2 TunnelingProtocol.....28

4.2 Ανταλλαγή πακέτων L2TP.....30

4.3 L2TP/IPsec……30
4.4 IPSec (InternetProtocolSecurity) ……31
4.6 Πρωτόκολλο AHP……32
4.7 Πρωτόκολλο ESP……33
4.5 Επισκόπηση αρχιτεκτονικής……34
4.8 Πρωτόκολλο IKMP……35
4.9 Πρωτόκολλο SSL……36
4.11 Intrusiondetectionsystem (IDS) ……38
4.12 Συστήματα ανίχνευσης εισβολής (IDS). ……39
Κεφάλαιο 5: Ασφάλεια του CloudComputing μέσα από βιομετρικά χαρακτηρίστηκα……42
5.1 Χαρακτηριστικά δακτυλικών αποτυπωμάτων. ……44
5.2 Συστήματα ανάγνωσης δαχτυλικών αποτυπωμάτων……45
5.2.2 Αισθητήρας Οπτικής Μετάδοσης……46
5.2.3 Αισθητήρας Οπτικού TFT……46
5.2.4 Αισθητήρας Ηλεκτρο-οπτικής Ανάγνωσης……46
5.2.5 Αισθητήρες Χωρητικής Ανίχνευσης: CapacitanceSilicon /CapacitanceTFT……46
5.2.6 Αισθητήρας Πεδίου RF……47
5.2.7 Αισθητήρες Πίεσης – Πίεσης TFT……47
5.2.8 Θερμικοί Αισθητήρες……48
5.2.8 Αισθητήρας Υπερήχων……48
5.3 Αλγόριθμος αναγνώρισης δακτυλικών αποτυπωμάτων……48
5.3.2 Ευθυγράμμιση περιστροφής και μετατόπισης……48
5.3.3 Κοινή περιοχή εξαγωγής……49
5.3.4 Ταίριασμα των δακτυλικών αποτυπωμάτων……49
5.4 Μειονεκτήματα των δακτυλικών αποτυπωμάτων……49
5.4.1 Τα δακτυλικά αποτυπώματα δεν είναι μυστικά……50
5.4.2 Το δακτυλικά αποτυπώματα δεν μπορούν να αλλαχτούν……50
5.4.3 Τα δακτυλικά αποτυπώματα έχουν πρόβλημα με τις κρυπτογραφικές συναρτήσεις hash……50
5.5 Συμπέρασμα……51
Κεφάλαιο 6: QRcode……52
6.1 Ιστορική Αναδρομή……52
6.2 Τεχνικά Στοιχεία για τα QRCodes……52

Κεφάλαιο 7: Προτεινόμενη αρχιτεκτονική ασφάλειας και πρόσβασης χρηστών σε υπηρεσίες cloud.....54

7.1 Εφαρμογή αρχιτεκτονικής με δακτυλικά αποτυπώματα και QRcodes.....54

Γενικά Συμπεράσματα.....57

Βιβλιογραφία.....59

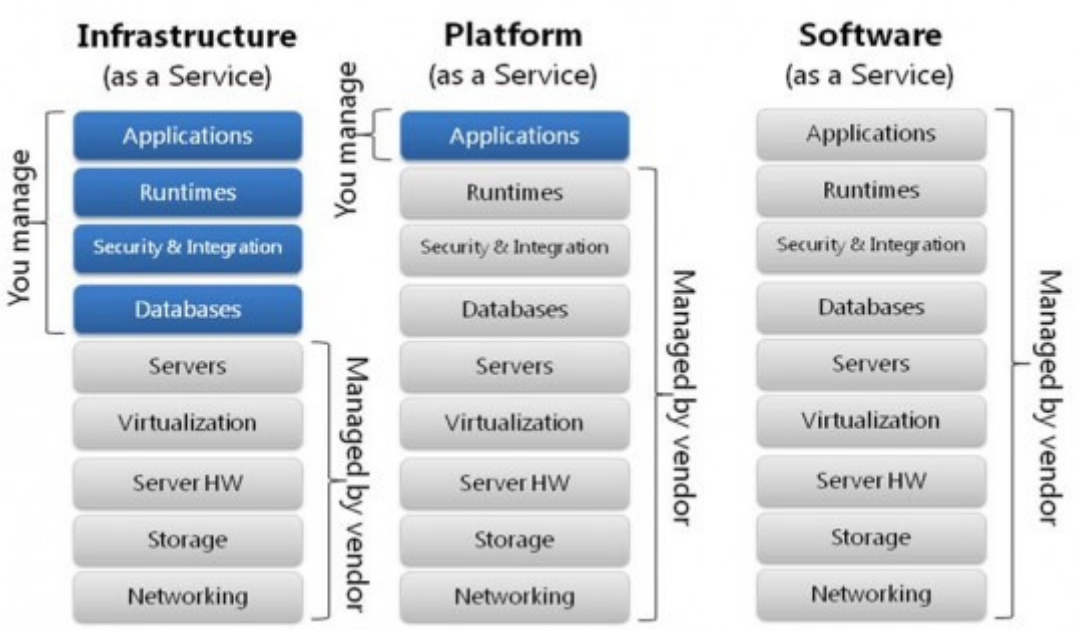
Κεφάλαιο 1: Εισαγωγή στο CloudComputing

1.1 Ο ορισμός του cloudcomputing κατά το NIST.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NationalInstituteofStandardsandTechnology)έχει ορίσει με σαφήνεια τον ορισμό του cloud computing και όλες τις έννοιες που σχετίζονται μαζί του.

Το cloud computing είναι ένα μοντέλο που επιτρέπει ευέλικτη, on-demand δικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης με τον πάροχο της υπηρεσίας. Αυτό το cloud μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από πέντε βασικά χαρακτηριστικά (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service), τρία μοντέλα παροχής υπηρεσιών(Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) Cloud Infrastructure as a Seervice (IaaS) , και τέσσερα μοντέλα ανάπτυξης (Private cloud, Community cloud, Public cloud, Hybrid cloud) [8].

1.2 Μοντέλα παροχής υπηρεσιών.



Εικόνα 1: Μοντέλα παροχής υπηρεσιών.

1.2.1SoftwareasaService (SaaS).

Η δυνατότητα που παρέχεται στον καταναλωτή να χρησιμοποιεί τις εφαρμογές του παρόχου που εκτελούνται σε μια υποδομή ενός cloud και να είναι προσβάσιμες από διάφορες συσκευές του πελάτη μέσα από σύνδεση ενός thin client, όπως ένα πρόγραμμα περιήγησης στο Web (π.χ. Web-based e-mail). Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει τις υποκείμενες υποδομές του cloud όπως το δίκτυο, servers, λειτουργικά συστήματα, μέσα αποθήκευσης ή ακόμη και κάποιες

μεμονωμένες δυνατότητες μιας εφαρμογής ανάλογα της ελευθερίας χρήσης που έχει ορίσει ο πάροχος.

1.2.2Platform as a Service (PaaS).

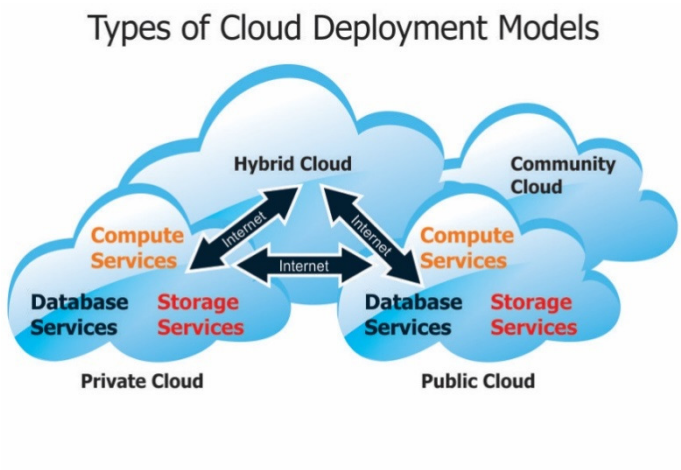
Η δυνατότητα που παρέχεται στον καταναλωτή είναι να αναπτύξει πάνω στην υποδομή του cloud δημιουργώντας καταναλωτικές εφαρμογές με τη χρήση γλωσσών προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο (π.χ. java, python, Net). Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή του cloud όπως το δίκτυο, servers, λειτουργικά συστήματα, μέσα αποθήκευσης αλλά ο καταναλωτής έχει τον έλεγχο της ανάπτυξης των εφαρμογών.

1.2.3Infrastructure as a Service (IaaS).

Η δυνατότητα που παρέχεται στον καταναλωτή είναι να νοικιάζει υπολογιστικούς πόρους όπως επεξεργαστική ισχύ, χώρος αποθήκευσης, την δικτύωση και άλλους υπολογιστικούς πόρους, όπου ο καταναλωτής είναι σε θέση να αναπτύξει και να τρέξει αυθαίρετο λογισμικό το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν διαχειρίζεται και δεν έχει τον έλεγχο της σχετικής υποδομής του cloud, αλλά έχει τον έλεγχο πάνω στα λειτουργικά συστήματα, μέσα αποθήκευση, εγκατεστημένες εφαρμογές και ενδεχομένως στην επιλογή της επιμέρους δικτύωσης (π.χ. firewalls, load balancers) [9].

1.3Μοντέλα Ανάπτυξης.

Υπάρχουν πολλές θεωρίες για την αρχιτεκτονική του cloud computing που προκαλεί την μετάβαση από τον κλασικό μοντέλο ανάπτυξης μιας επιχείρησης στο μοντέλο του cloud. Υπάρχουν τα public και τα private clouds που προσφέρουν οφέλει και υπάρχουν τρία βασικά μοντέλα να θεωρήσουμε και μεγάλη ποικιλία ανοιχτά API (application program interfaces) έναντι του πρωταρχικού μοντέλου.



Εικόνα 2: Μοντέλα Ανάπτυξης.

Τα τμήματα των IT μπορούν να διαλέξουν πού θα αναθέσουν τα προγράμματα τους σε public, private ή hybrid clouds και ο καθένας έχει τους συμβιβασμούς τους . Οι όροι public, private και

hybrid δεν ορίζονται με βάση την τοποθεσία αν και τα public clouds είναι τυπικά έξω στο internet και τα private υποθετικά μπορούν να φιλοξενούνται στον ίδιο χώρο μαζί με τα public.

Οι επιχειρήσεις μπορούν να κάνουν μια σειρά από συλλογισμούς για την σωστή χρήση του cloud computing και τις πιο πολλές φορές επιλέγουν περισσότερα από ένα μοντέλα για να λύσουν διαφορετικά προβλήματα. Ένα πρόγραμμα που είναι σε προσωρινή χρήση θα ήταν βέλτιστο να λειτουργήσει πάνω σε public cloud ώστε να αποφύγει την επιπλέον χρηματοδότηση και εξοπλισμό για ένα πρόβλημα που είναι προσωρινό. Αντίθετος, προγράμματα που έχουν συγκριμένες υπηρεσίες και χρίζουν ειδικής μεταχείρισης σε θέμα ασφάλειας και δεδομένων είναι καλύτερα να λειτουργούν σε private cloud.

1.3.1Δημόσιο Σύννεφο (Public cloud).

Τα public cloud μπορούν να λειτουργήσουν από τρίτους και να κατέχουν προγράμματα πολλαπλών πελατών μέσα σε έναν cloud server ή σύστημα αποθήκευση. Τα public cloud είναι συχνά μακριά από τις εγκαταστάσεις του εκάστοτε πελάτη και αποτρέπει την δημιουργία υποδομής με αποτέλεσμα την μείωση στα έξοδα και το ρίσκο.

Ένα από τα πλεονεκτήματα του public cloud είναι ότι μπορούν να είναι πιο μεγάλα από ότι ένα private cloud και έχουν πιο εύκολα την δυνατότητα της επεκτασιμότητας και την μετατόπιση τις υποδομής από τον cloud provider στην εταιρία που θέλει να το χρησιμοποιήσει.

Τμήματα του cloud computing μπορούν να διαχωριστούν για την αποκλειστική χρήση ενός πελάτη, δημιουργώντας έναν εικονικό datacenter. Αντί να περιορίζεται στην ανάπτυξη ενός image σε ένα virtual machine, ένα εικονικό ιδιωτικό κέντρο δεδομένων δίνει στους πελάτες μεγαλύτερη ορατότητα στην υποδομή και μπορούν να χειραγωγήσουν όχι μονο το image του virtual machine αλλά και τους servers, τα συστήματα αποθήκευσης, τις συσκευές και την τοπολογία δικτύου.

1.3.2 Ιδιωτικό Σύννεφο (Privatecloud).

Τα private cloud είναι φτιαγμένα για την αποκλειστική χρήση ενός μόνο πελάτη που του παρέχει σχεδόν την ολοκληρωτική διαχείριση των δεδομένων, της ασφάλειας και την ποιότητας της υπηρεσίας. Η υποδομή ανήκει στην εταιρία και έχει τον έλεγχο στο πως τα προγράμματα θα αναπτυχθούν πάνω στο private cloud. Τα private cloud μπορούν να υιοθετηθούν στηνβάση δεδομένων της εταιρίας αλλά μπορούν να αναπτυχθούν και σε κάποιο παράρτημα της εταιρίας.

Τα private clouds μπορούν να διαχειρίζονται από την εταιρία που τα κατέχει ή από έναν cloudprovider. Αυτό το μοντέλο δίνει την δυνατότητα στις εταιρίες να έχουν μεγάλο επίπεδο ελέγχου πάνω στην χρήση τον πόρων του cloud καθώς εισάγει την τεχνογνωσία που απαιτείται για την ίδρυση και λειτουργία του λειτουργικού περιβάλλοντος.

1.3.3Υβριδικό Σύννεφο (Hybridcloud).

Τα hybrid clouds είναι μια σύνθεση από δύο ή περισσότερα clouds (private ή public) που παραμένουν διακριτές οντότητες αλλά συνδέονται μεταξύ τους, προσφέροντας τα πλεονεκτήματα και την ανάπτυξη πολλαπλών μοντέλων. Το υβριδικό σύννεφο μπορεί επίσης να σημαίνει τη δυνατότητα σύνδεσης και συνεγκατάστασης διαχειριζόμενων ή και αποκλειστικών υπηρεσιών με τις πηγές του σύννεφου.

Η Gartner, Inc. ορίζει μια υπηρεσία υβριδικού cloud ως ένα σύννεφο με υπηρεσίες υπολογισμού, που αποτελείται από κάποιο συνδυασμό του private και του publiccloud, από διαφορετικούς

φορείς παροχής υπηρεσιών. Μια υπηρεσία hybridcloud ξεπερνάει την απομόνωση και τα όρια του παρόχου , έτσι ώστε να μην μπορούμε να το θέσουμε απλά σε μία κατηγορία όπως public , private ή communitycloud. Επιτρέπει σε κάποιον να επεκτείνει είτε την χωρητικότητα είτε την ικανότητα μιας υπηρεσίας του cloud, με την πρόσμιξη, ενσωμάτωση ή προσαρμογή με άλλη υπηρεσίαcloud.

Υπάρχουνπεριπτώσεις ποικίλες χρήσης για τη σύνθεση υβριδικού cloud. Για παράδειγμα, ένας οργανισμός μπορεί να αποθηκεύει ευαίσθητα δεδομένα πελατών στο σπίτι σε μια privatecloud εφαρμογή, αλλά διασυνδέεται σε εφαρμογή επιχειρηματικών πληροφοριών που παρέχονται από ένα δημόσιο cloud ως μια υπηρεσία λογισμικού. Αυτό το παράδειγμα του υβριδικού cloud επεκτείνει τις δυνατότητες της επιχείρησης δίνοντας μια συγκεκριμένη υπηρεσία προσθέτοντας εξωτερικές διαθέσιμες publiccloud υπηρεσίες. Υβριδική έκδοση toucloud εξαρτάται από έναν αριθμό παραγόντων όπως οι απαιτήσεις ασφάλειας των δεδομένων, το επίπεδο του ελέγχου που απαιτείται πάνω στα δεδομένα καθώς και το είδος των εφαρμογών που χρησιμοποιεί ένας οργανισμός. Ένα άλλο παράδειγμα υβριδικού cloud είναι εκείνο όπου οι οργανισμοί χρησιμοποιούν πόρους του publiccloud για την κάλυψη προσωρινών αναγκών που δεν μπορούν να καλυφθούν από το privatecloud. Αυτή η δυνατότητα επιτρέπει στα υβριδικά clouds να απασχολεί πόρους από αλλα clouds ανάλογα με τις ανάγκες τους.

1.3.3Κοινοτικό Σύννεφο (Communitycloud).

ToCommunitycloud μοιράζετε τις υπηρεσίες και τους πόρους με διάφορους οργανισμούς που έχουν κοινές ανησυχίες (ασφάλεια, δικαιοδοσία κ.λπ.). Μπορεί να διαχειριστεί είτε εσωτερικά είτε από τρίτους. και είτε και αυτοί το διαχειρίζονται εσωτερικά είτε εξωτερικά. Οι δαπάνες διαμοιράζονται σε λιγότερους χρήστες από ένα publiccloud αλλά περισσότερους από ένα private. Έτσι πολλές φορές καταφέρνουμε την μείωση στο κόστος [10, 11].

1.4Ubigiutouscomputing.

Το ubigiutous computing είναι μια προηγμένη έννοια του computing, όπου ένα υπολογιστικό σύστημα γίνεται να εμφανίζεται παντού και οπουδήποτε. Σε αντίθεση με το παραδοσιακό desktop computing το ubigiutous computing μπορεί να συμβεί χρησιμοποιώντας οποιαδήποτε συσκευή, σε οποιαδήποτε θέση, και σε οποιαδήποτε μορφή. Ένας χρήστης αλληλεπιδρά με τον υπολογιστή, τον οποίον μπορεί να υπάρχει σε πολλές διαφορετικές μορφές τερματικών, συμπεριλαμβανομένων των φορητών υπολογιστών, τα tablet και τα τηλέφωνα. Οι βασικές τεχνολογίες για την υποστήριξη του ubigiutous compiting περιλαμβάνει νέα τεχνολογικά υλικά όπως το προηγμένα middleware, λειτουργικά συστήματα, αισθητήρες, μικροεπεξεργαστές, δίκτυα, πρωτόκολλα επικοινώνιας και το διαδίκτυο. [1].

Η σύνδεση του ubigiutous computing με το cloud computing είναι ότι το ubigiutous είναι η έννοια ενώ το cloud computing είναι ένα επιχειρηματικό μοντέλο που την πραγματοποιεί. Cloud Computing είναι μια επανάσταση που θα καθορίσει όλα τα IT την δεύτερη δεκαετία του 21ου αιώνα. Αυτή η νέα μορφή του μοντέλου computing είναι απολύτως έτοιμη να δώσει λύσεις σε μια σειρά προβλημάτων των επιχειρήσεων στο πλαίσιο των μικρών και μεγάλων οργανισμών.

Είναι ένα επιχειρηματικό μοντέλο παροχής υπηρεσιών που υιοθετεί τις έννοιες του grid computing και utility computing. Μέσα από το cloud μπορείς να συλλέξεις τους πόρους του υπολογιστή από πολλαπλές τοποθεσίες για την επίτευξη ενός κοινού στόχου. Αυτοί οι πόροι μπορεί να είναι υπολογιστικοί πόροι, υπηρεσίες ή χορός αποθήκευσης και να υπολογίζονται σαν μια μετρήσιμη υπηρεσία όπως είναι το νερό και το ηλεκτρικό ρεύμα! Τέλος με βάση την

τεχνολογία του virtualization το cloud computing υλοποιεί τον διαχωρισμό της παραδοσιακής εξάρτησης των προγραμμάτων με το λειτουργικό σύστημα και αυτό με το hardware.

Σύμφωνα με το Cloud computing manifesto, τα βασικά χαρακτηριστικά του cloud είναι η δυνατότητα της δυναμικής κλιμάκωσης της υπολογιστικής ισχύος με έναν αποδοτικό τρόπο και η δυνατότητα του καταναλωτή να έχει το μεγαλύτερο μέρος αυτής τις ισχύος χωρίς να χρειάζεται να διαχειριστεί την πολυπλοκότητα της υποκείμενης τεχνολογίας [2].

Για να κατανοήσουμε όμως βαθύτερα τον ορισμό του cloudcomputing θα πρέπει να αναλύσουμε λίγο περισσότερο τις τρεις βασικές έννοιες που συνυπάρχουν μαζί του, το gridcomputing, το utilitycomputing και το virtualization.

1.5GridComputing.

Στο παρελθόν υπήρχαν δυο τρόποι για να δημιουργηθεί ένας υπέρ-υπολογιστής. Πρώτα υπάρχει η προσέγγιση του στυλ BlueGene, η οποία δημιουργεί έναν τεράστιο υπολογιστή με εκατοντάδες ίσως και πολύ περισσότερους επεξεργαστές. Η άλλη προσέγγιση που υιοθετήθηκε από την Google είναι αποκτώντας έναν τεράστιο αριθμό από μικρούς και χαμηλού κόστους υπολογιστές να τους ενσωματώσεις σε έναν cluster με τέτοιο τρόπο ώστε να δουλεύουν όλοι μαζί σαν ένας πολύ μεγάλος υπέρ-υπολογιστής. Βασικά οι υπέρ-υπολογιστές έχουν πολλούς επεξεργαστές τοποθετημένους σε ένα και μοναδικό μηχάνημα, και μοιράζονται κοινή μνήμη και I/O, ενώ οι cluster είναι δημιουργημένοι από πολλούς μικρότερους υπολογιστές κάθε ένας από τους οποίους περιέχουν τη δική τους μνήμη και I/O.

Παλιότερα οι υπολογιστές ενωνόντουσαν σε έναν cluster για να δημιουργήσουν το επιθυμητό αποτέλεσμα δηλαδή τον υπέρ-υπολογιστή. Αυτή η τεχνολογία ήταν γνωστή στη βιομηχανία και χρησιμοποιούνταν από πολλές εταιρίες πληροφορικής. Αυτή η τεχνολογία επέτρεπε να παραμετροποιήσεις έναν υπολογιστή στο να επικοινωνεί με άλλους με πρωτόκολλα ειδικά σχεδιασμένα για να εξισορροπούν τον υπολογιστικό φόρτο μεταξύ των μηχανημάτων. Σαν χρήστης δεν σε ενδιέφερε ποια κεντρική μονάδα εργασίας χρησιμοποιούσες για να τρέξεις το πρόγραμμα σου και ο cluster έδινε την εγγύηση ότι ο κώδικας θα τρέξει στην καλύτερη δυνατή διαθέσιμη μονάδα εκείνη τη στιγμή.

Στις αρχές της δεκαετίας του '90 οι IanFoster και CarlKesselman έφεραν στην επιφάνεια μια νέα ιδέα που ονομάστηκε “Grid”. Η αναλογία που χρησιμοποιήθηκε για την ιδέα αυτή ήταν το ηλεκτρικό διασυνδεδεμένο δίκτυο όπου οι χρήστες θα μπορούσαν να συνδεθούν στο Grid και να χρησιμοποιήσουν μια μετρήσιμη υπηρεσία. Αν οι εταιρίες μπορούν χωρίς να έχουν την δική τους ηλεκτρική παραγωγή, και όμως να χρησιμοποιούν ηλεκτρικό ρεύμα εξωτερικού παρόχου, γιατί αυτό να μην μπορεί να γίνει και με την υπολογιστική ισχύ; Να συνδέεσαι σε ένα Grid (πλέγμα) 34 υπολογιστών και να πληρώνεις για ότι χρησιμοποιείς. Η τεχνολογία του Grid επεκτείνει τις τεχνικές του cluster, όπου πολλοί διασυνδεδεμένοι ανεξάρτητοι clusters μπορούν να λειτουργήσουν σαν πλέγμα αλλά και παρά τη φύση τους να λειτουργήσουν σε ένα μοναδικό domain.

Η διαχείριση της αποθήκευσης, η επίβλεψη της ασφάλειας και η μετακίνηση δεδομένων ήταν το βασικό πρόβλημα που έπρεπε να επιλυθεί έτσι ώστε να μπορεί να αναπτυχθεί το Grid. Ένα σύνολο από εργαλεία ονομαζόμενο Globus δημιουργήθηκε για να επιλύσει αυτά τα θέματα, αλλά σε επίπεδο υποδομών hardware δεν υπήρχε ακόμα η διαθεσιμότητα και η πρόοδος σε ένα τέτοιο επίπεδο που να επιτρέπει τη πραγματική και καθολική επιτυχία του Grid.

Πιο σημαντικά όμως από αυτούς τους τεχνικούς περιορισμούς ήταν η έλλειψη από επιχειρήσεις για να το αγοράσουν. Η φύση του Grid σημαίνει ότι οι επιχειρήσεις θα πρέπει να μεταφέρουν τα δεδομένα και τις εφαρμογές τους σε μια λύση που προσφέρεται από μία τρίτη εταιρία-επιχείρηση. Αυτό δημιουργούσε πολύ μεγάλα εμπόδια στο ξεκίνημα της τεχνολογίας. Άλλο κομβικό ζήτημα που έπρεπε να διευθετηθεί ήταν η ασφάλεια δεδομένων και η εμπιστευτικότητα. Για πολλές επιχειρήσεις τα δεδομένα τους είναι υπερβολικά ευαίσθητα και είναι πολύ κρίσιμα για τον ίδιο τον επιχειρηματικό τους σκοπό. Το να δοθούν αυτά σε μια τρίτη επιχείρηση δεν θα ήταν καθόλου απλό και μάλιστα σχεδόν απίθανο να συμβεί. Για παράδειγμα οι τράπεζες ήταν πρόθυμες να αναθέσουν ένα τμήμα από τις υπηρεσίες τους αλλά ήθελαν να κρατήσουν τον έλεγχο από το hardware και το λογισμικό, χρησιμοποιώντας την εταιρία που θα ανέθετε τα δεδομένο σαν ένα χώρο εύρεσης προσωπικού.

Πηγαίνοντας το Grid ένα βήμα πιο μπροστά στην παροχή υπηρεσίας είναι το Cloud. Αυτό ενσωματώνει ιδέες από το gridcomputing και τις ολοκληρώνει σε υπηρεσίες που προσφέρονται από datacenters. Η άνοδος της εποχής του Cloud είναι μια ευρέως διαδεδομένη εξέλιξη εξαπλωμένη σε πολλά διαφορετικά hardware και τεχνολογίες καθώς και σε υποδομές και επίπεδα σύστασης. Πρώιμες προσπάθειες για την δημιουργία στάνταρντ ήταν μάλλον αδύναμες, γιατί το Cloud προήλθε από τον ιδιωτικό τομέα (Caryeretal. 2009). Μια τέτοια διασπαρμένη ανάπτυξη με πολύ λίγα τυποποιημένα στάνταρντ, ο κάθε πάροχος έχει αναπτύξει τη δική του υποδομή Cloud αντί να χρησιμοποιεί τις ήδη κανονικοποιημένες ρυθμίσεις, μια πολύ συγγενική κατάσταση με την εμφάνιση του TCP. Αυτή η εκ των έσω οπτική έχει κρατήσει αρκετά πίσω τη διαδικασία θέσπισης κανόνων .

Αν ορίσουμε την έννοια του Grid Computing σαν ορισμός είναι ότι το Grid Computing είναι μια μορφή κατανεμημένου υπολογιστικού συστήματος, όπως ένας εικονικός υπέρ υπολογιστής, που αποτελείτε από μια συστάδα συνδεδεμένων συστημάτων, τα οποία συνεργούν για να βγάλουν εις πέρας μεγάλες εργασίες. Με άλλα λόγια είναι ένα υπολογιστικό πλέγμα το οποίο χρησιμοποιεί τους πόρους από πολλούς υπολογιστές σε ένα δίκτυο το οποίο μπορεί να είναι τοπικό (LAN), δίκτυο ευρείας περιοχής (WAN) ή το διαδίκτυο(internet), για την επίλυση ενός μοναδικού προβλήματος την ίδια στιγμή [3, 4].

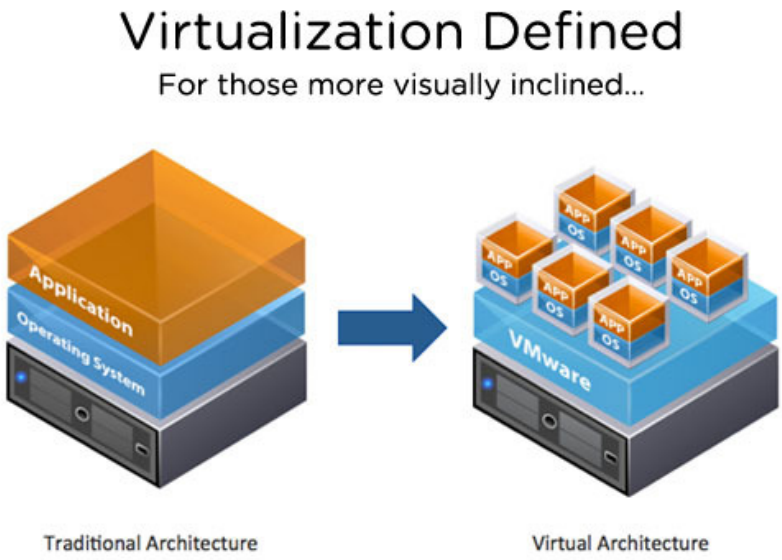
1.6UtilityComputing.

Το UtilityComputing είναι ένα μοντέλο στην παροχή υπηρεσιών στην οποία ένας πάροχος υπηρεσιών κάνει τους υπολογιστικούς πόρους και της διαχείρισης της υποδομής να είναι στη διάθεση του πελάτη, όπως απαιτείται, και τους χρεώνει για συγκεκριμένη χρήση και όχι με σταθερή χρέωση. Όπως και τα άλλα είδη του on-demandcomputing (όπως το gridcomputing), το utilitycomputing επιδιώκει να μεγιστοποιήσει την αποτελεσματική χρήση των πόρων ή / και την ελαχιστοποίηση των περιφερειακών δαπανών. Το utilitycomputing είναι το πακέτο των υπολογιστικών πόρων, όπως ο υπολογισμός των cpu's, χώροι αποθήκευσης και υπηρεσίες, ως μετρητή υπηρεσία. Αυτό το μοντέλο έχει το πλεονέκτημα του χαμηλού ή καθόλου αρχικού κόστους για την απόκτηση των υπολογιστικών πόρων. Πλέον οι υπολογιστικοί πόροι ουσιαστικά ενοικιάζονται.

Αυτό το πακέτο των υπηρεσιών πληροφορικής έγινε το θεμέλιο της αλλαγής στο "ondemand" λογισμικό ως υπηρεσία και cloudcomputing μοντέλα που διαδίδει περαιτέρω την ιδέα των υπολογιστών, εφαρμογών και δικτύων, ως υπηρεσία. Με λίγα λόγια είναι ο συνδυασμός υπολογιστικών πόρων ως μια μετρήσιμη υπηρεσία παρόμοια με τις υπηρεσίες κοινής ωφέλειας (όπως ηλεκτρικό ρεύμα, νερό, φυσικό αέριο και τηλέφωνο) [5].

1.7 Εικονικοποίηση(Virtualization).

Στηνεπιστήμη της πληροφορικής, ηεικονικοποίηση(virtualization) είναι ένας ευρύς όρος τωνυπολογιστικών συστημάτωνπου αναφέρεται σε έναν μηχανισμό αφαίρεσης στοχευμένο στην απόκρυψη λεπτομερειών της υλοποίησης και της κατάστασης ορισμένων υπολογιστικώνπόρωναπό τους πελάτες (π.χ.εφαρμογές, άλλα συστήματα, χρήστες κλπ). Η εν λόγω αφαίρεση μπορεί είτε να αναγκάζει έναν πόρο να συμπεριφέρεται ως πλειάδα πόρων (π.χ. μία συσκευή αποθήκευσης σεδιακομιστήτοπικού δικτύου), είτε πολλαπλούς πόρους να συμπεριφέρονται ως ένας (π.χ. συσκευές αποθήκευσης σεκατανεμημένα συστήματα). Η εικονικοποίηση δημιουργεί μία εξωτερική διασύνδεση οποία αποκρύπτει την υποκείμενη υλοποίηση (π.χ.πολυπλέκονταςτην πρόσβαση από διαφορετικούς χρήστες). Αυτή η προσέγγιση στην εικονικοποίηση αναφέρεται ως*εικονικοποίηση πόρων*. Μία άλλη προσέγγιση της ίδιας όμως νοοτροπίας είναι η*εικονικοποίηση πλατφόρμας*, όπου η αφαίρεση που επιτελείται προσομοιώνει ολόκληρους υπολογιστές. Το αντίθετο της εικονικοποίησης είναι ηδιαφάνεια. Στην περίπτωση της εικονικοποίησης ένας εικονικός πόρος είναι ορατός και αντιληπτός αλλά στην πραγματικότητα ανύπαρκτος, ενώ ένας διαφανής πόρος είναι υπαρκτός αλλά αόρατος.



Εικόνα 3: Virtualization.

Υπάρχουν τρεις τρόποι για να δημιουργηθούν εικονικοί διακομιστές:

- full virtualization
- para-virtualization
- OS-level virtualization

Όλοι μοιράζονται μερικά κοινά χαρακτηριστικά. Ο φυσικός server ονομάζεταιhost. Οι virtualservers ονομάζονται guests. Οι virtualservers συμπεριφέρονται σαν φυσικές μηχανές. Κάθε σύστημα χρησιμοποιεί μια διαφορετική προσέγγιση για την κατανομή φυσικών πόρων του διακομιστή σε εικονικές ανάγκες του διακομιστή.

1.7.1 Fullvirtualization.

Η πλήρης εικονικοποίηση χρησιμοποιεί ένα ειδικό είδος λογισμικού που ονομάζεται hypervisor. Το hypervisor αλληλεπιδρά άμεσα με την CPU και τον χώρο στο σκληρό δίσκο του

φυσικού server του. Χρησιμεύει ως μια πλατφόρμα για τα λειτουργικά συστήματα των virtualservers. Το hypervisor κρατά κάθε εικονικό διακομιστή εντελώς ανεξάρτητο και αγνοούν τους άλλους εικονικούς διακομιστές που λειτουργούν με τη φυσική μηχανή. Κάθε guestserver κινείται με δικά του OS - μπορείτε να έχει ακόμη και ένα guest να τρέχει στο Linux και έναν άλλον για τα Windows.

Το hypervisor παρακολουθεί τους πόρους του φυσικού server του. Καθόλη την διάρκεια ενός virtualserver που εκτελεί εφαρμογές ο hypervisor απορροφά τους πόρους από την φυσική μηχανή ώστε να τις μεταδώσει στο virtualserver. Hypervisors έχουν τις δικές τους ανάγκες επεξεργασίας, πράγμα που σημαίνει ότι ο φυσικός server πρέπει να σπαταλήσει κάποια επεξεργαστική ισχύ και τους πόρους για να εκτελέσει την εφαρμογή hypervisor. Αυτό μπορεί να επηρεάσει τη συνολική απόδοση του server και να επιβραδύνει τις εφαρμογές. Είναι δυνατόν να προσομοιώνονται ταυτόχρονα πολλαπλές εικονικές μηχανές, εντελώς απομονωμένες μεταξύ τους, από τον ίδιο hypervisor. Η εικονικοποίηση πλατφόρμας και του hypervisorεμφανίστηκε αρχικά τη δεκαετία του 1960, πριν από την επέλαση των μικροϋπολογιστών σε μεγάλα συγκεντρωτικά συστήματα (mainframes), αλλά μετά το2000και την αλματώδη αύξηση των επιδόσεων του υλικού τωνPCέχει γίνει πλέον κοινή πρακτική.

1.7.2 Paravirtualization.

Η προσέγγιση παρα-virtualization είναι λίγο διαφορετική. Σε αντίθεση με την πλήρη τεχνική virtualization, οι διακομιστές των επισκεπτών σε ένα σύστημα παρα-εικονικοποίησης γνωρίζουν το ένα το άλλο. Ένα hypervisor στην παρα-εικονικοποίηση δεν χρειάζεται τόσο πολύ επεξεργαστική ισχύ για να διαχειρίζεται τα λειτουργικά συστήματα επισκεπτών επειδή κάθε λειτουργικό σύστημα έχει ήδη επίγνωση των αιτημάτων των άλλων λειτουργικών συστημάτων που βρίσκονται στον φυσικό server. Ολόκληρο το σύστημα λειτουργεί μαζί ως μία συνεκτική μονάδα.

1.7.3 OS-levelvirtualization.

Μια προσέγγιση του virtualization σε επίπεδο λειτουργικού συστήματος δεν χρησιμοποιεί ένα hypervisor σε όλους. Αντ 'αυτού, η δυνατότητα virtualization είναι μέρος του hostOS, το οποίο εκτελεί όλες τις λειτουργίες ενός πλήρως virtualizedhypervisor. Ο μεγαλύτερος περιορισμός αυτής της προσέγγισης είναι ότι όλοι οι guestservers πρέπει να εκτελούν το ίδιο λειτουργικό σύστημα. Κάθε εικονικός διακομιστής παραμένει ανεξάρτητος από όλα τα άλλα, αλλά δεν μπορεί να αναμίξει και να ταιριάξει τα λειτουργικά συστήματα μεταξύ τους. Επειδή όλα τα λειτουργικά συστήματα των guest πρέπει να είναι το ίδιο, αυτό ονομάζεται ένα ομοιογενές περιβάλλον [6, 7].

1.8Εφαρμογές.

Οι εφαρμογές που παρέχονται χωρίζονται σε τέσσερις βασικές κατηγορίες. Τις υπηρεσίες πληροφορικής (CloudITServices), τις εμπορικές εφαρμογές (BusinessApplications), τις εφαρμογές ενίσχυσης παραγωγικότητας (ProductivityApplications) και τις εφαρμογές κοινωνικής δικτύωσης (SocialMediaApplications).

Τα πλεονεκτήματα που προσφέρουν οι cloud εφαρμογές είναι τα εξής [16]:

- Αδιάλειπτη διαθεσιμότητα αποθηκευτικούχώρου.
- Οργανωμένη με προδιαγραφές αποθήκευση.
- Διαβαθμισμένη πρόσβαση από οποιοδήποτε σημείο.

- Τήρηση αντιγράφων ασφαλείας.
- Δυνατότητα αναζήτησης και ομαδοποίησης/ταξινόμησης με πολλαπλά κριτήρια.
- Σημαντική εξοικονόμηση πόρων για την δημιουργία φιλοξενία και ανταλλαγή δεδομένων.
- Συγκέντρωση των βιομηχανικών συστημάτων κάτω από κοινές προδιαγραφές και υποδομές.
- Ομοιογένεια των εφαρμογών για την εύκολη ανταλλαγή δεδομένων μεταξύ των βιομηχανιών.
- Αποφυγή επανεκπαίδευσης προσωπικού κατά την μετάθεση από τη μια θέση στην άλλη.
- Εξοικονόμησηενέργειας.

Κεφάλαιο 2: Ιστορική αναδρομή

Η πρώτη επιστημονική χρήση του όρου cloudcomputing έγινε σε μια διάλεξη το 1997 από τον ChellappaRamnath.

Το cloudcomputing μπορεί να φαίνεται σαν ένα σχετικά νέος όρος αλλά στηρίζεται σε πολλά χρόνια κατανεμημένων τεχνολογιών. Ο πραγματικός όρος «νέφος» προέρχεται από την τηλεφωνία όπου οι τηλεπικοινωνιακές εταιρίες που μέχρι το 1990 προσέφεραν κύριος αποκλειστικά point το point κυκλώματα άρχισαν να προσφέρουν υπηρεσίες Εικονικών Ιδιωτικών Δικτύων (VirtualPrivateNetwork – VPN) με συγκρίσιμη ποιότητα υπηρεσίας αλλά και με χαμηλότερο κόστος.

Το σύμβολο του νέφους χρησιμοποιήθηκε για να υποδηλώσει το σημείο οριοθέτησης ανάμεσα σε αυτό που είναι ευθύνη του παρόχου και αυτό που είναι ευθύνη του χρήστη. Το νέφος επεκτείνει αυτό το όριο για να καλύψει servers καθώς και υποδομή δικτύου. Από την δεκαετία του 1960 το νέφος έχει αναπτυχθεί σε πολλά επίπεδα. Παρόλα αυτά είχε αργή ανάπτυξη για το κοινό μέχρι την δεκαετία του 1990 που το διαδίκτυο άρχισε να προσφέρει σημαντικό εύρος ζώνης. Ένα από τα πρώτα ορόσημα στην εξέλιξη του νέφους ήταν η άφιξη της Salesforce.com το 1999, που πρωτοπόρησε την ιδέα της παροχής εφαρμογών σε επιχειρήσεις μέσω ενός απλού website. Η εταιρία άνοιξε τον δρόμο σε εξειδικευμένες και μη εταιρείες να παρέχουν εφαρμογές μέσω διαδικτύου.

Η Amazon έπαιξε καθοριστικό ρόλο στην εξέλιξη του νέφους εκσυγχρονίζοντας τα κέντρα δεδομένων τα οποία όπως τα περισσότερα δίκτυα υπολογιστών χρησιμοποιούσαν το 10% της χωρητικότητας τους κάθε χρονική στιγμή. Αφού διαπιστώθηκε ότι η αρχιτεκτονική του νέφους οδήγησε σε σημαντικές βελτιώσεις στην απόδοση η Amazon ξεκίνησε μια προσπάθεια ανάπτυξης νέων προϊόντων για παροχή υπηρεσιών σε εξωτερικούς πελάτες και εισήγαγε το AmazonWebService το 2006. Στις αρχές του 2008 το Eucalyptus έγινε η πρώτη AWSAPIplatform ανοιχτού κώδικα για την ανάπτυξη ιδιωτικών νεφών. Ένα μεγάλο βήμα έγινε το 2009 καθώς το Web 2.0 έφτασε στο απόγειο του ενώ η Google και άλλες εταιρείες άρχισαν να προσφέρουν browser-based επιχειρησιακές εφαρμογές όπως το GoogleApps. Τον Μάρτιο του 2010 ο SteveBallmer της Microsoft δήλωσε «το 75% των ανθρώπων μας χρησιμοποιούν αποκλειστικά εξ ολοκλήρου το νέφος, σε ένα χρόνο από τώρα το ποσοστό αυτό θα είναι 90%» [12, 13, 14, 15].

Η ιστορική αναδρομή δεν θα μπορούσε να μην περιέχει τους πρωτοπόρους στην ιστορία της δημιουργίας του cloudcomputing. Το cloudcomputing θα μπορούσαμε να δηλώσουμε ότι δεν έχει έναν πατέρα αλλά πολλά άτομα που σίγουρα συντέλεσαν μεγάλη επιρροή και έμπνευση. Ας αναφέρουμε μερικούς από τους “πατεράδες” και να πούμε δυο λόγια για τον καθένα.

2.1 Douglas F.Parkhill.

Ήταν ο συγγραφέας του βιβλίου, του1966, *The Challenge of the Computer Utility*. Στο βιβλίο ο Parkhill διερευνά σε βάθος πολλά από τα σύγχρονα χαρακτηριστικά του cloudcomputing (ελαστική τροφοδότηση μέσω μιας υπηρεσίας κοινής ωφέλειας) καθώς και τη σύγκριση με τη βιομηχανία ηλεκτρικής ενέργειας.

2.2 JohnMcCarthy.

Το1961ήταν ο πρώτος που πρότεινε δημόσια (σε μια ομιλία που έδωσε για να γιορτάσει τα εκατό χρόνια του MIT) ότι η τεχνολογία πολυχρηστικής πολυδιεργασίας στα υπολογιστικά συστήματα(«*χρονομερισμός*»), μπορεί στο μέλλον να χρησιμοποιηθεί για πώληση υπολογιστικής ισχύος μέσω δικτύων χρήσης κοινής ωφέλειας (όπως συμβαίνει με την ύδρευση ή την ηλεκτρική ενέργεια). Η ιδέα αυτή ήταν πολύ δημοφιλής προς το τέλος της δεκαετίας του '60 αλλά εξασθένησε μέχρι τα μέσα της δεκαετίας του '70 καθώς έγινε σαφές ότι τουλικό, το λογισμικό και οι υφιστάμενες τεχνολογίες τηλεπικοινωνιών δεν ήταν ακόμη έτοιμες. Εντούτοις από το 2000 η ιδέα έχει έρθει ξανά στην επιφάνεια με νέες μορφές και στηριγμένη στοΔιαδίκτυο (cloudcomputing)

2.3 J.C.R. Licklider.

Ο Licklider έπαιξε μεγάλο ρόλο στη σύλληψη και τη χρηματοδότηση της έρευνας που κατέληξε στοARPAnet (AdvanceResearchProjectsAgencyNetwork).Αυτός διατύπωσε τις πρώτες ιδέες ενός παγκόσμιου δικτύου ηλεκτρονικών υπολογιστών τον Αύγουστο του 1962 στο BBN σε μια σειρά από υπομνήματα συζητώντας την έννοια « διαγαλαξιακό δίκτυο υπολογιστών».Αυτές οι ιδέες περιέχονται στην ιδέα του Διαδικτύου όπως είναι σήμερα συμπεριλαμβανομένου βέβαια και του υπολογιστικού νέφους.

2.4 JohnKemenyandThomasKurtz.

Οι καθηγητές του DartmouthKemeny και Kurtz είχαν σχεδιάσει μια βασική γλώσσα προγραμματισμού που επιτρέπει στους μαθητές να γράψουν τα προγράμματα σχετικά με το σύστημα DartmouthTimeSharing (DTSS) την πρώτη επιτυχημένη μεγάλης κλίμακας εφαρμογή του time-sharing το 1964. Η τεχνολογία αυτή ονομάζεται χρονομεριστικής μίσθωση και οι υποκείμενες έννοιες όπως απομακρυσμένη πρόσβαση και η κοινή χρήση πόρων ήταν τα αρχικά σημάδια αυτό που είναι τώρα το cloudcomputing. Η εισαγωγή της BASIC λειτούργησε σαν ένα κλειδί για την βασική έννοια της χρήσης τουcloudcomputing.

2.5 MarcBenioff.

Ο MarcBenioff είναι ο πρωτοπόρος που δημιούργησε τον όρο πλατφόρμα ως υπηρεσία (PaaS). Είναι ο συντάκτης τριών βιβλίων συμπεριλαμβανόμενου του εθνικού bestseller «πίσω από το σύννεφο». Ο Benioff αντιπρόεδρος της Oracle από την ηλικία 26 ετών ίδρυσε τηνSalesforce.com το 1999 και παρείχε την λειτουργία softwareasservice σαν ένα μοντέλο που αντικαθιστούσε τα παραδοσιακά λογισμικά για της επιχειρήσεις.

Κεφάλαιο 3: Ασφάλεια στο CloudComputing

Σε αυτό το κεφάλαιο θα μιλήσουμε για την ασφάλεια πάνω στο cloudcomputing. Η ασφάλεια είναι ένας γενικευμένος όρος και για να κατανοήσουμε καλύτερα θα πρέπει να την χωρίσουμε με σημείο αναφοράς την ειδικότητας τις ασφάλειας. Τα διάφορα επίπεδα που είναι διαχωρισμένη η ασφάλεια είναι τα εξής:

- Ασφάλεια διασύνδεσης,
- Ασφάλεια επιπέδου SaaS,
- Ασφάλεια επιπέδουPaas,
- Ασφάλεια επιπέδουIaas,
- Ασφάλεια στην ακεραιτότητα τον δεδομένων,
- Ασφάλεια περιβάλλοντος (environment control, equipment maintenance, location and protection) (philosophy of csp security).

Η αν το πάρουμε με την σειρά τις πρόσβασης και ποιο γενικευμένα, τα επίπεδα ασφάλειας σαν securitylayer είτε σαν securitylevels είναι τα εξής.

- level 1: Physical level of security,
- level 2: network security,
- level 3: Os καιApplication security.

Όπωςείναικατανοητότοεπίπεδοασφάλειαςπεριβάλλοντοςανήκειστολevel 1 αλλά η ασφάλεια ακεραιότητας τον δεδομένων και η ασφάλεια επιπέδου SaaS ανήκουν στον level 3. Σε όλα τα πράγματα πάντα υπάρχουν δυο όψεις του νομίσματος για αυτό πριν αναπτύξουμε την ιδέα της ασφάλειας στο cloud ας κάνουμε μια αντιφατική κίνηση και ας αναλύσουμε για αρχή τα πρόβλημα και την "ανασφάλεια" του cloud.

3.1ΕπίπεδαΑσφαλείαςcloud (Security Levels).

3.1.1 Level 1:physicallevelofsecurity.

Η ασφάλεια του περιβάλλοντος βασίζεται στην εμπιστοσύνη του προμηθευτή του cloud . Είναι η ασφάλεια που έχει η υποδομή και η φυσική θέση των βάσεων δεδομένων. Για να υπάρχει ένα στάνταρ ικανοποιητικής ασφάλειας θα πρέπει ο χορός που λειτουργεί το cloud να φυλάσσεται από φύλακες που να τηρούν βάρδιες, να υπάρχει κλειστό κύκλωμα παρακολούθησης, περίφραξη και αποκλεισμό από εξωτερική επικοινωνία η υποδομή. Μέτρα συντήρησης τις υποδομής και πλάνο σχεδίου εκτάκτου ανάγκης σε κατάσταση φυσικής καταστροφής όπως είναι η φωτιά, ο σεισμός, η πλημμύρα κ.τ.λ..

Μέσα στην ασφάλεια του περιβάλλοντος ανήκει επίσης και αρχιτεκτονική τις υποδομής. Η εγκατάσταση firewall ενισχύουν την ασφάλεια σε επίθεση όπως και η εγκατάσταση ενός αριθμού ups ενισχύουν την ασφάλεια σε έκτακτη ανάγκης έλλειψης τροφοδοσίας.

3.1.2 Level 2: network level of security.

ToNetworksecurityείναιηασφάλειαδιασύνδεσης. Είναι η ασφάλεια που πρέπει να παρέχεται στον χρήστη από την στιγμή που τα δεδομένα του έχουν φύγει από τις βάσεις δεδομένων μέχρι να φτάσουν στο δικό του υπολογιστή. Η ασφάλεια σε αυτόν τον τομέα δεν έχει κάποια αξιόλογη διαφορά από την ασφάλεια που υπάρχει γενικός στο internet. Κανένας χρήστης του cloud δεν θα ήθελε να πέσει θύμα της επίθεσης maninthemiddle. Για όσους δεν γνωρίσουν η

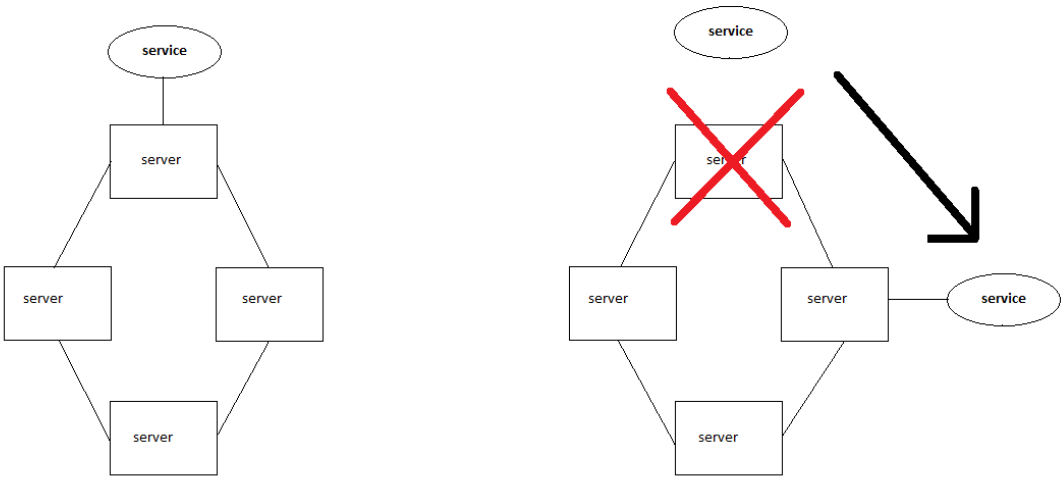
επίθεση είναι μια μορφή υποκλοπής μιας συζήτησης καθώς ο επιτιθέμενος κάνει ανεξάρτητες συνδέσεις με τα θύματα του έχοντας αυτοί άγνοια με ποιον μιλάνε. Στην περίπτωση του cloud θα μπορούσε ο επιτιθέμενος να κλέψει τα αρχεία μας είτε να υποκλέψει τα ιδιωτικά κλειδιά τις επικοινωνίας μας με τον διακομιστή του cloud και να τα χρησιμοποιήσεις με δικιά του βούληση. Η αποφυγή αυτόν τον επιθέσεων και κάθε είδος επιθέσεων υποκλοπής δεδομένων στην επικοινωνία επιτυγχάνεται ως έναν βαθμό με τις επεκτάσεις στην ασφάλεια του DNS (DNSEC) , τους αλγορίθμου κρυπτογράφησης και τα πρωτόκολλα ασφάλειας.

Ας δούμε κάποια από τα κυριότερα και τα ποιο διαδεδομένα πρωτόκολλα ασφάλειας όπως ssl, ssh, ipsec κ.τ.λ..

3.1.3 Level 3: OSκαιApplicationsecurity.

Σε αυτό το level εμπεριέχονται i και τα περισσότερα επίπεδα ασφάλειας. Όπως το επίπεδο application, iaas, paas όπως και ένα μέρος τις ασφάλειας της ακεραιότητας των δεδομένων το υπόλοιπο ανήκει στο level 2 Ασφάλεια προσδίδει και το operatingsystem που μέσα από την λειτουργία του virtualmachine είναι η γέφυρα που συνδέει το hardware με το software όπως και στα κοινά πρότυπα τις αρχιτεκτονικής ενός υπολογιστικού συστήματος αλλά από την άλλη στην συγκεκριμένη περίπτωση απαγκιστρώνει την εξάρτηση του software από το hardware.

Στο cloud δεν έχουμε operatingsystem σαν τα windows ή τα linux που έχουμε στο προσωπικά μας pc. Αρχικά έχουμε να κάνουμε με virtualization και πρώτα πριν βάλουμε OSθα χρειαστούμε hypervisor. Έτσι ένα είδος ασφάλειας είναι ότι το λειτουργικό σύστημα και τα service που παρέχει ο provider δεν συνδέονται άμεσα με το hardware. Λειτουργούν σε κυψέλες και αυτό ελαττώνει το κίνδυνο αν πάθει κάτι το hardware κομμάτι δεν θα σταματήσει και την λειτουργία του λειτουργικό σύστημα και μετέπειτα το service που παρέχει. Εφόσον λοιπόν μιλάμε για κυψέλες αυτόματα θα πρέπει να συνειδητοποιήσουμε την διαφορά από το παραδοσιακό σύστημα παροχών υπηρεσιών. Από αυτήν την αρχιτεκτονική τον κυψελών δεν υπάρχει η αυτονομία του server. Το κέρδος στην ασφάλεια είναι ότι αν συμβεί μια βλάβη σε ένα server είτε η συγκεκριμένη βλάβη είναι η διακοπή της τροφοδοσίας είτε η ανταπόκριση ενός επιμέρους συστήματος του hardware για παράδειγμα η διακοπή λειτουργίας σκληρού δίσκου, επεξεργαστή κ.τ.λ. Η υπηρεσία αυτόματα συνεχίζεται σε server της κυψέλης.



Εικόνα 4: Αλλαγή Κυψέλης.

Παρέχονται ασφάλεια για την συνεχόμενη λειτουργία της υπηρεσίας , την ακεραιότητα και την διαθεσιμότητα τον δεδομένων πάνω στο cloud.

3.2Απειλές κατά CSA.

Σύμφωνα με τον οργανισμό CloudSecurityAlliance (CSA) οι 9 πιο σημαντικές απειλές για τον CloudComputing είναι οι ακόλουθες [37]:

3.2.1 Παραβίαση Δεδομένων (Databreaches).

Η συγκεκριμένη απειλή αναφέρεται στο γεγονός πως τα προσωπικά αρχεία χρηστών πέφτουν σε λάθος χέρια.

3.2.2 Απώλεια Δεδομένων (DataLoss).

Επιπλέον υπάρχει η πιθανότητα να χαθούν αρχεία είτε από πρόθεση είτε κατά λάθος.

3.2.3 ΥποκλοπήΛογαριασμώνήΥπηρεσιώνκατά την Μεταφορά (AccountorServiceTrafficHijacking).

Ένας πιθανός επιτιθέμενος μπορεί να χρησιμοποιήσει επιθέσεις τύπου phishing για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό ή τις υπηρεσίες ενός νόμιμου χρήστη.

3.2.4 InsecureInterfacesandAPIs.

Η ασφάλεια του cloudcomputing βασίζεται στην ασφάλεια των διεπαφών και APIs που χρησιμοποιούνται. Συνεπώς, πιθανά κενά ασφάλειας σε αυτά μεταφέρουν άμεσα τις επιπτώσεις στο σύνολο της εγκατάστασης.

3.2.5 Άρνηση Παροχής Υπηρεσιών (DenialofService).

Η άρνηση παροχής υπηρεσιών δεν επιτρέπει σε νόμιμους χρήστες να προσπελάσουν δεδομένα και υπηρεσίες. Κατά την επίθεση αυτή ο επιτιθέμενος δημιουργεί επιπρόσθετη κίνηση με σκοπό να εξαντλήσει τους διαθέσιμους πόρους του συστήματος και να το καταστήσει μη διαθέσιμο.

3.2.6 MaliciousInsiders.

Η εκ των έσω απειλή ορίζει την ύπαρξη ενός επιτιθέμενου που βρίσκεται εσωτερικά του οργανισμού. Το αποτέλεσμα είναι να έχει την πλήρη γνώση των συστημάτων έτσι ώστε να προκαλέσει και την μεγαλύτερη επίπτωση κατά την επίθεση.

3.2.7 Κατάχρηση Υπηρεσιών Νέφους (AbuseofCloudServices).

Η συγκεκριμένη απειλή περιλαμβάνει την εκμετάλλευση των διαθέσιμων πόρων του υπολογιστικού συστήματος για την δημιουργία μιας επίθεσης (π.χ. DOS).

3.2.8 ΑνεπαρκήςΕπιμέλεια (InsufficientDueDiligence).

Επιχειρησιακές ευθύνες όπως η αντιμετώπιση περιστατικών, κρυπτογράφηση και την παρακολούθηση της ασφάλειας περιλαμβάνουν άγνωστα επίπεδα κινδύνου.

3.2.9 SharedTechnologyIssues.

Το γεγονός πως το cloudcomputing προσφέρει τον διαμοιρασμό υπηρεσιών, περιλαμβάνει και τον κίνδυνο μεταφοράς της όποιας απειλής μέσα στο υπολογιστικό περιβάλλον.

3.3Προβλήματα στην ασφάλεια

3.3.1 Άγνωστη Βάση Δεδομένων (Unkowndatabase).

Που βρίσκονται τα αρχεία μας; Όταν μιλάμε για ασφάλεια όλοι στο μυαλό μας έχουμε τους αλγόριθμους κρυπτογράφησης, τα firewalls ή έστω τα antivirus που εγκαθιστούμε στους υπολογιστές μας. Η ασφάλεια όμως είναι κάτι πιο βαθύ. Σε ένα οικιακό δίκτυο ξέρουμε ασυναίσθητα την τοποθεσία τον αρχείων μας. Έτσι η ασφάλεια περιτριγυρίζει αυτά τα αρχεία σαν στρώματα τείχους από το εξωτερικό περιβάλλον και τους κινδύνους. Στην περίπτωση του cloudcomputing αυτό δεν μπορούμε να το γνωρίζουμε. Φυσικά μπορούμε να επικοινωνήσουμε με τον provider μας και να μας αναφέρει που βρίσκονται οι βάσεις δεδομένων. Η απάντηση όμως εξακολουθεί να μην είναι αρκετή. Η εικόνα του cloud που μας έχει δοθεί είναι όπως στην Εικόνα 4 .

Εικόνα 5:CloudComputing.

Μια ουτοπία ότι ο καθένας έχει τα αρχεία του μέσα στο σύννεφο (cloud). Ας δούμε όμως μια πιο ρεαλιστική εικόνα για το που βρίσκονται βάσεις δεδομένων στην Εικόνα 5.Ας συγκρίνουμε τώρα την Εικόνα 5 με τις βάσεις δεδομένων με την Εικόνα 6. Η Εικόνα 6 μας δείχνει τους μολυσμένους υπολογιστές από τον ίο conficker (είναι ένα worm για την ακρίβεια) το έτος 2012 που πρωτοεμφανίστηκε τον Νοέμβριο του 2008. Κανένας δεν θα ήθελε να έχει τα αρχεία του σε μια περιοχή που θεωρείτε "μολυσμένη". Και όμως κανένας δεν το έχει στο μυαλό του όταν μιλάμε για «αποθήκευση στο cloud». Υποσυνείδητα θεωρούμε ότι είναι όλα ασφαλές πάνω στο σύννεφο.

Εικόνα 6: Τοποθεσίες βάσεων δεδομένων.

Εικόνα 7: Μολυσμένοι Υπολογιστές από τον ιό Conficker.

3.3.2 Ένα είδος επιθέσεις είναι η επίθεση στην «επεκτασιμότητα» (scalability).

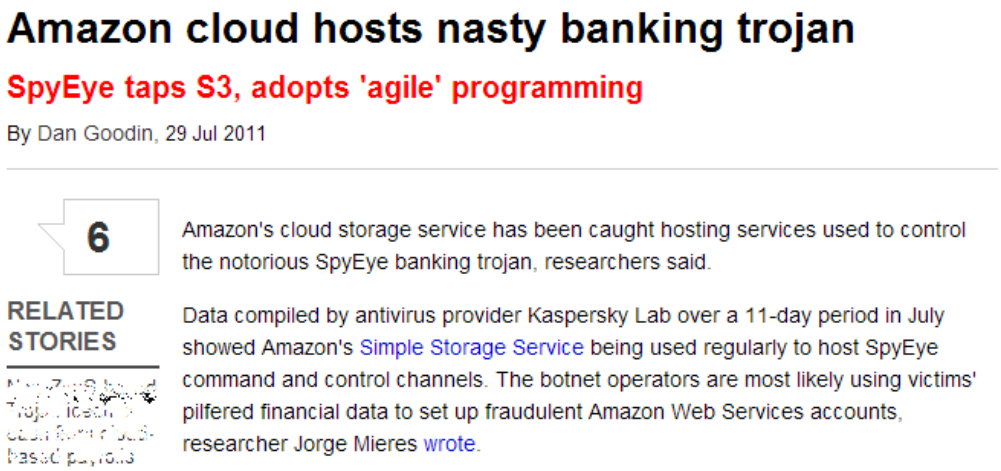
Όταν έχουμε ένα κοινό από πελάτες η λειτουργία τις επεκτασιμότητας μας βοηθά να πληρούμε τις ανάγκες τους έτσι όταν χρειαστούν μεγαλύτερη επεξεργαστική ισχύ να μπορέσει ο provider να τους την παρέχει. Τι θα συμβεί όμως αν δεν έχουμε καλοπροαίρετους πελάτες και έχουμε μια ομάδα από hackers ή ένα botnet και κάνουν μια επίθεση DoS; Έτσι προκαλείται ένα scalingup και αυτό σαν αποτέλεσμα έχει την κακομεταχείριση των πόρων και η άνοδος του κόστους.

Υπάρχει και η αντίθετη πράξη σαν έννοια στην επίθεση στην επεκτασιμότητα. Ένας hackerμπορεί να βρει πρόσβαση στο cloudinfrastructure με αποτέλεσμα να διαχειριστεί την κατανομή των πόρων δίνοντας του την δυνατότητα να προκαλέσει ένα scalingdown. Με τον όρο scalingdown εννοούμε να μην δίνει τους διαθέσιμους πόρους στους πελάτες την ώρα που το χρειάζονται με αποτέλεσμα να μην ικανοποιούνται οι απαιτήσεις των πελατών. Αυτό έχει ως αποτέλεσμα να μην ικανοποιούνται την απαιτήσεις των πελατών και έτσι ο providerνα χάνει πελάτες άρα και έσοδα.

3.3.3 Κατάχρηση των πόρων του νέφους (Abuseofcloudresources).

Φυσικά υπάρχουν και οι επιθέσεις απέναντι στις πηγές τουcloudcomputing. Το cloudcomputing έχει πολλές δυνατότητες να μας βοηθήσει δίνοντας μας πόρους είτε εργαλεία. Αυτές τις δυνατότητες όπως και στην επεκτασιμότητα μπορεί να τις χρησιμοποιήσει και ένας με κακή βούληση είτε hacker είτε ένα botnet. Έχουν συμβεί επιθέσεις όπως ένα cloud να αποθηκεύει

ένα κακόβουλο λογισμικό. Εδώ βλέπουμε hackers να μπορούν να επιτεθούν μέσα από το cloud και τα εργαλεία του σε άλλες εταιρίες.



Amazon cloud hosts nasty banking trojan

SpyEye taps S3, adopts 'agile' programming

By Dan Goodin, 29 Jul 2011

6

Amazon's cloud storage service has been caught hosting services used to control the notorious SpyEye banking trojan, researchers said.

RELATED STORIES

Data compiled by antivirus provider Kaspersky Lab over a 11-day period in July showed Amazon's Simple Storage Service being used regularly to host SpyEye command and control channels. The botnet operators are most likely using victims' pilfered financial data to set up fraudulent Amazon Web Services accounts, researcher Jorge Mieres wrote.

Εικόνα 8:Επίθεση στο Amazoncloud.

Hackers Use Amazon to Crack Apple Users' Clouds

ADAM GAUNTLETT | 8 AUGUST 2012 9:49 PM

18

Phone password resets for Apple ID are frozen for 24 hours as Apple faces a hacking crisis.

Last weekend Wired reporter Mat Honan had his Apple ID hacked, and everything went to hell in a handbasket. His Google account was deleted, his Twitter used to broadcast racist and homophobic messages, and all data was erased on his iPhone, iPad, and MacBook. Honan admits that part of the problem was his habit of using the same security details for each account - something that more than a few people do - but says that the bigger issue was the Cloud and Apple support, which gave the hackers access to everything they wanted so long as they provided Honan's name, address, and email account.

Εικόνα 9:Επίθεση στους χρήστες τουνέφους τηςAppleμε τη χρήση του νέφους τηςAmazon.

Ακόμα και στα μέσα κοινωνικής δικτύωσης (Εικόνα 9).

Hackers use Amazon cloud to scrape mass number of LinkedIn member profiles

EC2 service helps hackers bypass measures designed to protect LinkedIn users.

by **Dan Goodin** - Jan 8 2014, 9:10pm GTBST

HACKING 58

LinkedIn is suing a gang of hackers who used Amazon's cloud computing service to circumvent security measures and copy data from hundreds of thousands of member profiles each day.

Image courtesy of TheTruthAbout.

Image courtesy TheTruthAbout

"Since May 2013, unknown persons and/or entities employing various automated software programs (often referred to as 'bots') have registered thousands of fake LinkedIn member accounts and have extracted and copied data from many member profile pages," company attorneys alleged in a complaint filed this week in US District Court in Northern California. "This practice, known as 'scraping,' is explicitly barred by LinkedIn's User Agreement, which prohibits access to LinkedIn 'through scraping, spidering, crawling, or other technology or software used to access data without the express written consent of LinkedIn or its Members.'"

Εικόνα 10: Επίθεση στο κοινωνικό δίκτυο Linkedinμε τη χρήση του νέφους Amazon.

Τέλος βλέπουμε την «κακή» χρήση του cloud ακόμα και σαν είδος εργασίας στην Εικόνα 10. Με πόρους από cloud να «σπάνε» κωδικούς WPAkey έναντι αμοιβής.

Cloud service cracks VPN passwords in 24 hours

At the Black Hat hacker conference in Las Vegas, encryption expert Moxie Marlinspike promised that his CloudCracker web service was able to crack any VPN or WiFi connection secured using MS-CHAPv2 within 24 hours. The cost? Around $200.

CloudCracker

Εικόνα 11: Υπηρεσία Cloudσπάει VPNκωδικούς εντός 24 ωρών.

Από την άποψη των πραγματικών απειλών σε έναν εικονικό περιβάλλον άρα και στην βάση της δομής του cloudcomputing έχουμε 3 κατηγορίες με επίκεντρο τον hypervisor.

Hyperjacking : Περιλαμβάνει την υπονόμευση του hypervisor ή την εισαγωγή ενός ψευδούς hypervisor. Με άλλα λόγια είναι η ικανότητα του επιτιθέμενου να εγκαταστήσει έναν hypervisor και να πάρει τον έλεγχο του υποκείμενου εξοπλισμό. Ο κίνδυνος αυτής της επίθεσης είναι ότι τα hypervisor τρέχουν στην βάση τον επιπέδων τις ασφαλείας του λογισμικού και είναι σχεδόν αδύνατον να το ανιχνεύσει οποιοδήποτε λειτουργικό σύστημα, κάνοντας τον επιτιθέμενο απόλυτο κυρίαρχο πάνω στο virtualmachine εγκαθιστώντας προγράμματα χωρίς κάποιο λογισμικό να μπορεί να το ανακαλύψει.

VMEscape : Ονομάζεται η επίθεση παράκαμψης τις ασφάλειας τις απομόνωσης τις εικονικής μηχανής και έρχεται σε λειτουργική επαφή με τον εκάστοτε hypervisor.

VMTHIEF: Είναι η ικανότητα ο επιτιθέμενος να κλέψει ένα εικονικό αρχείο ηλεκτρονικά το οποίο στην συνέχεια να μπορεί να το τοποθετήσει και να το τρέξει όπου αυτός το επιθυμεί. Είναι μια επίθεση που είναι ισοδύναμη με το να υπάρχει κλοπή ενός ολόκληρου φυσικού server χωρίς να χρειάζεται να παράκαμψη το φυσικό επίπεδο τις ασφάλειας.

Για αυτό και πολλοί θεωρούν την έννοια του cloudcomputingabuzzword δηλαδή κάτι που έχει υπερεκτιμηθεί μόνο από την ονομασία του και το marketing. Είναι όμως έτσι; Υποκειμενικά ο καθένας θα μπορούσε να καταθέσει την απάντηση του. Εδώ δεν θα απαντήσουμε στην ερώτηση απλά θα αναπτύξουμε την ασφάλεια του cloud [17, 18].

Κεφάλαιο 4: Πρωτόκολλα ασφαλείας

4.1 Layer 2 TunnelingProtocol.

Στην δικτύωση υπολογιστών το Layer 2 πρωτόκολλο σήραγγας (L2TP) είναι ένα πρωτόκολλο που χρησιμοποιείται για τη στήριξη εικονικών ιδιωτικών δικτύων (VPN) ή ως μέρος της παροχής υπηρεσιών από τους ISPs. Δεν παρέχει καμία κρυπτογράφηση ή κάποιο πρωτόκολλο εμπιστευτικότητας από μόνο του. Αντίθετα βασίζεται σε ένα πρωτόκολλο κρυπτογράφησης που περνά μέσα από την σήραγγα για να παρέχει την προστασία των δεδομένων.

Δημοσιεύθηκε το 1999 ως προτεινόμενο πρότυπο RFC 2661. Το L2TP έχει τις ρίζες του κυρίως σε δύο παλαιότερα πρωτόκολλα ενθυλάκωσης για Point-to-Point επικοινωνίες: Layer 2 Πρωτόκολλο της CiscoForwarding (L2F) και USRoboticsPoint-to-PointProtocol (PPTP). Μια νέα έκδοση του εν λόγω πρωτοκόλλου το L2TPv3 δημοσιεύτηκε ως προτεινόμενο πρότυπο RFC 3931 το 2005. Το L2TPv3 παρέχει πρόσθετα χαρακτηριστικά ασφαλείας, βελτιωμένη ενθυλάκωση και την ικανότητα να μεταφέρει δεδομένα συνδέσεις PPP και μέσω ενός δικτύου IP (π.χ., FrameRelay, Ethernet, ATM, κλπ.).

Το σύνολο το πακέτου L2TP συμπεριλαμβανομένου του ωφέλιμου φορτίου και της κεφαλίδας L2TP αποστέλλεται εντός του UserDatagramProtocol (UDP) datagram. Είναι συνηθισμένο να μεταφέρει PPP συνεδρίες μέσα σε μια σήραγγα L2TP. Το L2TP δεν παρέχει την εμπιστευτικότητα ή άλλους τρόπους αυθεντικοποίηση από μόνη της. Το πρωτόκολλο IPsec χρησιμοποιείται συχνά για να εξασφαλίσει ασφάλεια στα πακέτα L2TP παρέχοντας την εμπιστευτικότητα, την ακεραιότητα και την επαλήθευση ταυτότητας. Ο συνδυασμός αυτών των δύο πρωτοκόλλων είναι γενικά γνωστό ως L2TP/IPsec.

Τα δύο άκρα μιας σήραγγας L2TP ονομάζονται LAC (L2TPAccessConcentrator) και LNS (L2TPNetworkServer). Το LAC είναι ο δημιουργός της σήραγγας ενώ το LNS είναι ο server ο οποίος περιμένει για νέες σήραγγες. Μόλις καθιερωθεί μια σήραγγα η κυκλοφορία του δικτύου μεταξύ των δυο σημείων είναι αμφίδρομη. Τα πρωτόκολλα υψηλότερου επιπέδου στη συνέχεια τρέχουν μέσα από τη σήραγγα L2TP. Για να διευκολυνθεί αυτό μια περίοδο λειτουργίας L2TP (ή «κλήση») είναι εγκατεστημένη εντός της σήραγγας για κάθε πρωτόκολλο υψηλότερου επιπέδου όπως το PPP. Είτε το LAC είτε τοLNS μπορεί να κινήσει συνεδρίες. Η κίνηση κάθε συνεδρίας απομονώνεται από το L2TP, ώστε να είναι δυνατή η δημιουργία πολλαπλών εικονικών δικτύων σε ένα ενιαίο τούνελ.

Τα πακέτα που ανταλλάσσονται στο πλαίσιο μιας σήραγγας L2TP κατηγοριοποιούνται είτε ως πακέτα ελέγχου είτε ως πακέτα δεδομένων. Το L2TP παρέχει δυνατότητες αξιοπιστίας για τα πακέτα ελέγχου αλλά καμία αξιοπιστία για τα πακέτα δεδομένων. Η αξιοπιστία εάν είναι επιθυμητό πρέπει να παρέχετε από τα πρόσθετα πρωτόκολλα που τρέχουν σε κάθε σύνοδο της σήραγγας L2TP .

Το L2TP επιτρέπει τη δημιουργία ενός ιδεατού ιδιωτικού δικτύου dialup (VPDN) για να συνδεθεί σε έναν απομακρυσμένο υπολογιστή-πελάτη στο εταιρικό δίκτυό της χρησιμοποιώντας μια κοινή υποδομή η οποία θα μπορούσε να είναι το Διαδίκτυο ή το δίκτυο ενός παρόχου υπηρεσιών.

Μια σήραγγα L2TP μπορεί να επεκταθεί σε μια ολόκληρη συνεδρία PPP ή μόνο στα ένα τμήμα μιας περιόδου δύο τμημάτων. Αυτό μπορεί να αντιπροσωπεύεται από τέσσερα διαφορετικά μοντέλα σηράγγων και ποιό συγκεκριμένα:

- Εθελοντικήσήραγγα(voluntary tunnel),
- Υποχρεωτικήσήραγγα(compulsory tunnel) - εισερχόμενηκλήση,
- Υποχρεωτική σήραγγα(compulsorytunnel) - απομακρυσμένη σύνδεση,
- Σύνδεσης L2TPmultihop.

Ένα πακέτο L2TP αποτελείται από:

Bits 0–15	Bits 16–31
Flags and Version Info	Length (opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset Size (opt)	Offset Pad (opt).....
Payload data	

Πίνακας 1: L2TP.

Σημαίες και έκδοση:
Σημαίες ελέγχου που υποδεικνύει τα πακέτων δεδομένων / ελέγχου με την παρουσία του μήκους και της ακολουθίας.

Μήκος (προαιρετικό):
Συνολικό μήκος του μηνύματος σε bytes υπάρχει μόνο όταν έχει οριστεί σημαία μήκους.

ID σήραγγας:
Δείχνει το αναγνωριστικό για τη σύνδεση ελέγχου.

SessionID(ID κλήσης):
Δείχνει το αναγνωριστικό για μια σύνοδο μέσα σε ένα τούνελ.

Ns (προαιρετικό):
Αύξων αριθμός για το μήνυμα δεδομένων ή ελέγχου ξεκινώντας από το μηδέν και προσαύξηση κατά ένα (modulo 216) για κάθε μήνυμα που στέλνετε. Υπάρχει μόνον όταν οριστεί η σημαία ακολουθίας.

Nr (προαιρετικό):
Αύξων αριθμός για το μήνυμα που πρέπει να λάβει. Το Nr βασίζετε στο Ns του τελευταίου στην σειρά μήνυμα που έλαβε συν ένα (modulo 216). Στα μηνύματα δεδομένων το Nr επιφυλάσσεται και εάν υπάρχει (όπως υποδεικνύεται από το bitS) πρέπει να αγνοηθεί κατά την παραλαβή.

Offset Μέγεθος (προαιρετικό)
Καθορίζει που βρίσκονται τα δεδομένα ωφέλιμου φορτίου ύστερα από την επικεφαλίδα L2TP. Εάν το πεδίο offset είναι παρόν η κεφαλίδα L2TP τελειώνει μετά το τελευταίο byte του offsetpadding. Το πεδίο αυτό υπάρχει εάν κάποια μετατόπιση έχει οριστεί από την σημαία.

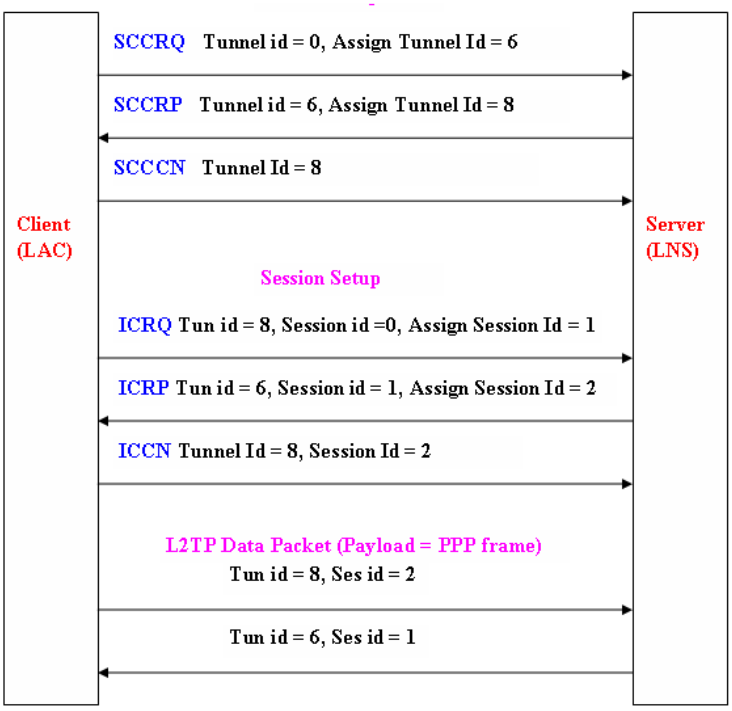
OffsetPad (προαιρετικό):
Μεταβλητό μήκος όπως ορίζεται από το μέγεθος του offset. Τα περιεχόμενα αυτού του πεδίου είναι απροσδιόριστα.

Ωφέλιμο φορτίο δεδομένων:
Μεταβλητό μήκος (μέγεθος ωφέλιμου φορτίου = μέγιστο μέγεθος του πακέτου UDP - μέγεθος L2TP επικεφαλίδας).

4.2 Ανταλλαγή πακέτων L2TP.

Κατά τη στιγμή της εγκατάστασης μιας σύνδεσης L2TP, ανταλλάσσονται πολλά πακέτα ελέγχου μεταξύ του διακομιστή και του πελάτη για τη δημιουργία της σήραγγας. Η μια πλευρά ζητά από την άλλη (peertopeer) να εκχωρήσει μια συγκεκριμένη σήραγγα και διάρκεια μέσω αυτών των πακέτων ελέγχου. Στη συνέχεια χρησιμοποιώντας αυτό το τούνελ και την ταυτότητα συνόδου τα πακέτα δεδομένων ανταλλάσσονται σε συμπιεσμένα πλαίσια PPP ως φορτίο.

Ο κατάλογος των μηνυμάτων L2TP ελέγχου που ανταλλάσσονται μεταξύ LAC και LNS για χειραψία πριν από την ίδρυση της σήραγγας στη εθελοντική σήραγγα (voluntarytunnel)Εικόνα 11.



Εικόνα 12: L2TP Control and Data Packets.

4.3 L2TP/IPsec.

Λόγω της έλλειψης της εμπιστευτικότητας που χαρακτηρίζουν το πρωτόκολλο L2TP, συχνά εφαρμόζετε μαζί με το πρωτόκολλο IPsec. Αυτό αναφέρεται ως L2TP/IPsec και τυποποιείται στο IETFRFC 3193. Η διαδικασία της δημιουργίας ενός L2TP/IPsecVPN έχει ως εξής:

- Διαπραγμάτευση IPsec συσχετισμού ασφαλείας (SA) γίνετε συνήθως μέσω του πρωτοκόλλου InternetKeyExchange (IKE). Αυτό πραγματοποιείται μέσω της θύρας UDP 500 και συνήθως χρησιμοποιείτε είτε ένας κοινός κωδικός (τα λεγόμενα «pre-shared κλειδιά») ή τα δημόσια κλειδιά ή και τα πιστοποιητικά X.509 και στα δύο άκρα.
- Ίδρυση επικοινωνίας και μεταφορά δεδομένων EncapsulatingSecurityPayload (ESP). Ο αριθμός πρωτοκόλλου IP για ESP είναι 50. Σε αυτό το σημείο, ένα ασφαλές κανάλι έχει δημιουργηθεί αλλά δεν γίνετε καμία μεταφορά δεδομένων στην σήραγγα.
- Δημιουργία μιας L2TP σήραγγας μεταξύ των άκρων του SA. Η πραγματική διαπραγμάτευση των παραμέτρων πραγματοποιείται μέσω ασφαλούς καναλιού της

S.A. στο πλαίσιο της κρυπτογράφησης του IPsec. Το L2TP χρησιμοποιεί τηθύρα UDP 1701.

Όταν ολοκληρωθεί η διαδικασία, τα πακέτα L2TP μεταξύ των δυο άκρων ενθυλακώνονται από το IPsec. Από την στιγμή που το ίδιο το πακέτο L2TP είναι τυλιγμένο και κρυμμένο μέσα στο πακέτο IPsec δεν υπάρχουν πληροφορίες σχετικά με την εσωτερική αρχιτεκτονική του ιδιωτικού δικτύου ούτε κάποια περεταίρω πληροφορία μπορεί να παρθεί από το κρυπτογραφημένο πακέτο. Επίσης δεν είναι απαραίτητο να ανοίξετε τη θύρα UDP 1701 για το firewall που υπάρχει μεταξύ των δυο τελικών άκρων, δεδομένου ότι τα πακέτα δεν θα αναδιπλωθούν και αποκρυπτογραφηθούν πρίν φτάσουν σε ένα από τα δυο άκρα(peers).

Ένα πιθανό σημείο σύγχυσης για το L2TP/IPsec είναι η χρήση των όρων σήραγγας και ασφαλές κανάλι. Ο όρος σήραγγα αναφέρεται σε ένα κανάλι το οποίο επιτρέπει ανέγγιχτα πακέτα μεταφερθούν από το ένα δίκτυο να σε ένα άλλο δίκτυο. Στην περίπτωση του L2TP/PPP γίνετε μεταφορά L2TP/PPP πακέτων πάνω σε δίκτυο IP. Ένα ασφαλές κανάλι αναφέρεται σε μια σύνδεση μέσα στον οποίο εξασφαλίζεται η εμπιστευτικότητα όλων των δεδομένων. Στο L2TP/IPsec πρώτα το IPsec παρέχει ένα ασφαλές κανάλι και τότε το L2TP παρέχει μια σήραγγα [19].

4.4 IPSec(InternetProtocolSecurity).

Όταν σχεδιάστηκε το IPv6 πριν από μερικά χρόνια, υπήρχαν ισχυρές πιέσεις να συμπεριληφθούν σε αυτό λειτουργίες ασφάλειας. Ο βασικός στόχος ήταν να εξασφαλιστεί ότι η επόμενη γενιά του IP θα είχε διαθέσιμους ισχυρούς κρυπτογραφικούς μηχανισμούς για τους χρήστες εκείνους που θα επιθυμούσαν να τους χρησιμοποιήσουν. Σύμφωνα με τους στόχους σχεδίασης οι μηχανισμοί αυτοί έπρεπε να είναι ανεξάρτητοι από αλγόριθμους έτσι ώστε να είναι δυνατή η αλλαγή των αλγόριθμων χωρίς να επηρεάζεται η υπόλοιπη υλοποίηση. Οι μηχανισμοί θα έπρεπε επίσης να είναι χρήσιμοι στην επιβολή μιας μεγάλης ποικιλίας πολιτικών ασφάλειας αλλά και ταυτόχρονα θα έπρεπε να σχεδιαστούν με τέτοιον τρόπο ώστε να αποφευχθούν δυσμενείς επιπτώσεις στους χρήστες του Internet που δεν χρησιμοποιούν καθόλου μηχανισμούς ασφάλειας για τη διακίνηση των δεδομένων τους.

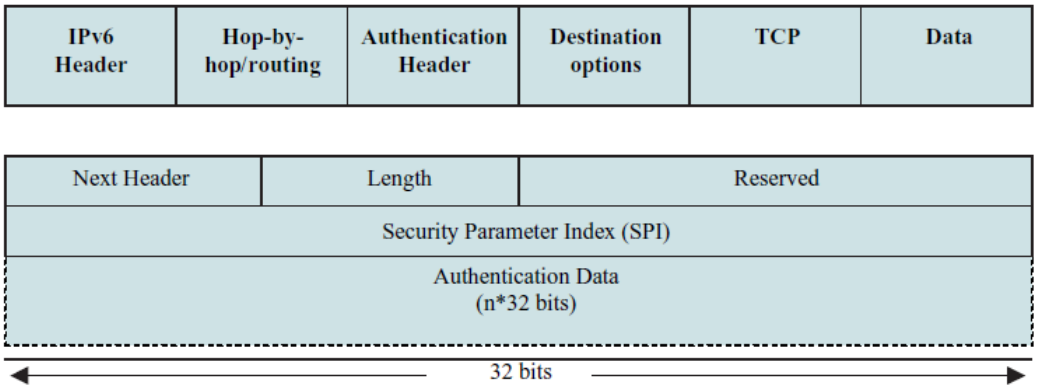
Το αποτέλεσμα της προσπάθειας αυτής ήταν η προδιαγραφή μιας ολοκληρωμένης αρχιτεκτονικής ασφάλειας για το IPv6 η οποία συνδυάζει μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης.

Στο τέλος του 1992, η InternetEngineeringTaskForce (IETF) συγκρότησε μια ομάδα εργασίας με στόχο την προτυποποίηση ενός πρωτοκόλλου ασφάλειας IP (IPSecurityProtocol –– IPSP) και ενός πρωτοκόλλου διαχείρισης κλειδιών Internet (InternetKeyManagementProtocol – IKMP). Σύντομα έγινε αντιληπτό ότι η ίδια αρχιτεκτονική που σχεδιαζόταν για το IPv6 μπορούσε να χρησιμοποιηθεί και για το IPv4. Η βασική διαφορά είναι ότι οι μηχανισμοί ασφάλειας που περιγράφονται στην αρχιτεκτονική πρέπει εκ των υστέρων να ενταχθούν στις υλοποιήσεις του IPv4, ενώ ενυπάρχουν στις υλοποιήσεις του IPv6 εξ αρχής. Τα IPSP και IKMP συνδέονται μόνο μέσω συνάψεων ασφάλειας (SecurityAssociations – SAs), στις οποίες γίνονται αναφορές από δείκτες παραμέτρων ασφάλειας (SecurityParameterIndices – SPIs). Βασικά το IKMP χρησιμοποιείται για να εγκατασταθούν SAs και να αρχικοποιηθούν SPIs, ενώ το IPSP χρησιμοποιεί αυτές τις SAs και τα SPIs για να κρυπτογραφήσει πακέτα IP.

4.6 Πρωτόκολλο AHP.

Το πρωτόκολλο αυτό χρησιμοποιείται όταν η ακεραιότητα και αυθεντικότητα του πακέτου IP ή του περιεχομένου του πρέπει να προστατευτούν αλλά όχι απαραίτητα η εμπιστευτικότητα του ίδιου του πακέτου. Για παράδειγμα, σε μια μεταφορά χρημάτων θέλουμε να είμαστε σίγουροι ότι το ποσό που μεταφέρεται δεν θα αλλοιωθεί, αλλά δεν έχει ιδιαίτερη σημασία αν κάποιος μάθει το ύψος του. Υπάρχουν βέβαια και περιπτώσεις όπου το ύψος του ποσού που μεταφέρεται αποτελεί σημαντικότατη πληροφορία για κάποιους τρίτους.

Το πρωτόκολλο AHP παρέχει μια επιπλέον επικεφαλίδα μεταξύ των επικεφαλίδων των επιπέδων IP και μεταφοράς η οποία περιέχει κάποια δεδομένα αυθεντικοποίησης τα οποία ο αποδέκτης επαληθεύει ώστε να διαπιστώσει αν ο αποστολέας ήταν πράγματι αυτός που ισχυρίζεται πως ήταν. Για το σκοπό αυτό χρησιμοποιείται μια μονόδρομη συνάρτηση σύνοψης (hashfunction) με κλειδί όπως η MD5 με κλειδί ή oSHA με κλειδί. Ο υπολογισμός και η επαλήθευση δεδομένων αυθεντικοποίησης με τον τρόπο αυτό γίνονται πολύ αποτελεσματικότερα απ' ότι αν κρυπτογραφούσαμε και αποκρυπτογραφούσαμε όλο το πακέτο. Στην Εικόνα 12 φαίνεται η δομή της επικεφαλίδας αυτής και η θέση της μέσα σε ένα πακέτο IPv6. Κάθε γραμμή της επικεφαλίδας αντιστοιχεί σε λέξη 32 bits.



Εικόνα 13: Δομή επικεφαλίδας.

Το πεδίο *Nextheader*(μήκους 8 bits) χρησιμοποιείται για την αναγνώριση του τύπου των δεδομένων που ακολουθούν την επικεφαλίδα αυθεντικοποίησης. Το πεδίο *Payloadlength*(μήκους 8 bits) καθορίζει το μήκος της επικεφαλίδας αυθεντικοποίησης σε λέξεις 32 bits, μειωμένο κατά 2. Το πεδίο *Reserved*(μήκους 16 bits) είναι δεσμευμένο για μελλοντική χρήση. Το πεδίο *Securityparameterindex*(SPI) (μήκους 32 bits) καθορίζει τη σύναψη ασφάλειας του πακέτου. Η τιμή 0 σημαίνει ότι δεν υπάρχει σύναψη ασφάλειας. Το πεδίο *Authenticationdata*περιέχει ένα μεταβλητό πλήθος λέξεων μήκους 32 bits που περιγράφουν τα δεδομένα αυθεντικοποίησης, π.χ. έναν κώδικα αυθεντικοποίησης μηνύματος ή μια ψηφιακή υπογραφή.

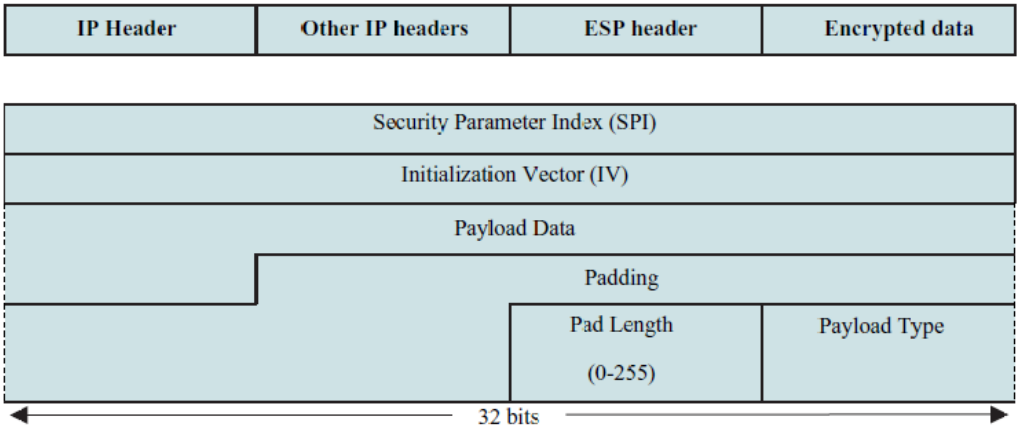
Για να αυθεντικοποιηθεί ένα πακέτο, ο αποστολέας πρέπει πρώτα να εντοπίσει μια σύναψη ασφάλειας, καθορίζοντας παραμέτρους όπως ο αλγόριθμος ελέγχου ακεραιότητας, το κρυπτογραφικό κλειδί και το μήκος των δεδομένων αυθεντικοποίησης. Κανονικά η ταυτότητα του χρήστη, η διεύθυνση προορισμού και ο δείκτης παραμέτρων ασφάλειας (SPI) καθορίζουν ποιά σύναψη ασφάλειας θα χρησιμοποιηθεί. Συνήθως, για αυθεντικοποίηση χρησιμοποιείται ένας αλγόριθμος κώδικα αυθεντικοποίησης μηνύματος. Οι προκαθορισμένες επιλογές που

πρέπει να υποστηρίζονται από όλες τις υλοποιήσεις IPsec είναι ο HMAC με τον MD5 και τον SHA–1. Ωστόσο, μπορούν να χρησιμοποιηθούν και άλλες συναρτήσεις ελέγχου ακεραιότητας. Ο υπολογισμός των δεδομένων αυθεντικοποίησης θεωρεί τα πεδία του πακέτου, όπως αυτά εμφανίζονται στην πλευρά του δέκτη. Μερικά πεδία θα αλλάξουν κατά τη μετάδοση, όπως το hoplimit στην επικεφαλίδα IP. Μερικά πεδία δεν είναι ακόμη γνωστά, όπως τα δεδομένα αυθεντικοποίησης στην επικεφαλίδα αυθεντικοποίησης. Τα πεδία αυτά γεμίζουν με μηδενικά κατά τον υπολογισμό του κώδικα αυθεντικοποίησης μηνύματος. Ο κώδικας αυτός εισάγεται στη συνέχεια στο κατάλληλο πεδίο δεδομένων της επικεφαλίδας αυθεντικοποίησης. Ο δέκτης του πακέτου αναφέρεται στο SPI και στη διεύθυνση προορισμού για να εντοπίσει τη σχετική σύναψη ασφάλειας και να επαληθεύσει τα δεδομένα αυθεντικοποίησης. Αν αποτύχει η αυθεντικοποίηση, η αποτυχία πρέπει να καταγραφεί και το πακέτο να απορριφθεί.

Σ' αυτόν τον αλγόριθμο, κάποια πεδία της επικεφαλίδας IP δεν καλύπτονται από το μηχανισμό προστασίας. Για περισσότερη προστασία, η λειτουργία σήραγγας προσθέτει μια εξωτερική IP επικεφαλίδα που περιέχει κάποια άλλη διεύθυνση IP, συνήθως τη διεύθυνση ενός ηλεκτρονικού αναχώματος (firewall). Η εσωτερική επικεφαλίδα IP περιέχει τις αρχικές διευθύνσεις προορισμού και προέλευσης και προστατεύεται πλήρως από την επικεφαλίδα αυθεντικοποίησης.

4.7 Πρωτόκολλο ESP.

Το πρωτόκολλο αυτό χρησιμοποιείται για να κρυπτογραφήσει και να ενσωματώσει είτε μόνο το περιεχόμενο επιπέδου μεταφοράς είτε ολόκληρο το πακέτο IP, ανάλογα με τον τρόπο χρήσης, όπως θα δούμε αμέσως μετά. Το υποσύστημα υλοποίησης IP πρέπει να περιέχει μια επικεφαλίδα IP και να κρυπτογραφεί τμήματα του πακέτου IP, αντίστοιχα. Η κρυπτογράφηση γίνεται στην πλευρά του αποστολέα και η αποκρυπτογράφηση στην πλευρά του δέκτη. Η ακριβής μορφή των δεδομένων περιεχομένου εξαρτάται από τον συγκεκριμένο αλγόριθμο κρυπτογράφησης και το συγκεκριμένο μετασχηματισμό που χρησιμοποιείται. Το ESP προστατεύει την εμπιστευτικότητα. Ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται, μπορεί επίσης να προστατεύει την ακεραιότητα και την αυθεντικότητα. Η επικεφαλίδα ESP συνήθως τοποθετείται μπροστά από τα κρυπτογραφημένα δεδομένα, όπως φαίνεται στην Εικόνα 13και περιέχει το SPI. Η δομή της έχει ως εξής: Το πεδίο *SecurityParameterIndex*(μήκους 32 bits) αναφέρεται στο δείκτη παραμέτρων ασφάλειας του δέκτη. Το πεδίο *InitializationVector*αποτελείται από μεταβλητό πλήθος λέξεων μήκους 32 bits, των οποίων το ακριβές πλήθος ορίζεται ως παράμετρος της σύναψης ασφάλειας. Το περιεχόμενο του πεδίου αυτού είναι κανονικά το αποτέλεσμα μιας γεννήτριας τυχαίων αριθμών. Το πεδίο *PayloadData*περιέχει τα κρυπτογραφημένα δεδομένα. Το πεδίο *Padding*(μεταβλητού μήκους) συνήθως γεμίζει με τυχαία bits. Το μήκος του πεδίου επιλέγεται έτσι ώστε το συνολικό μήκος των πεδίων PayloadData και Paddingmod 8 να ισούται με 6. Το πεδίο *PadLength*(μήκους 8 bits) καθορίζει το μήκος του πεδίου Padding. Το πεδίο *PayloadType*(μήκους 8 bits) περιέχει τον κωδικό του πρωτοκόλλου των δεδομένων του περιεχομένου. Πριν κρυπτογραφήσουμε ένα πακέτο, ο πομπός πάλι εντοπίζει μια σύναψη ασφάλειας για να καθορίσει ποιον αλγόριθμο κρυπτογράφησης και ποιο κλειδί θα χρησιμοποιήσει. Η σύναψη αυτή είναι διαφορετική από εκείνη που χρησιμοποιείται με το AHP.



Εικόνα 14: Επικεφαλίδα ESP.

Ο πομπός έχει στη συνέχεια δύο επιλογές τρόπου λειτουργίας του ESP:

- Σε λειτουργία μεταφοράς, ένα πλαίσιο από ανώτερο πρωτόκολλο, όπως, π.χ., από το TCP ή το UDP, ενσωματώνεται στο ESP. Η επικεφαλίδα IP δεν κρυπτογραφείται. Η λειτουργία αυτή παρέχει προστασία των πακέτων που μεταδίδονται μεταξύ δύο κόμβων απ' άκρη σε άκρη.
- Σε λειτουργία σήραγγας, ολόκληρο το IP πακέτο ενσωματώνεται στο ESP. Αυτό το ESP μεταδίδεται μέσα σε ένα άλλο πακέτο IP με μη κρυπτογραφημένες επικεφαλίδες. Επομένως, η λειτουργία αυτή μπορεί να ονομαστεί ≪IP μέσα στο IP≫. Η λειτουργία αυτή μπορεί να εφαρμοστεί μεταξύ ηλεκτρονικών αναχωμάτων για να δημιουργήσει ένα ιδεατό ιδιωτικό δίκτυο (VirtualPrivateNetwork – VPN).

Ο δέκτης του πακέτου εντοπίζει τη σχετική σύναψη ασφάλειας και αποκρυπτογραφεί το κρυπτογραφημένο περιεχόμενο. Αν η αποκρυπτογράφηση αποτύχει, το γεγονός καταγράφεται και το πακέτο απορρίπτεται. Μέχρι τώρα έχουμε ξεπεράσει τη συζήτηση των ζητημάτων των σχετικών με τη διαχείριση κλειδιών μέσα στο IPsec. Αυτό έγινε γιατί το IPsec προδιαγράφει υπηρεσίες αυθεντικοποίησης και κρυπτογράφησης ανεξάρτητα από τα πρωτόκολλα διαχείρισης κλειδιών, που διαμορφώνουν τις σχέσεις ασφάλειας, και τα κλειδιά των συνόδων. Έτσι, οι υπηρεσίες του IPsec δε συσχετίζονται με κάποιο συγκεκριμένο πρωτόκολλο διαχείρισης κλειδιών. Αν ένα τέτοιο πρωτόκολλο βρεθεί ελαττωματικό, μπορεί να αντικατασταθεί χωρίς περαιτέρω επιπτώσεις στην υλοποίηση του IPsec. Μπορούμε όμως τώρα να ολοκληρώσουμε τη συζήτησή μας, κάνοντας αναφορά στο IKMP [22, 23].

4.5 Επισκόπηση αρχιτεκτονικής.

Κάθε υποσύστημα υλοποίησης IPsec περιέχει υλοποιήσεις του IPSP και του IKMP, μια βάση δεδομένων πολιτικής ασφάλειας και μια βάση δεδομένων συνάψεων ασφάλειας. Το IPSP περιέχει τα πρωτόκολλα *AuthenticationHeaderProtocol*(AHP) και *EncapsulatingSecurityPayloadProtocol*(ESP) τα οποία είτε μεμονωμένα είτε σε συνεργασία παρέχουν τις αντίστοιχες υπηρεσίες στη σύναψη ασφάλειας. Αν απαιτείται προστασία και με το AHP και με το ESP, τα επικοινωνούντα υποσυστήματα υλοποίησης IPsec πρέπει να εγκαταστήσουν και να συντηρήσουν δύο συνάψεις ασφάλειας. Ομοίως, προκειμένου να επιτευχθεί αμφίδρομη επικοινωνία μεταξύ δύο κεντρικών συστημάτων το υποσύστημα υλοποίησης IPsec πρέπει να εγκαταστήσει και να συντηρήσει δύο συνάψεις ασφάλειας, μία για κάθε κατεύθυνση επικοινωνίας.

Τόσο το AHP όσο και το ESP υποστηρίζουν δύο τρόπους λειτουργίας, την λειτουργία σήραγγας (tunnelmode) και τη λειτουργία μεταφοράς (transportmode). Στη *λειτουργία μεταφοράς* προστατεύουν κυρίως πρωτόκολλα ανώτερων επιπέδων. Ο τρόπος αυτός είναι ο απλούστερος και ο πιο συνηθισμένος για χρήση μεταξύ τελικών συστημάτων. Στη *λειτουργία σήραγγας* προστατεύουν σειρές πακέτων IP χρησιμοποιώντας ενσωμάτωση IP. Η βάση δεδομένων πολιτικής ασφάλειας, την οποία εγκαθιστά και συντηρεί ένας χρήστης ή ένας διαχειριστής συστήματος μέσα στο υποσύστημα υλοποίησης IPsec περιέχει απαιτήσεις για το συγκεκριμένο επίπεδο προστασίας. Ο συγκεκριμένος τρόπος επεξεργασίας των πακέτων κάθε εφαρμογής επιλέγεται ταυτίζοντας πληροφορίες των επικεφαλίδων επιπέδου IP και επιπέδου μεταφοράς (διευθύνσεις IP πομπού και δέκτη, αριθμοί θυρών κτλ.) με εγγραφές της βάσης. Μια σύναψη ασφάλειας είτε αποδέχεται τις υπηρεσίες ασφάλειας IPsec κάθε πακέτου είτε το απορρίπτει είτε του επιτρέπει να παρακάμψει πλήρως τα πρωτόκολλα IPsec.

Κάθε σύναψη ασφάλειας αναγνωρίζεται μοναδικά από μια τριάδα αριθμών, που αποτελείται από ένα δείκτη παραμέτρων ασφάλειας, μια IP διεύθυνση προορισμού και ένα όνομα που καθορίζει το AHP ή το ESP ως πρωτόκολλο ασφάλειας. Η βάση δεδομένων σύναψης ασφάλειας περιέχει μια εγγραφή για κάθε σύναψη που ορίζει τις παραμέτρους ασφάλειάς της [20, 21].

4.8 Πρωτόκολλο IKMP.

Το IPSP υποθέτει ότι υπάρχουν συνάψεις ασφάλειας μεταξύ των οντοτήτων που επιθυμούν να χρησιμοποιήσουν το IPsec. Ο σκοπός του πρωτοκόλλου IKMP είναι να διαπραγματευτεί τις κρυπτογραφικές δυνατότητες και των δύο μερών, ώστε να συμφωνήσουν σε αλγόριθμους και παραμέτρους και να ανταλλάξουν κλειδιά. Με άλλα λόγια, το πρωτόκολλο εγκαθιστά και συντηρεί τις συνάψεις ασφάλειας που θα χρησιμοποιήσουν τα πρωτόκολλα AHP και ESP.

Η ιστορία του IKMP είναι μεγάλη. Η τρέχουσα έκδοση του πρωτοκόλλου συνδυάζει το πρωτόκολλο *InternetSecurityAssociationKeyManagementProtocol*(ISAKMP), που αναπτύχθηκε από την NSA, και το πρωτόκολλο καθορισμού κλειδιού *Oakley*, που αναπτύχθηκε από το Πανεπιστήμιο της Αριζόνα. Το ISAKMP χρησιμοποιείται για τη διαπραγμάτευση αμοιβαία υποστηριζόμενων αλγόριθμων και μαθηματικών δομών για την ανταλλαγή κλειδιών Diffie–Hellman και το επακόλουθο βήμα αυθεντικοποίησης.

Πρόσφατα, το ISAKMP/Oakley μετονομάστηκε σε *InternetKeyExchange*(IKE) και πιθανόν κάποτε θα αντικαταστήσει το IKMP. Η πρόταση ISAKMP/Oakley (και IKE) συνδυάζει ανταλλαγή κλειδιών Diffie–Hellman και επακόλουθη αυθεντικοποίηση των παραμέτρων Diffie–Hellman.

Η ανταλλαγή κλειδιών επέρχεται σε τρεις φάσεις. Στην πρώτη φάση, τα δύο μέρη ανταλλάσσουν cookiesώστε να προστατευτούν από επιθέσεις συμφόρησης πόρων (resource–cloggingattacks) μια ειδική μορφή επιθέσεων άρνησης παροχής υπηρεσίας (denial–of–serviceattacks), κατά την οποία ο επιτιθέμενος κατακλύζει το θύμα με υπολογισμούς μεγάλης πολυπλοκότητας, όπως, π.χ. η εκτέλεση πολλών ανταλλαγών κλειδιών Diffie–Hellman ταυτόχρονα. Στη δεύτερη φάση, εκτελούν μια ανταλλαγή κλειδιών Diffie–Hellman, ώστε αμοιβαία να υπολογίσουν το κλειδί μιας συνόδου. Το κλειδί αυτό μπορεί στη συνέχεια να χρησιμοποιηθεί μέσα στα πρωτόκολλα IPsec, έτσι ώστε να προστατευτούν οι μετέπειτα επικοινωνίες. Τα δύο μέρη, προκειμένου να αυθεντικοποιηθούν αμοιβαία και να προστατευτούν από επιθέσεις ενδιαμέσου (Man–in–the–middleattack), καταλήγουν με την ανταλλαγή ψηφιακών υπογραφών για αυθεντικοποίηση. Τόσο η μαθηματική δομή

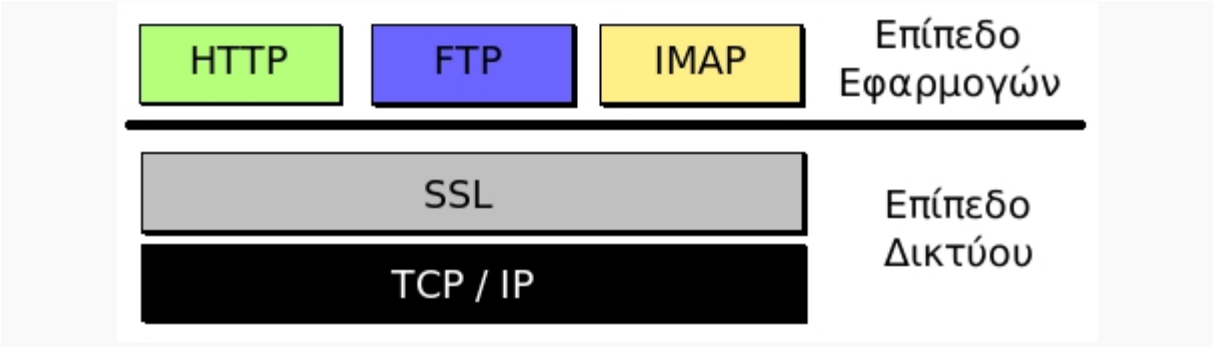
(πολλαπλασιαστική ομάδα σε πεπερασμένο πεδίο) στην οποία θα πραγματοποιηθεί η ανταλλαγή Diffie–Hellman όσο και η μέθοδος της επακόλουθης αυθεντικοποίησης είναι διαπραγματεύσιμες [24].

4.9 Πρωτόκολλο SSL.

Το πρωτόκολλο SSL (SecureSocketsLayer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (TransportLayerSecurity), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλαTCP/IP (TransferControlProtocol / InternetProtocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και toIMAP(email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.



Εικόνα 15:

Το SSLλειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.

Το SSLπροσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client,
- Πιστοποίηση του client από τον server,
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - DataEncryptionStandard, DSA - DigitalSignatureAlgorithm, KEA - KeyExchangeAlgorithm, MD5 - MessageDigest, RC2/RC4, RSA, SHA-1 - SecureHashAlgorithm, SKIPJACK, Triple-DES.

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχειωςεξής:

- Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
- Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
- Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
- Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
- Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
- Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
- Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

4.11 Intrusiondetectionsystem(IDS).

Ένα επιμέρους κομμάτι της ασφάλειας του cloudcomputing είναι η εγκατάσταση ενός συστήματος ανίχνευσης εισβολής γνωστά ως instrusiondetectionsystem (ids). Αποτελεί σύστημα παρακολούθησης και ανάλυσης των συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών. Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης. Οι λόγοι εγκατάστασης ενός συστήματος ανίχνευσης εισβολής ποικίλουν. Οι πιο σημαντικοί από αυτούς τους λόγους είναι η πρόληψη προβλημάτων, η ανίχνευση παραβιάσεων, η τεκμηρίωση υπαρκτών απειλών και ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας.

Ένα σύστημα ανίχνευσης εισβολών υπάρχει σε δυο κυρίως τύπους, το δικτυακό κομμάτι ανίχνευσης εισβολών networkbased (NIDS) και το κομμάτι υποδομής hostbased (hids).

4.11.1 Networkintrusiondetectionsystem (NIDS).

Ένα σύστημα (NIDS) μπορεί να τοποθετηθεί σε στρατηγικές θέσεις ή σημεία εντός του δικτύου για την παρακολούθηση της κυκλοφορίας προς και από όλες τις συσκευές του δικτύου, Εκτελεί μια ανάλυση για μια κυκλοφορία που διέρχεται σε ολόκληρο το υποδίκτυο, εργάζεται σε μια ετερόκλητη λειτουργία, και ταιριάζει με την κίνηση που έχει περάσει στα υποδίκτυα σε βιβλιοθήκη με γνωστές επιθέσεις. Μόλις προσδιοριστεί η επίθεση, ή μη φυσιολογική συμπεριφορά είναι αισθητή, η ειδοποίηση μπορεί να σταλεί στον διαχειριστή.Το NIDS θα πρέπει να εγκατασταθεί στο υποδίκτυο όπου βρίσκονται τα firewalls για να δείτε αν κάποιος προσπαθεί να σπάσει το τείχος προστασίας. Λειτουργώντας ιδανικά θα σαρώσει όλη την εισερχόμενη και εξερχόμενη κίνηση, ωστόσο κάτι τέτοιο θα μπορούσε να δημιουργήσει ένα εμπόδιο που θα μπορούσε να προκαλέσει μια συμφόρηση στη συνολική ταχύτητα του δικτύου.

4.11.2 HostIntrusionDetectionSystems (HIDS).

Τα host συστήματα ανίχνευσης εισβολής λειτουργούν σε κάθε συσκευή στο δίκτυο. Ένα HIDS παρακολουθεί τα εισερχόμενα και εξερχόμενα πακέτα με τη συσκευή και ειδοποιεί τον χρήστη ή διαχειριστή εάν μια ύποπτη δραστηριότητα ανιχνευτεί. Παίρνει ένα στιγμιότυπο από τα υπάρχοντα αρχεία του συστήματος και το ταιριάζει με ένα προηγούμενο στιγμιότυπο που έχει παρθεί. Εάν τα κρίσιμα αρχεία συστήματος έχουν τροποποιηθεί ή διαγραφεί, η ειδοποίηση αποστέλλεται στον διαχειριστή. Ένα παράδειγμα της χρήσης HIDS είναι να μπορεί να δει αν έχουν τροποποιηθεί οι ρυθμίσεις σε μηχανές, οι οποίες δεν αναμένεται να αλλάξουν τις ρυθμίσεις τους.

4.11.3 Σύγκριση IDS με firewalls.

Αν και τα δύο σχετίζονται με την ασφάλεια του δικτύου , ένα σύστημα ανίχνευσης εισβολής (IDS) διαφέρει από ένα τείχος προστασίας είναι ότι ένα τείχος προστασίας σταματά μια εισβολή από το να συμβεί εντελώς. ΤαFirewalls έχουν περιορισμένη την πρόσβαση μεταξύ των δικτύων για την πρόληψη της εισβολής και δεν σηματοδοτούν μια επίθεση από το εσωτερικό του δίκτυο. Ένα IDS αξιολογεί μια ύποπτη εισβολή αφού έχει πραγματοποιηθεί και ενεργοποιήσει τον συναγερμό. Ένα IDS παρακολουθεί επίσης, για επιθέσεις που προέρχονται από το εσωτερικό ενός συστήματος. Αυτό επιτυγχάνεται παραδοσιακά με την εξέταση των

επικοινωνιών δικτύου, τον εντοπισμό πρότυπων (συχνά γνωστό ως υπογραφές) των κοινών επιθέσεων σε συστήματα πληροφορικής και την άμεση ενημέρωση στον διαχειριστή. Με λίγα λόγια θα μπορούσαμε να αποκαλέσουμε ένα σύστημα ανίχνευσης εισβολών σαν μια άλλη μορφή ενός firewall επιπέδου εφαρμογής.

4.12 Συστήματα ανίχνευσης εισβολής (IDS).

Στην ορολογία υπολογιστών ένα Honeypot είναι μια παγίδα ανιχνεύει παρεμποδίζει κάθε απόπειρα σε μη εξουσιοδοτημένη χρήση των συστημάτων πληροφοριών. Σε γενικές γραμμές ένα honeypot αποτελείται από έναν υπολογιστή, τα δεδομένα, ή μια τοποθεσία που φαίνεται να είναι μέρος ενός δικτύου, η οποία φαίνεται να περιέχει πληροφορίες ή έναν πόρο αξίας στους επιτιθέμενους αλλά στην πραγματικότητα έχει απομονωθεί και να παρακολουθείται. Αυτό είναι παρόμοιο με της μυστικές υπηρεσίες που κάνει η αστυνομία για να δελεάσει μια εγκληματική ενέργεια [26, 27, 28, 29].

4.12.1 IntrusionPreventionSystem(IDPS).

Ένα intrusionPreventionsystem πολλές φόρες αποκαλείτε καιintrusiondetectionandpreventionsystems(IDPS) και θεωρείτε ένα είδος επέκτασης του intursiondetectionsystem (IDS)που μιλήσαμε παραπάνω γιατί και μετά δυο συστήματα υπάρχει η παρακολούθηση ενός δικτύου για μια κακόβουλη δραστηριότητα. Οι κύριες διαφορές τους είναι ότι ένα intrusionpreventionsystem σε αντίθεση με ένα intrusiondetectionsystem, τοποθετούνται σε σειρά και είναι σε θέση να αποτρέψουν ενεργά τις εισβολές που ανιχνεύονται και όχι απλά να ειδοποιήσουν τον διαχειριστή. Πιο συγκεκριμένα ένα IPS μπορεί να εκτελέσει ενέργειες όπως την σήμανση ενός συναγερμού, την απόρριψη κακόβουλων πακέτων και διακοπή της σύνδεσης του δικτύου με την επιτιθέμενη διεύθυνση IP. Ένα IPS μπορεί επίσης να διορθώσει λάθη του CyclicngRendundancyCheck (CRC) [30].

4.12.2 CyclicngRendundancyCheck(CRC).

Είναι ένας κώδικας ανίχνευσης σφαλμάτων που χρησιμοποιείτε συνήθως σε δίκτυα και συσκευές αποθήκευσης για τον εντοπισμό τυχαίων αλλαγών σε ανεπεξέργαστα δεδομένα. Τα κομμάτια δεδομένων που εισέρχονται στα συστήματα περνούν μια τιμή έλεγχου με βάσης το υπόλοιπο μιας πολυωνυμικής διαίρεσης του περιεχομένου τους. για την ανάκτηση επαναλαμβάνεται ο υπολογισμός και αν οι τιμές έλεγχου δεν ταιριάζουν τα δεδομένα έχουν επεξεργαστεί [31].

4.12.3 ChineseWall.

Η Virtualization τεχνολογία έχει υιοθετηθεί ευρέως στο «Υπολογιστικό Νέφος» για να ανταποκριθεί στις απαιτήσεις της on-demand επεκτασιμότητας του cloudcomputing. Αν και το virtualization βελτιώνεται, η χρήση των συσκευών hardware και η ευελιξία, φέρνει νέες προκλήσεις για την ασφάλεια. Οι χρήστες αντιμετωπίζουν ένα νέο είδος επιθέσεων που ονομάζεται inter-VM (VirtualMachine) attack, η οποία στοχεύει στα VMs που λειτουργούν στην ίδια φυσική μηχανή. Για την εξάλειψη των πιθανών VM επιθέσεων από τους ανταγωνιστές, προτείνεται ένας κεντρικός μηχανισμός ελέγχου με βάση την «Κινεζική πολιτική ασφαλείας Wall» να απαγορεύσει την ανάπτυξη και λειτουργία VMs των ανταγωνιστών στα ίδια μηχανήματα έτσι ώστε να επιτυγχάνεται φυσική απομόνωση.

Ιστορική εξέλιξη.

Η πολιτική του CW είναι αρχικά μια εμπορική πολιτική ασφάλειας, η οποία εκδόθηκε για να διαχωρίσει τους ανθρώπους με σύγκρουση συμφερόντων και να τους αποτρέψει από την

πρόσβαση και την ανταλλαγή πληροφοριών, ώστε ότι οι επενδυτικές αποφάσεις να μην επηρεαστούν.

Το 1989, οι Brewer και Nash πρότειναν μια μαθηματική θεωρία η οποία υλοποιεί την πολιτική CW και εισάγει τον τομέα της ασφάλειας του υπολογιστή. Αρχικά, ένα πρόσωπο (ένα θέμα), έχει την ελευθερία να έχει πρόσβαση στα δεδομένα (ένα αντικείμενο) και σε κάθε σύνολο δεδομένων. Από τη στιγμή που αποκτά πρόσβαση σε ένα σύνολο δεδομένων, ένα ChineseWall έχει δημιουργηθεί γι 'αυτόν έτσι ώστε να μην μπορούν να έχουν πρόσβαση άλλα σύνολα δεδομένων που βρίσκονται στην ίδια κατηγορία σύγκρουση συμφερόντων. Η πολιτική CW έχει επεκταθεί και εφαρμοστεί σε διάφορους τομείς.

Για την προστασία του hypervisor και των συστημάτων στα VMs, η απομόνωση των πόρων και η διαχείριση εκτελούνται σε αρχικό στάδιο. Κάθε VM ελέγχεται από τον hypervisor ώστε να έχει πρόσβαση στους δικούς του πόρους μόνο, όπως οι διευθύνσεις μνήμης και ο χώρος στο δίσκο. Και η χρήση της CPU είναι περιορισμένη από τα VMs για την πρόληψη, κάποιο από τα VMs να πάρει την άδεια του επιβλέποντα στη πλατφόρμα. Ωστόσο, τα τρωτά σημεία της virtualization πλατφόρμας εξακολουθούν να υπάρχουν ακόμα. Στο εικονικό περιβάλλον, επιβάλουμε την πολιτική CW για την εξάλειψη της ενδεχόμενης μεταξύ των VM επιθέσεων από τους ανταγωνιστές. Μόλις ένα VM φορτώνεται και εκτελείται σε ένα φυσικό μηχάνημα, τα υπόλοιπα VMs με σύγκρουση συμφερόντων δεν επιτρέπεται να εργάζονται στο ίδιο μηχάνημα. Με βάση την CW πολιτική, τα VMs με σύγκρουση συμφερόντων χωρίζονται για να λειτουργούν με διαφορετικές φυσικές μηχανές για να επιτευχθεί η φυσική απομόνωση [32, 33, 34, 35].

ChineseWall Κεντρικό Σύστημα Διαχείρισης (CWCMS).

Χτίζουμε το ChineseWall Κεντρικό Σύστημα Διαχείρισης (CWCMS) σε μια εσωτερική ενσωματωμένη πειραματική πλατφόρμα τύπου «Υπολογιστικού Νέφους». Το σύστημα CWCMS διαχειρίζεται αποτελεσματικά τα VMs και επιβάλει την ChineseWallπολιτική ασφάλειας στο cloud. Επιπλέον, το CWCMS χρησιμοποιεί τον αλγόριθμο χρωματισμού γραφήματος για να επιτευχθεί η καλύτερη αξιοποίηση των πόρων στο σύννεφο.

Η Virtualization τεχνολογία παίζει έναν πολύ σημαντικό ρόλο στην κατασκευή των νεφών. Το Virtualization επιτρέπει στους οργανισμούς να χρησιμοποιήσουν τις συσκευές υλικού πιο αποτελεσματικά και με μεγαλύτερη ευελιξία. Με το virtualization, το υλικό προσομοιώνεται και επιτρέπει πολλαπλές εικονικές μηχανές (VM) να τρέξουν ταυτόχρονα σε ένα μόνο υπολογιστή. Κάθε VM τρέχει το δικό του λειτουργικό σύστημα (OS) και εφαρμογές στο εικονικό υλικό, σαν να έχει πρόσβαση στους δικούς του πόρους σαν να τρέχει σε έναν ανεξάρτητο υπολογιστή. Μέσα από τον έλεγχο μιας εικονικής οθόνης της μηχανής (VMM), που ονομάζεται hypervisor, οι VMs μοιράζονται τους ίδιους πόρους του υλικού, αλλά δεν παρεμβάλλονται μεταξύ τους.

Παρόλο που το virtualization βελτιώνει την χρήση του υλικού, τις συσκευές και την ευελιξία, φέρνει νέες προκλήσεις ασφαλείας. Οι χρήστες αντιμετωπίζουν ένα νέο είδος επιθέσεων που ονομάζεται VM επίθεση, η οποία στοχεύει σε VMs που τρέχουν στο ίδιο φυσικό μηχάνημα. Σε ένα εικονικό περιβάλλον, ένα VM είναι πιθανό να δεχτεί επίθεση όχι μόνο από εξωτερικούς υπολογιστές, αλλά και από άλλα VMs που βρίσκονται στην ίδια φυσική μηχανή. Ένα VM μπορεί να επιτεθεί σε ένα άλλο VM άμεσα, ή να επιτεθεί στο hypervisor πρώτα και στη συνέχεια με τον έλεγχο του hypervisor να επιτεθούν σε άλλα VMs στο ίδιο μηχάνημα. Τα συστήματα ανταγωνιστές μπορούν να λειτουργούν με τα ίδια μηχανήματα, αν νοικιάσουν VMs από τον ίδιο

πωλητή σύννεφο. Οι επιτυχείς από-μέσα- VM επιθέσεις που ξεκίνησαν από τους ανταγωνιστές πρόκειται να είναι περισσότερο επιβλαβής από ό, τι ποτέ.

Για να εξαλείψουμε τις πιθανές από-μέσα-VM επιθέσεις από τους ανταγωνιστές, έχουμε προτείνει έναν κεντρικό μηχανισμό ελέγχου που βασίζεται στην ChineseWall πολιτική ασφάλειας για να απαγορεύσουν την ανάπτυξη και τη λειτουργία ανταγωνιστικών VMs στις ίδιες μηχανές. Λόγω της σύγκρουσης συμφερόντων ο κεντρικός έλεγχος αναπτύσσει έναν μηχανισμό ελέγχου VMs με συγκρουόμενα συμφέροντα για διαφορετικές φυσικές μηχανές ώστε η φυσική απομόνωση να μπορεί να επιτευχθεί. Η δουλειά αυτή ενισχύει την ασφάλεια του cloudcomputing για την προστασία των συστημάτων και των δεδομένων στο «Υπολογιστικό Νέφος».

Χτίζουμε το ChineseWall Σύστημα Κεντρικής Διαχείρισης (CWCMS) με τονπροτεινόμενο μηχανισμό με ένα εσωτερικό ενσωματωμένο σύννεφο που χρησιμοποιεί πυρήνα που βασίζεται σε μια VirtualMachine (KVM) ως λύση. Το CWCMS διαχειρίζεται και συντονίζει τα εργαλεία των VMs για πλατφόρμες virtualization, εξασφαλίζοντας ότι τα εργαλεία ακολουθούν τη CW πολιτική που καθορίζεται. Οι αναπτύξεις των VMs περιορίζονται από τη σύγκρουση συμφερόντων όταν η ChineseWall πολιτική ασφαλείας υιοθετείται. Εάν η σύγκρουση σχέσεων δεν έχουν ρυθμιστεί λογικά ή τα VMs δεν έχουν αναπτυχθεί με ένα καλά προγραμματισμένο τρόπο, τότε οι πωλητές της τεχνολογίας σύννεφο οφείλουν να διαθέσουν περισσότερες φυσικές μηχανές για την ανάπτυξη VM. Αντί την ανάπτυξη ενός VM σε μια διαθέσιμη φυσική μηχανή αυθαίρετα πρέπει πρώτα να διαπιστωθεί εάν μια σύγκρουση συμφερόντων βρίσκεται σε εξέλιξη, τότε το CWCMS χρησιμοποιεί τον αλγόριθμο χρωματισμού γραφήματος για να αναλύσει τη σύγκρουση συμφερόντων μεταξύ των σχέσεων. Σκοπός είναι να βρούμε μια καλή λύση για τη διανομή των VMs σε διαφορετικές φυσικές μηχανές. Κάνει τη διαχείριση της πολιτικής CW πολύ ευκολότερη και πιο αποτελεσματική.

Κεφάλαιο 5: Ασφάλεια του CloudComputing μέσα απόβιομετρικά χαρακτηρίστηκα

Όταν αναφερόμαστε στην ασφάλεια δεν μπορούμε να παραβλέψουμε την έννοια της μοναδικότητας. Όταν αναφέρουμε μοναδικότητα αυτό που έρχεται στο μυαλό στον καθένα είναι η μοναδικότητα που υπάρχει στο κάθε άνθρωπο.

Τα βιομετρικά χαρακτηρίστηκα είναι αυτά που χαρακτηρίζουν την μοναδικότητα του ατόμου. Βιομετρικά στην ουσία συνδέεται με την μέτρηση φυσιολογικών χαρακτηριστικών για την αναγνώριση του ατόμου.

Είναι χαρακτηριστικά του σώματος που ορίζουν μια φυσική ταυτότητα του ατόμου. Τα βιομετρικά χαρακτηριστικά είναι :

- Τα δαχτυλικά αποτυπώματα,
- Ίριδα του ματιού,
- Αμφιβληστροειδής,
- Γεωμετρία αυτιών,
- Γεωμετρία παλάμης,
- Γεωμετρία φλεβών,
- Χαρακτηρίστηκα προσώπου,
- Γεωμετρία υποστρωμάτωννυχιών,
- Οδοντοστοιχία,
- Στάσησώματος,
- Απορρόφησηφάσματος,
- Θερμόγραμμα προσώπου,
- Αναγνώριση φωνής,
- DNA,
- Οσμή.

Αυτά είναι κάποια από βιομετρικά χαρακτηριστικά που μπορούν να χρησιμοποιηθούν σε με μια ταυτοποίηση. Φυσικά κάποια μένουν απαράλλακτα στο χρόνο ενώ κάποια άλλα θα πρέπει να ενημερώνονται συνεχώς για την σωστή ταυτοποίηση. Για παράδειγμα με τα χρόνια η γεωμετρία των αυτιών αλλάζει, το ίδιο μπορούμε να ισχυριστούμε για την οδοντοστοιχία που μπορεί να αλλάξει με την πάροδο του χρόνου ή ακόμα και με τεχνητή αλλαγή που θα κάνουμε εμείς.

Στην συγκεκριμένη πτυχιακή θα αναφερθούμε κυρίως στην ταυτοποίηση μέσω των δαχτυλικών αποτυπωμάτων καθώς είναι ο πιο διαδεδομένος τρόπος αυθεντικοποίησης και ο πιο προσιτός στο να υλοποιηθεί στον εμπορικό τομέα. Επίσης, είναι από τα βιομετρικά χαρακτηρίστηκα που μένουν ανεξίτηλα στην πάροδο του χρόνου το οποίο είναι ένα μεγάλο πλεονέκτημα σε σύγκριση με τα άλλα.

Σε επίπεδο εφαρμογής για να παρέχεται η πρόσβαση σε έναν χρήστη πρέπει να περάσει από δυο στάδια, το στάδιο της ταυτοποίησης και της αυθεντικοποίησης.

Η ταυτοποίηση ενός λογικού υποκειμένου καλείτε η διαδικασία εκείνη , κατά την οποία το λογικό υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που απαιτούνται

προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλαση στους πόρους του.

Η αυθεντικοποίηση ενός λογικού υποκειμένου, καλείται να η διαδικασία εκείνη, κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελέγχει η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία ταυτοποίησης. Αν μπορούσαμε να κατηγοριοποιήσουμε τους τύπους ελέγχων αυθεντικοποίησης θα ήταν 4 τύποι.

Τύπος 1: κάτι που το λογικό υποκείμενο γνωρίζει (πχ ένα συνθηματικό –PIN)

Μειονεκτήματα :

Τα τεκμήρια αυθεντικοποίησης εύκολα μπορούν να αντιγράφουν , συνήθως είναι εύκολο να τα μαντέψει κανείς , χωρίς ιδιαίτερες τεχνικές γνώσεις , ενώ μπορούν να αποκαλυφθούν και με αυτοματοποιημένες μεθόδους .

Πλεονεκτήματα :

Είναι εύκολα ως προς την υλοποίηση και εφαρμογή , τροποποιούνται εύκολα. Δεν χάνονται ή κλέβονται , ενώ αν και είναι απλά στην χρήση τους , στην περίπτωση που είναι ένας μοναδικός συνδυασμός αριθμών και γραμμάτων , δεν αποκαλύπτονται εύκολα.

Τύπος 2: κάτι που το λογικό υποκείμενο κατέχει (πχ μαγνητική συσκευή αναγνώρισης, έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)

Μειονεκτήματα:

Το κόστος θα μπορούσαμε να πούμε είναι αρκετά υψηλό, ενώ δεν είναι αρκετά δύσκολο να χαθούν ή ακόμα και να κλαπούν .

Πλεονεκτήματα

Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα.

Τύπος 3: κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (συστήματα βιομετρικής τεχνολογίας πχ: εφαρμογές δαχτυλιών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού)

Μειονεκτήματα :

Υπάρχουν αρκετές δυσκολίες κατά την διαδικασία κατασκευής αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος και δυστυχώς δεν είναι αλάνθαστα.

Πλεονεκτήματα:

Παρέχουν μεγαλύτερη ασφάλεια από ένα συνθηματικό (τύπο 1) ή ακόμη και από μια μαγνητική συσκευή αναγνώρισης (τύπος 2)

Τύπος 4: κάτι που προσδιορίζει την τοποθεσίας που βρίσκεται το λογικό υποκείμενο (πχ διεύθυνση ip)

Μειονεκτήματα :

Δυσκολία στην εξακρίβωση στοιχείων στον χρήστη . Υπάρχει πρόβλημα όταν έχουμε dynamicip και πρόβλημα όταν υπάρχει μετακίνηση τοποθεσίας του χρήστη.

Πλεονεκτήματα:

Είναι ένας εύκολος και βοηθητικός και όχι κύριος τρόπος ταυτοποίησης όταν αναφερόμαστε σε staticip.

5.1 Χαρακτηριστικά δακτυλικών αποτυπωμάτων.

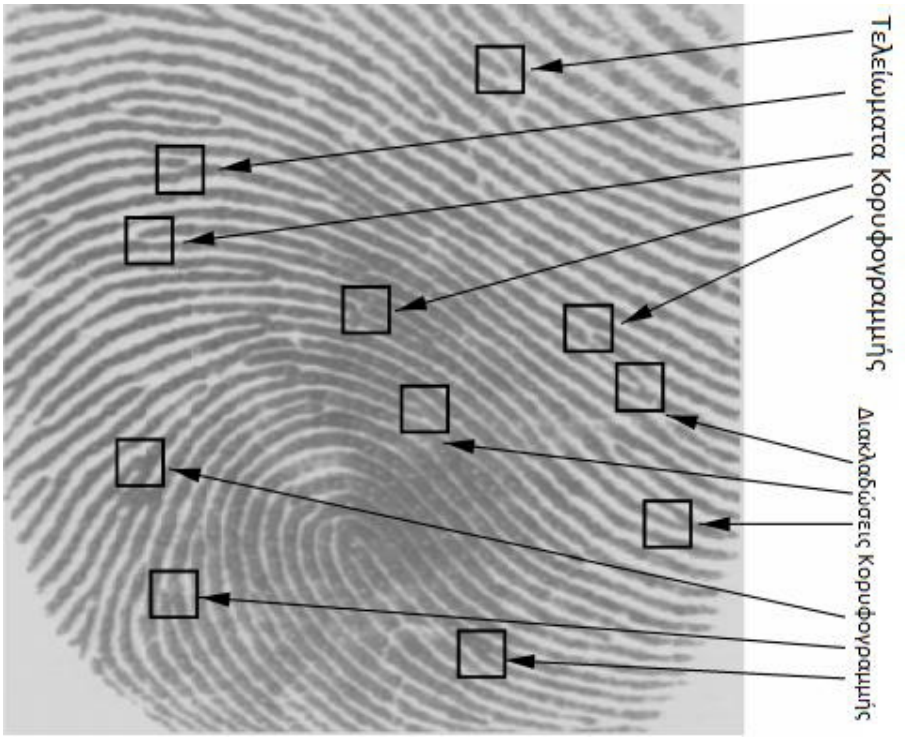
Εικόνα 16: Δακτυλικό Αποτύπωμα.

Σε ένα δακτυλικό αποτύπωμα μπορούν να εντοπιστούν έως και 150 διαφορετικά τοπικά χαρακτηριστικά (νησίδες, κοντές κορυφογραμμές, περιφράξεις και άλλα) τα οποία καλούνται μικρολεπτομέρειες. Αυτά τα τοπικά χαρακτηριστικά δεν είναι ομαλά κατανεμημένα πάνω στο δάκτυλο. Τα περισσότερα από αυτά εξαρτώνται από τις συνθήκες αποτύπωσης (μέθοδο επίπεδης ή ολισθαίνουσας αποτύπωσης, με χρήση μελάνης ή ηλεκτρονικού σαρωτή) και την ποιότητα του δακτυλικού αποτυπώματος. Τα δύο πιο προεξέχοντα χαρακτηριστικάείναι:

1. Τελείωμα-Κορυφογραμμής
2. Διακλαδώσεις-Κορυφογραμμών

Ως τελείωμα-κορυφογραμμής νοείται το σημείο όπου η κορυφογραμμή τερματίζει απότομα. Ως διακλάδωση-κορυφογραμμής νοείται το σημείο όπου μία κορυφογραμμή διχαλώνετε ή διαχωρίζεται σε δύο νέες κορυφογραμμές. Μια χαρακτηριστική εικόνα δακτυλικού

αποτυπώματος παρουσιάζεται στο Σχήμα 1.1 στην οποία περιλαμβάνονται 40-100 μικρολεπτομέρειες .



Εικόνα 17: Μορφολογία και τοπολογία δακτυλικού αποτυπώματος.

Η μορφολογία και η τοπολογία των κορυφογραμμών και των κοιλάδων πάνω στο δακτυλικό αποτύπωμα επιτρέπει την εφαρμογή κατάλληλων μαθηματικών μοντέλων και αλγορίθμων επεξεργασίας εικόνων προκειμένου να εξαχθούν κατάλληλες πληροφορίες που χαρακτηρίζουν κάθε δακτυλικό αποτύπωμα βάσει τις οποίες πραγματοποιείται τελικά η αναγνώριση και ταυτοποίηση των ατόμων.

5.2 Συστήματα ανάγνωσης δαχτυλικών αποτυπωμάτων.

Σε γενικές γραμμές, υπάρχουν οι παρακάτω τεχνικές ανίχνευσης δακτυλικών αποτυπωμάτων:

- ΟπτικήςΑνάκλασης (Optic reflection),
- ΟπτικήςΜετάδοσης (Optic Transmission),
- Οπτικού TFT,
- Ηλεκτρο-οπτικής ανάγνωσης,
- Χωρητικής ανίχνευσης (capacitance silicon),
- Χωρητικής TFT (capacitance tft),
- Πεδίου RF,
- Πίεσης TFT,
- Θερμική,
- Υπερήχων.

5.2.1 Αισθητήρας ΟπτικήςΑνάκλασης.

Πρόκειται για ένα από τους πλέον παλιούς τρόπους ανάγνωσης δακτυλικών αποτυπωμάτων. Η αρχή λειτουργίας του είναι εξαιρετικά απλή. Ο χρήστης πιέζει το δάχτυλο του στην επιφάνεια ενός πρίσματος που φωτίζεται από μια πηγή. Στο σημείο επαφής, το φως δεν ανακλάται αλλά απορροφάται. Από την άλλη πλευρά του πρίσματος, το φως που εξέρχεται (η εικόνα) μεταδίδεται μέσω ενός φακού σε ένα αισθητήρα CCD/CMOS και τα δεδομένα που προκύπτουν μεταφέρονται σε ένα κύκλωμα ψηφιοποίησης(framegrabber). Παραλλαγή της παραπάνω τεχνολογίας είναι ο αισθητήρας οπτικής ανίχνευσης με σάρωση: εδώ ο χρήστης θα πρέπει να κυλίσει το δάχτυλο του πάνω στην επιφάνεια του ανιχνευτή. Ο ανιχνευτής είναι μικρότερος σε μέγεθος. Η εταιρία Casio σε συνεργασία με την AlpsElectric δημιούργησαν το 2003 ένα ανιχνευτή όπου ο αισθητήρας βρίσκεται εσωτερικά σε ένα μικρό κύλινδρο ο οποίος περιστρέφεται καθώς ο χρήστης περνάει το δάχτυλο του.

5.2.2 Αισθητήρας Οπτικής Μετάδοσης.

Στο σύστημα αυτό, το δάχτυλο φωτίζεται άμεσα από μια φωτεινή πηγή (συνήθως φωτοεκπέμπουσα δίοδο, LED) τοποθετημένη από την αντίθετη πλευρά του δαχτυλικού αποτυπώματος. Το φως που εξέρχεται, διαβάζεται απευθείας από μια CMOScamera: Παραλλαγές της παραπάνω μεθόδου περιλαμβάνουν φωτισμό από τις άκρες του δακτύλου, όπως συμβαίνει στον αισθητήρα που ανέπτυξε η NEC. Το μέγεθος του CMOS είναι περίπου όσο το δάχτυλο και ο φωτισμός γίνεται από LED τοποθετημένα περιμετρικά:

5.2.3 Αισθητήρας Οπτικού TFT.

Πρόκειται για παραλλαγή της προηγούμενης μεθόδου, όπου αντί για κάμερα τύπου CMOS, χρησιμοποιείται μια μικρή TFT οθόνη στην οποία πιέζει ο χρήστης το δάχτυλο του. Το σύστημα αυτό τα καταφέρνει καλά ακόμα και με υγρά ή λερωμένα δάχτυλα ενώ δεν έχει πρόβλημα να λειτουργήσει σε πολύ σκοτεινό ή πολύ φωτεινό περιβάλλον.

5.2.4 Αισθητήρας Ηλεκτρο-οπτικής Ανάγνωσης.

Κάποια πολυμερή έχουν την ιδιότητα να εκπέμπουν φως όταν εκτίθενται σε υψηλές τάσεις. Στον αισθητήρα ηλεκτρο-οπτικής ανάγνωσης, το πολυμερές ακουμπάει σε μια κάμερα CMOS η οποία αναγκαστικά έχει το μέγεθος του δακτύλου. Ο χρήστης ακουμπάει στην πάνω πλευρά του πολυμερούς ουσιαστικά κλείνοντας με το δάχτυλο του το κύκλωμα στα σημεία που εφάπτονται οι παρυφές. Το πολυμερές εκπέμπει φως στα σημεία των παρυφών.

5.2.5 ΑισθητήρεςΧωρητικήςΑνίχνευσης: CapacitanceSilicon /CapacitanceTFT.

Ο πιο δημοφιλής τρόπος ανίχνευσης μετά την οπτική ανίχνευση, βασίζεται στη μέτρηση της χωρητικότητας (capacitance). Το δάκτυλο δρα σαν οπλισμός ενός πυκνωτή καθώς πιέζεται στην επιφάνεια του ανιχνευτή. Η χωρητικότητα μεταβάλλεται ανάλογα με το αν ακουμπάει παρυφή ή κοιλάδα. Η μέτρηση αυτή της μεταβλητής χωρητικότητας μας δίνει τελικά την εικόνα του αποτυπώματος. Καθώς οι χωρητικότητες είναι πολύ μικρές και απαιτείται μεγάλη ευαισθησία για να γίνει σωστή ανάγνωση της τιμής τους (με βάση το ηλεκτρικό πεδίο), το πάχος της επίστρωσης του αισθητήρα πρέπει να είναι πολύ μικρό (σε επίπεδο λίγων microns), καθώς η χωρητικότητα μειώνεται με το τετράγωνο της απόστασης μεταξύ των οπλισμών του πυκνωτή (Στη χωρητική ανίχνευση ο ένας οπλισμός είναι το δάχτυλο και το άλλο ο αισθητήρας, έτσι είναι σημαντικό το ενδιάμεσο τους κενό να είναι όσο το δυνατό μικρότερο). Ένα άλλο μειονέκτημα της χωρητικής ανίχνευσης είναι η σχετικά εύκολα παρεμβολή της από ηλεκτρικά πεδία που μπορεί να παράγονται από άλλες συσκευές. Τυχόν ηλεκτροστατική εκφόρτιση από το δέρμα του χρήστη μπορεί επίσης να καταστρέψει αισθητήρες αυτού του τύπου.

CapacitanceSilicon.

Σε αυτή τη μέθοδο χωρητικής ανίχνευσης ο αισθητήρας αποτελείται από ένα CMOS κύκλωμα, το οποίο είναι παραλλαγή του οπτικού αισθητήρα (CMOS) που χρησιμοποιείται στην οπτική ανίχνευση. Στη συγκεκριμένη περίπτωση ωστόσο δεν χρησιμοποιούνται οι οπτικές του ιδιότητες αλλά η δυνατότητα του να μετράει το ηλεκτρικό πεδίο που σχηματίζεται από το φαινόμενο χωρητικότητας στο οποίο αναφερθήκαμε παραπάνω. Η μέθοδος αυτή είναι ιδιαίτερα δημοφιλής καθώς οι αισθητήρες είναι μικροί σε μέγεθος, έχουν χαμηλό κόστος και κατανάλωση και μπορούν εύκολα να ενσωματωθούν σε χαμηλού κόστους καταναλωτικές συσκευές.

ActiveCapacitanceSilicon.

Πρόκειται για μια παραλλαγή της προηγούμενης μεθόδου (που μπορεί να περιγραφεί και σαν passivecapacitancesilicon) στην οποία πριν τη μέτρηση της χωρητικότητας, διοχετεύεται ηλεκτρικό ρεύμα στη διεπαφή δακτύλου – αισθητήρα. Υπάρχει με αυτό τον τρόπο ένας κύκλος φόρτισης (κατά τον οποίο το φορτίο αποθηκεύεται στην χωρητικότητα δακτύλου – αισθητήρα) και ένας κύκλος εκφόρτισης κατά τον οποίο γίνεται και η μέτρηση. Η χωρητικότητα υπολογίζεται συγκρίνοντας τη λαμβανόμενη τάση με μια τάση αναφοράς. Σε σχέση με την προηγούμενη παθητική ανίχνευση χωρητικότητας, η μέθοδος αυτή έχει το πλεονέκτημα ότι δεν επηρεάζεται ιδιαίτερα από λερωμένα ή υγρά δάχτυλα καθώς το ρεύμα διέρχεται μέσα από το δέρμα και η μέτρηση στην πραγματικότητα γίνεται κάτω από την επιφάνεια της επιδερμίδας (όπως και στον αισθητήρα υπερήχων που θα δούμε παρακάτω).

CapacitanceTFT.

Σε αντιστοιχία με την οπτική TFT μέθοδο, υπάρχει η αντίστοιχη χωρητική που αντικαθιστά τον αισθητήρα CMOS της προηγούμενης κατηγορίας με ένα αισθητήρα TFT, παραλλαγή της τεχνολογίας που συναντάμε στις αντίστοιχες οθόνες.

5.2.6 Αισθητήρας Πεδίου RF.

Αυτό το είδος ανίχνευσης πολλές φορές συγχέεται με την χωρητική ανίχνευση. Ο αισθητήρας παρέχει ένα ραδιοφωνικό σήμα (RF) χαμηλής συχνότητας το οποίο εισέρχεται. Αισθητήρας CapacitanceSilicon στο δάχτυλο του χρήστη. Το σήμα που επιστρέφει από το δάχτυλο μετριέται από τον αισθητήρα ο οποίος έχει και το ρόλο της κεραίας. Η ισχύς του σήματος που επιστρέφει εξαρτάται σε κάθε σημείο από τη χωρητικότητα/αντίσταση της επαφής του δακτύλου με τον αισθητήρα: είναι ισχυρότερο στις παρυφές και ασθενέστερο στις κοιλάδες.

5.2.7 Αισθητήρες Πίεσης – Πίεσης TFT.

Η ιδέα της ανίχνευσης ενός δακτυλικού αποτυπώματος με βάση την πίεση είναι μια από τις πλέον παλιές – καθώς σε αυτή βασίζεται και η αρχική καταγραφή με χαρτί και μελάνι. Η καταγραφή ηλεκτρικού σήματος που μεταβάλλεται ανάλογα με την πίεση βασίζεται στο πιεζοηλεκτρικό φαινόμενο το οποίο είναι γνωστό εδώ και πολλά χρόνια. Οι πιεζοηλεκτρικοί αισθητήρες ωστόσο παρουσιάζουν χαμηλή ευαισθησία και η ανάγκη ύπαρξης ενός προστατευτικού στρώματος πάνω στον αισθητήρα αλλοιώνει ακόμα περισσότερο την εικόνα (οι γραμμές εξομαλύνονται και θολώνουν). Κάποια από τα προβλήματα αυτά αντιμετωπίζονται ωστόσο με σχετική επιτυχία σε σύγχρονες υλοποιήσεις. Για τον αισθητήρα μπορεί να χρησιμοποιηθεί κύκλωμα CMOS ή TFT όπως έχουμε συναντήσει και στις προηγούμενες μεθόδους.

5.2.8 Θερμικοί Αισθητήρες.

Η τεχνική βασίζεται στην ύπαρξη πυρο-ηλεκτρικού υλικού που μετατρέπει τη διαφορά θερμοκρασίας μεταξύ δύο υλικών σε ηλεκτρικό σήμα. Ο αισθητήρας αυτού του τύπου δεν μετράει τη διαφορά θερμοκρασίας μεταξύ παρυφής και κοιλάδας στο αποτύπωμα (η διαφορά αυτή είναι μηδαμινή) αλλά τη διαφορά θερμοκρασίας μεταξύ δακτύλου και αισθητήρα. Για την ακρίβεια, μετριέται η θερμοκρασία των παρυφών καθώς μόνο αυτές έρχονται στην πραγματικότητα σε επαφή με τον αισθητήρα. Ένα πρόβλημα της συγκεκριμένης μεθόδου είναι ότι το σήμα εξαφανίζεται πολύ γρήγορα: αρχικά η διαφορά θερμοκρασίας δακτύλου – αισθητήρα είναι μεγάλη, αλλά καθώς το δάχτυλο παραμένει πάνω στον αισθητήρα, έρχονται και τα δύο στην ίδια θερμοκρασία πολύ γρήγορα (σε αυτό συμβάλει φυσικά και το μικρό μέγεθος του αισθητήρα). Καθώς το ηλεκτρικό σήμα παράγεται μόνο όσο υπάρχει διαφορά θερμοκρασίας, εξαφανίζεται μόλις επέλθει θερμική ισορροπία (τυπικά σε περίπου 1/10 του δευτερολέπτου).

5.2.8 Αισθητήρας Υπερήχων.

Η ανίχνευση δακτυλικών αποτυπωμάτων με χρήση υπερήχων προσφέρει κάποια πλεονεκτήματα, ωστόσο δεν είναι διαδεδομένη: Οι αισθητήρες είναι μεγάλοι, δύσχρηστοι και περιέχουν αρκετά μηχανικά μέρη. Το μέγεθος και το κόστος τους, κάνουν αδύνατη τη χρήση τους σε φορητές συσκευές και χαμηλού κόστους υπολογιστές. Το βασικό τους πλεονέκτημα είναι η δυνατότητα τους να διαβάζουν το δακτυλικό αποτύπωμα από το δέρμα που βρίσκεται κάτω από την επιδερμίδα. Έτσι δεν επηρεάζονται από νερό, σκόνη, βρωμιά και παρέχουν αρκετά πιο αξιόπιστη μέτρηση σε σχέση με άλλες μεθόδους. Πρόσφατα, η εταιρία UltraScan (www.ultra-scan.com) παρουσίασε ένα αισθητήρα υπερήχων σε μορφή chip ο οποίος υπόσχεται όλα τα πλεονεκτήματα των υπερήχων σε μικρότερο μέγεθος και ευκολότερη εφαρμογή.[38][39]

5.3 Αλγόριθμος αναγνώρισης δακτυλικών αποτυπωμάτων.

Παρακάτω δίνονται περισσότερες λεπτομέρειες για τον αλγόριθμο αναγνώρισης δακτυλικών αποτυπωμάτων. Ο εν λόγω αλγόριθμος αποτελείται από τέσσερα βήματα.

1. Ανίχνευση του πυρήνα.

2. Ευθυγράμμιση περιστροφής και μετατόπισης.

3. Κοινή περιοχή εξαγωγής.

4. Ταίριασμα των δακτυλικών αποτυπωμάτων.

5.3.1 Ανίχνευση πυρήνα.

Αυτό το βήμα εντοπίζει τον πυρήνα του καταχωρημένου δακτυλικού αποτυπώματος f(n1,n2) και της εισερχόμενης εικόνας g(n1,n2) ώστε να ευθυγραμμιστεί η μετατόπιση ανάμεσα στις δύο εικόνες. Ο πυρήνας ορίζεται ως ένα και μοναδικό σημείο σε μια εικόνα αναπαράστασης του δακτυλικού αποτυπώματος που παρουσιάζει την μέγιστη καμπυλότητα των κορυφογραμμών.

5.3.2Ευθυγράμμιση περιστροφής και μετατόπισης.

Πρέπει να εξομαλυνθεί η μετατόπιση και η περιστροφή ανάμεσα στο καταχωρημένο δακτυλικό αποτύπωμα f(n1,n2) και στο εισερχόμενο g(n1,n2) ώστε να εκτελεστεί υψηλής ακρίβειας ταίριασμα. Στην περίπτωση που και τα δύο αποτυπώματα έχουν τον δικό τους πυρήνα, τότε

γίνετε ευθυγράμμιση ανάμεσα στις δύο εικόνες με βάση των πυρήνα τους. Μετά ακολουθεί η εξομάλυνση της περιστροφής με βάση τα ακόλουθα:

Πρώτα, δημιουργείτε ένα ζευγάρι από τις περιστρεμμένες εικόνες fθ(n1,n2) των καταχωρημένων αποτυπωμάτων f(n1,n2) στο εύρος της γωνίας $-40° \leq \theta \leq 40°$ με διάστημα γωνίας 1°. Η γωνία περιστροφής θ της εισερχόμενης εικόνας σε σύγκριση με την ελεγχόμενη εικόνα μπορεί να προσδιοριστεί με βάση την αξιολόγηση της ομοιότητας ανάμεσα στο περιστρεφόμενο αντίγραφο της καταχωρημένης εικόνας fθ(n1,n2) $(-40° \leq \theta \leq 40°)$ και της εισερχόμενης εικόνας g(n1,n2) χρησιμοποιώντας της λειτουργία BLPOC. Όταν είτε η f(n1,n2) είτε η g(n1,n2) δεν έχει τον δικό της πυρήνα, πρέπει να εξομαλυνθεί πρώτα η περιστροφή με την διαδικασία που περιγράψαμε πριν από λίγο.

Μετά, ευθυγραμμίζεται το εκτόπισμα μεταξύ της περιστρεμμένης-κανονικοποιημένης εικόνας fθ(n1,n2) και της εισερχόμενης εικόνας g(n1,n2).

Τέλος, έχουμε τις κανονικοποιημένες εκδόσεις της καταχωρημένης εικόνας και της εικόνας εισόδου οι οποίες συμβολίζονται από τα f'(n1,n2) και g'(n1,n2).

5.3.3 Κοινή περιοχή εξαγωγής.

Επόμενο βήμα είναι η εξαγωγή της επικαλυπτόμενης περιοχής των δύο εικόνων f'(n1,n2) και g'(n1,n2). Αυτή η διαδικασία βελτιώνει την ακρίβεια του ταιριάσματος των δακτυλικών αποτυπωμάτων, δεδομένου ότι οι μη επικαλυπτόμενες περιοχές των δύο εικόνων μπορούν να καθιστούν ασυσχέτιστες συνιστώσες της λειτουργίας BLPOC. Προκειμένου να εντοπιστούν οι πραγματικές περιοχές της καταχωρημένης εικόνας f'(n1,n2) και της εικόνας εισόδου g'(n1,n2), εξετάζονται οι άξονες προβολής n1 και n2 των τιμών των πίξελ. Μόνο οι κοινές επηρεασμένες περιοχές της εικόνας, f''(n1, n2) και g''(n1, n2), με το ίδιο μέγεθος εξάγονται για το επόμενο βήμα του ταιριάσματος.

5.3.4 Ταίριασμα των δακτυλικών αποτυπωμάτων.

Υπολογίζεται η λειτουργία BLPOC$n_{f''}^{K1} n_{g''}^{K2}(n1, n2)$ ανάμεσα στις δύο εικόνες που έχουν εξαχθεί f''(n1, n2) και g''(n1, n2) και δημιουργείτε το αντίστοιχο αποτέλεσμα. Η λειτουργία BLPOC μπορεί να δώσει πολλαπλές κορυφές συσχέτισης ως επακόλουθο των ελαστικών παραμορφώσεων των δακτυλικών αποτυπωμάτων.

5.4 Μειονεκτήματα των δακτυλικών αποτυπωμάτων.

Στον τομέα της ασφάλειας στο ιντερνέτ χρησιμοποιούμε πάντα έναν τρόπο ταυτοποίησης ώστε να έχουμε πρόσβαση στο αντικείμενο που θέλουμε να κάνουμε είσοδο. Ο πιο διαδεδομένος τρόπος είναι ένας κωδικός πρόσβασης.

Οι κωδικοί πρόσβασης δεν είναι ασφαλείς. Κανείς δεν φτιάχνει καλούς κωδικούς πρόσβασης και όταν τους φτιάχνουν τους ξαναχρησιμοποιούν σε διαφορετικές ιστοσελίδες και servers. Ακόμα και εάν χρησιμοποιήσετε ένα αξιόπιστο passwordmanager μπορούν εύκολα το «σπάσουν» και να αποκτήσουν πρόσβαση σε όλους τους κωδικούς πρόσβασής σας. Αλλά ξέρετε τι είναι χειρότερο από έναν κωδικό πρόσβασης; Ένα δακτυλικό αποτύπωμα. Τα δακτυλικά αποτυπώματα έχουν αρκετά προβλήματα και δεν πρέπει να χρησιμοποιηθούν αντί κάποιου κωδικού πρόσβασης.

Οι κωδικοί πρόσβασης υποτίθεται ότι είναι μυστικοί, όπως π.χ. το όνομα του κατοικίδιου της παιδικής σας ηλικίας. Αντίθετα τα δακτυλικά αποτυπώματα τα έχει κάποιος μαζί του όπου και να πάει. Επίσης οι κωδικοί πρόσβασης μπορούν να αλλαχτούν σε περίπτωση που κάποιος κωδικός αποκαλυφθεί ενώ στο δαχτυλικό αποτύπωμα δεν γίνετε αυτό. Τέλος και σημαντικότερο πρέπει ο κωδικός πρόσβασής να είναι hashable, δηλαδή κωδικοποιήσιμος για να είναι ασφαλής και ο χρήστης και η βάση δεδομένων στο οποίο αποθηκεύεται από την κλοπή.

5.4.1 Τα δακτυλικά αποτυπώματα δεν είναι μυστικά.

Το πρώτο και ίσως πιο προφανές πρόβλημα με τη χρήση δακτυλικών αποτυπωμάτων αντί ενός μυστικού κωδικού πρόσβασης είναι ότι τα δακτυλικά αποτυπώματα δεν είναι μυστικά καθόλου. Σκεφτείτε ότι οποιοσδήποτε έχει στην κατοχή του κάτι που έχετε ακουμπήσει έχει απευθείας και τα δακτυλικά σας αποτυπώματα. Σκεφτείτε λοιπόν από πόσα διαφορετικά αντικείμενα που χρησιμοποιούμε στην καθημερινότητα μας μπορεί κάποιος να βρει και να ανακτήσει τα δακτυλικά μας αποτυπώματα.

Ένας χάκερ ονόματι Ιαν Krissler , όταν είχε κυκλοφορήσει το touchID στο iPhone 5's. αγόρασε μια συσκευή αμέσως και μέσα σε δύο ημέρες κατάφερε να παραβιάσει το σύστημα touchID με ένα ψεύτικο αποτύπωμα. Επίσης ο ίδιος άνθρωπος κατάφερε να δημιουργήσει ένα ψεύτικο αποτύπωμα από μια υψηλής ευκρίνειας φωτογραφία. Ήταν το αποτύπωμα την υπουργού άμυνας της Γερμανίας UrsulavonderLeyen και κατάφερε να το δημιουργήσει από μια φωτογραφία του χεριού της σε μια συνέντευξη τύπου.

5.4.2 Το δακτυλικά αποτυπώματα δεν μπορούν να αλλαχτούν.

Ένας κωδικός πρόσβασης εάν διαρρεύσει δίνετε η επιλογή στον χρήστη να τον αλλάξει ενώ το δακτυλικό αποτύπωμα δεν μπορεί να αλλαχτεί. Τρανό παράδειγμα μια κυβερνητική υπηρεσία της Αμερικής που ως σύστημα εισόδου στις εγκαταστάσεις της είχε ένα κωδικό πρόσβασης και μια κάρτα στην οποία είχαν αποθήκευση ψηφιακά το δακτυλικό αποτύπωμα. Κάποια στιγμή λοιπόν παραβιάστηκαν τα συστήματα ασφάλειας που είχαν από κάποιους τρίτους και κλαπήκαν 5,6 εκατομμύρια δακτυλικά αποτυπώματα σε ψηφιακή μορφή. Για να ξανακάνουν το σύστημα τους ασφαλή έπρεπε να βρουν έναν τρίτο τρόπο αυθεντικοποιησης και άπλα άλλαξαν τους κωδικούς. Το σύστημα με τα δακτυλικά αποτυπώματα δεν μπορούσαν να το ξαναχρησιμοποιήσουν διότι δεν μπορούν να αλλαχτούν και είναι μοναδικά.

5.4.3 Τα δακτυλικά αποτυπώματα έχουν πρόβλημα με τις κρυπτογραφικές συναρτήσεις hash.

Όταν πάει κάποιος χρηστής να συνδεθεί στο cloud, σε μια ιστοσελίδα η μια υπηρεσία και καταχωρεί τον κωδικό του, στην βάση δεδομένων δεν στέλνετε ο κωδικός του χρηστή για επιβεβαίωση αλλά μια στοιχειοσειρά που δημιουργήθηκε περνώντας τον κωδικό του χρηστή από μια κρυπτογραφική συνάρτηση hash(π.χ MD5, SH1, SH2).

Στην βάση δεδομένων δεν είναι αποθηκευμένοι οι κωδικοί αυτούσιοι αλλά οι στοιχειοσειρες των κωδικών πρόσβασης όλων το χρηστών. Για κάθε κωδικό πρόσβασης με την βοήθεια μιας συγκεκριμένης συνάρτηση hash δημιουργείτε μια συγκεκριμένη στοιχειοσειρά η οποία συγκρίνεται με την στοιχειοσειρά που είναι αποθηκευμένη στην βάση δεδομένων του cloud από την εγγραφή του χρηστή και ανάλογα αποκτάει ο χρηστής πρόσβαση. Στα δακτυλικά αποτυπώματα δεν γίνετε να παραχθεί η ίδια στοιχειοσειρα πάντα. Ο χρήστης μπορεί να πιέσει περισσότερο τον αισθητήρα η μπορεί να μετατοπίσει το δάκτυλο του όταν ακουμπήσει τον

αισθητήρα, ακόμα και να έχει κοπεί. Κάθε μικροαλλαγή θα επιφέρει διαφορετική στοιχειοσειρα.

Γι'αυτό τον λόγο οι εταιρίες που έχουν δημιουργήσει αισθητήρες και λογισμικό για δακτυλικά αποτυπώματα χρησιμοποιούν την τεχνική <<κατά προσέγγιση>>. Όποτε αν η στοιχειοσειρά που δημιουργηθεί από τον αισθητήρα του δακτυλικού αποτυπώματος είναι περίπου ίδιος την στοιχειοσειρά που είναι αποθηκευμένος στην βάση δεδομένων τότε επιβεβαιώνετε ο χρήστης και του δίνετε πρόσβαση στο cloud. Εν κατακλείδι η <<κατά προσέγγιση τεχνική>> δημιουργεί πολλά κενά στην ασφάλεια ενός συστήματος. Πλέον δεν χρειάζεται καν το αποτύπωμα ενός χρήστη, μπορεί και να εισέρθει κάποιος στο σύστημα εάν δημιουργήσει ένα αποτύπωμα που θα είναι παρόμοιο με του χρήστη.[40]

5.5 Συμπέρασμα.

Το συμπέρασμα είναι ότι οι βιομετρικοί αισθητήρες για δακτυλικά αποτυπώματα δεν είναι τόσο ασφαλείς όσο πιστεύαμε. Δεν θεωρούνται πιο ασφαλή από έναν μυστικό κωδικό πρόσβασης. Ο συνδυασμός τους μπορεί να είναι ποιο ασφαλές αλλά όχι τόσο πρακτικός όπως προανέφερα.

Κεφάλαιο 6: QRcode

Τα QRCodes είναι σύγχρονοι γραμμωτοί κώδικες δύο διαστάσεων (2D) ταχείας αποκωδικοποίησης (γνωστοί και ωςmatrixcode) και αποτελούν μια σύγχρονη μετεξέλιξη των γνωστών σε όλους μας γραμμωτών κωδικών barcodes μιας διάστασης. Τα μονοδιάστατα barcodes είχαν δημιουργηθεί από την ανάγκη αποθήκευσης κάποιων πληροφοριών σχετικές με το προϊόν, την προέλευση και την συσκευασία του, και η σάρωση γίνεται μηχανικά με μια στενή δέσμη φωτός από τα barcodereaders. Η εταιρεία Denso-Wave, θυγατρική της Toyota, δημιούργησε έναν νέο γραμμωτό κώδικα και πρότυπο ISO, ο οποίος πλέον είναι δισδιάστατος, για να έχει την δυνατότητα αποθήκευσης περισσοτέρων δεδομένων.

Αυτό το νέο είδος barcode ονομάστηκε QRCode και προέρχεται από τα αρχικά των αγγλικών λέξεων "QuickResponse" που σημαίνουν Γρήγορη Ανταπόκριση, διότι οι γιαπωνέζοι δημιουργοί του είχαν σαν σκοπό την ταχύτατη αποκωδικοποίηση του πλήθους των πληροφοριών μέσα από το σκανάρισμα αυτών των σχημάτων δύο διαστάσεων με την χρήση τεχνολογικού εξοπλισμού σκάνερ ή την χρήση των κινητών τηλεφώνων τύπου smartphones με την εγκατάσταση ανάλογου λογισμικού. Αυτά με τις δυνατότητες που έχουν ανιχνεύουν την δύο διαστάσεων ψηφιακή εικόνα από έναν αισθητήρα εικόνας ημιαγωγού και στη συνέχεια ψηφιακά αναλύονται από έναν προγραμματισμένο επεξεργαστή.

6.1 Ιστορική Αναδρομή.

Στα πρώτα στάδια επινόησης και εφαρμογής, η χρήση τους από το 1994 εφαρμόστηκε αρχικά και περιορίστηκε στην βιομηχανία κατασκευής αυτοκινήτων για τον εντοπισμό των ανταλλακτικών σε διάφορα στάδια της παραγωγής, διότι η Denso-Wave ειδική στις εφαρμογές barcodescanner, η οποία και τα επινόησε, δούλευε για λογαριασμό της αυτοκινητοβιομηχανίας Toyota.

Σύντομα όμως η χρήση τους ξεπέρασαν τις βιομηχανικές εφαρμογές και έγιναν δημοφιλή και σε άλλες εφαρμογές καθημερινής χρήσης, κατακτώντας τον χώρο της διαφήμισης και της τυποποίησης προσφέροντας τεράστιες δυνατότητες πληροφόρησης στους καταναλωτές λόγω της ταχύτητας ανάγνωσης του μεγάλου όγκου πληροφοριών σε σύγκριση με τα παλιά παραδοσιακά UPCbarcodes.

Ευρεία διάδοση και χρήση των QRCode έγινε στην αρχή κυρίως στην Ιαπωνία και την Αμερική αλλά τελευταία η χρήση τους διαδόθηκε παντού με τις στατιστικές να δείχνουν ότι κατά τον μήνα Ιούνιο του 2011, 14 εκατομμύρια χρήστες έχουν σκανάρει ένα QRCode ή ένα barcode. Ένα ποσοστό 58% από αυτούς τους χρήστες έχουν σκανάρει ένα QR ή barcode από το σπίτι τους, ενώ 39% σκανάρισαν από καταστήματα λιανικής πώλησης; 53% από τα 14 εκατομμύρια χρηστών ήταν άνδρες μεταξύ 18 και 34 ετών.»

6.2 Τεχνικά Στοιχεία για τα QRCodes.

Ο κώδικας αποτελείται από μαύρες ενότητες (τετράγωνες κουκκίδες) οι οποίες διατάσσονται σε ένα τετράγωνο σχέδιο σε λευκό φόντο. Οι κωδικοποιημένες, byte / binary, Kanji), ή μέσω υποστηριζόμενων πληροφορίες μπορεί να αποτελούνται από τέσσερα τυποποιημένα είδη ("modes") των δεδομένων (αριθμητικά, αλφαριθμητικά επεκτάσεων, σχεδόν κάθε είδος δεδομένων.

Ο όγκος των δεδομένων που μπορούν να αποθηκευτούν σε ένα QRCode εξαρτάται από τον τύπο δεδομένων (mode, ή σύνολο χαρακτήρων εισόδου), έκδοση (1, ..., 40, αναφέροντας τις συνολικές διαστάσεις του συμβόλου), και το σφάλμα επίπεδο διόρθωσης (errorcorrectionlevel).

Σε ένα QRCode μπορούν να αποθηκευτούν δεδομένα που έχουν μέγεθος 7.089 αριθμητικοί χαρακτήρες, 4.296 αλφαριθμητικοί χαρακτήρες, 2.953 χαρακτήρες binary (bytes).

Η Γιαπωνέζικη NTTDoCoMo έχει δημιουργήσει τα defacto πρότυπα για την κωδικοποίηση κάθε είδους δεδομένων, όπως URL's, στοιχεία επικοινωνίας, bookmark, map, κλπ.

Στην εφαρμογής τους στην καθημερινή μας ζωή μεγάλο ρόλο έπαιξαν ευρεία η διάδοση των κινητών τηλεφώνων smartphones (Android, Iphone κλπ) αλλά και τον tablet (ipad κλπ) διότι έβαλαν μέσα στην τσέπη του καθενός έναν σαρωτή γραμμωτού κώδικα (barcodescanner) το οποίο χωρίς ιδιαίτερες τεχνικές γνώσεις μπορεί να το χρησιμοποιεί καθημερινά παντού. Συνεπώς οι χρήστες πλέον μπορούν εύκολα και γρήγορα, σαρώνοντας το QRCode με την φωτογραφική μηχανή του κινητού τους και την χρήση κατάλληλου λογισμικού ή μια app (συντόμευση για το application) και του αλγορίθμου διόρθωσης σφαλμάτων, να αποκωδικοποιήσουν με αξιοπιστία, ταχύτητα και ασφάλεια το πλήθος πληροφοριών, να τις αποθηκεύσουν, να της χρησιμοποιήσουν αργότερα ή να τις επεξεργαστούν κάνοντας ταυτόχρονη χρήση και του ιντερνέτ.[41]

Κεφάλαιο 7: Προτεινόμενη αρχιτεκτονική ασφάλειας και πρόσβασης χρηστών σε υπηρεσίες cloud

Στην συγκεκριμένη πτυχιακή θα αναφερθούμε και σε μια αρχιτεκτονική που θα μπορεί να μας παρέχει της προαπαιτούμενες ασφάλειες όπως έχουμε αναφέρει παραπάνω και με την ευκολία της πρόσβασης. Πόσες φόρες έχουμε χρειαστεί να κάνουμε login σε έναν δημόσιο χώρο; Είναι ένα από τα πιο συχνά φαινόμενα και άβολα ταυτόχρονος όταν έχεις στο μυαλό σου την είσοδο το στοιχείων μπροστά σε τρίτους μάρτυρες. Εμείς θα προτείνουμε μια αρχιτεκτονική η όποια θα εξαλείφει το κίνδυνο της χρήσης της υπηρεσίας σε δημοσίους χώρου. Προσφέροντας την δυνατότητα της πρόσβασης χωρίς καμία είσοδο προσωπικών στοιχείων. Η αρχιτεκτονική παρέχει ασφάλεια και ευκολία στην πρόσβαση μέσω των δαχτυλικών αποτυπωμάτων και με μέσω QRcode που θα αναφερθούμε σε λίγο.Τα δακτυλικά αποτυπώματα όπως προείπαμε δεν είναι ο καταλληλότερος τρόπος για να κάνουμε ταυτοποίηση στοιχείων μέσω διαδικτύου αλλά είναι αρκετά κατάλληλος όταν αναφέρεται στο ξεκλείδωμα και ταυτοποίηση μέσω μιας συσκευής.

7.1 Εφαρμογή αρχιτεκτονικής με δακτυλικά αποτυπώματα και QRcodes.

Η αρχιτεκτονική για να τεθεί σε λειτουργία προϋποθέτει κάποια τεχνικά χαρακτηριστικά.

Βασικό χαρακτηριστικό είναι ο εξοπλισμός του χρήστη και συγκεκριμένα θα αναφερθούμε σε εφαρμογή κινητού τηλεφώνου οπότε το κινητό τηλέφωνο του χρήστη να είναι συμβατό με δυνατότητα αναγνώρισης δακτυλικών αποτυπωμάτων. Σήμερα μπορεί να είναι περιορισμένος ο αριθμός το κινητών τηλεφώνων με τις κατάλληλες προϋποθέσεις αλλά με την εξέλιξη της τεχνολογίας και τις ανάγκες των καταναλωτών είναι πολύ πιθανόν σε λίγο χρονικό διάστημα όλα τα κινητά τηλέφωνα να είναι αναβαθμισμένα με την εξής δυνατότητα. Μια άλλη προϋπόθεση είναι να έχει κάμερα το κινητό τηλέφωνο ώστε να μπορεί να κάνει αναγνώριση του QRcode κάτι το οποίο είναι τυποποιημένο σε κάθε κινητό και τέλος φυσικό ακόλουθο να υποστηρίζει λειτουργικό σύστημα που μπορεί να εκτελέσει εφαρμογές.

Δεδομένο ότι οι παραπάνω προϋποθέσεις ισχύουν ο χρηστής θα πρέπει να κατεβάσει μια εφαρμογή της υπηρεσίας cloud που χρησιμοποιεί και θα κάνει την ταυτοποίηση μέσα στην εφαρμογή βάζοντας τα στοιχειά πρόσβασης του λογαριασμού (username και password) .

Η εφαρμογή τότε θα ζητήσει να γίνει αναγνώριση του δακτυλικού αποτυπώματος του χρήστη .Αφού γίνει είσοδος του δακτυλικού αποτυπώματος η εφαρμογή παντρεύει τα στοιχειά του χρήστη με το δακτυλικό αποτύπωμα.

Ένα πλεονέκτημα είναι ότι ο συνδρομητής χρησιμοποιεί ήδη εφαρμογή χωρίς να χρειάζεται να βάλει τα στοιχειά πρόσβασης.

Η συνεχεία της αρχιτεκτονικής είναι όταν ο συνδρομητής θέλει να κάνει είσοδο στο λογαριασμό μέσω κάποιου ηλεκτρονικού υπολογιστή που δεν τηρεί τις προϋπόθεση για αναγνώριση δακτυλικού αποτυπώματος. Ο συνδρομητής μπαίνει στην σελίδα της υπηρεσίας του από έναν περιηγητή και στην σελίδα εμφανίζονται δυο επιλογές.

- Να γίνει είσοδος μέσω στοιχείων πρόσβασης
- Να γίνει είσοδος μέσωQRcode

Σε αυτήν την φάση ο server έχει στείλει ένα μοναδικό cookie στον browser του χρήστη με το οποίο έχει αντιστοιχήσει μοναδικά την συνεδρία με αυτόν τον browser.

Το QRcode θα ενεργοποιεί ένα link το οποίο θα είναι ενεργοποιημένο για ένα μικρό χρονικό διάστημα. Ο χρηστής αν επιλέξει την δεύτερη επιλογή θα σκανάρει μέσω της εφαρμογής στο κινητό όπου έχει ήδη ταχτοποιηθεί η είσοδος μέσω δακτυλικού αποτυπώματος το εμφανιζόμενο στην οθόνη QRcode για να εισέρθει στην υπηρεσία.

Η εφαρμογή διαβάζοντας το QRcode θα κάνει αναγνώριση του συνδέσμου που έχει το qrcode και αφού γίνετε η αυθεντικοποίηση στο server της υπηρεσίας ότι ο σύνδεσμος είναι έγκυρος και έπειτα στέλνει τα στοιχειά πρόσβασης του χρήστη.

Ο server κάνει ταυτοποίηση των στοιχείων πρόσβασης και δίνει την πρόσβαση στο χρήστη. Σε αυτό το σημείο το σύστημα του server θεωρεί ότι η συνεδρία που είχε κωδικοποιηθεί με το συγκεκριμένο cookie πλέον ανήκει στον αρμόδιο χρήστη. Τελικά γίνετε η είσοδος του χρήστη στην υπηρεσία από ιδιωτικό ή κοινόχρηστο υπολογιστή χωρίς της εισαγωγή του username και password.

Εικόνα 18: Προτεινόμενη Αρχιτεκτονική Ασφαλείας και Πρόσβασης.

Γενικά Συμπεράσματα

Το cloudcomputing υπόσχεται να έχει εκτεταμένες συνέπειες για τα συστήματα και τα δίκτυα εταιριών και άλλων οργανισμών. Δίνει έμφαση στο κόστος και στην απόδοση των οφελών του δημοσίου cloudcomputing, ωστόσο, τείνει να επισκιάσει μερικά από τα θεμελιώδη προβλήματα ασφάλειας και ιδιωτικότητας, τα οποία αντιμετωπίζουν εταιρίες και άλλοι οργανισμοί στα υπολογιστικά περιβάλλοντα.

Πολλά από τα χαρακτηριστικά που κάνουν το cloudcomputing ελκυστικό μπορούν επίσης να έρχονται σε αντίθεση με την παραδοσιακή ασφάλεια, τα παραδοσιακά μοντέλα και τους παραδοσιακούς ελέγχους. Πολλά κρίσιμα κομμάτια της τεχνολογίας, όπως η λύση για την ομοσπονδιακή εμπιστοσύνη, δεν έχουνε ακόμα υλοποιηθεί πλήρως, επηρεάζοντας έτσι την επιτυχή ανάπτυξη του cloudcomputing.

Ο καθορισμός της ασφάλειας πολύπλοκων συστημάτων ηλεκτρονικών υπολογιστών είναι επίσης ένα μακροχρόνιο θέμα που απασχολεί τους υπολογιστές και το cloudcomputing ειδικότερα. Η επίτευξη και υλοποίηση ιδιοτήτων υψηλής αξιοπιστίας είναι ένας απατηλός στόχος της ασφάλειας των υπολογιστών για τους ερευνητές και τους επαγγελματίες και όπως αποδεικνύεται είναι μια εργασία που προοδεύει στο cloudcomputing. Παρόλα αυτά, το δημόσιο cloudcomputing είναι ένα συναρπαστικό υπολογιστικό πλέγμα το οποίο οι οργανισμοί πρέπει να ενσωματώσουν ως μέρος της τεχνολογίας των πληροφοριών τους. Αυτός που λογοδοτεί για την ασφάλεια και την προστασία της ιδιωτικής ζωής στα δημόσια cloud παραμένει να είναι ο οργανισμός.

Τα εταιρικά δεδομένα πρέπει να προστατεύονται με τέτοιο τρόπο που να συνάδει με τις πολιτικές, είτε στο κέντρο πληροφορικής του οργανισμού ή στο cloud. Ο οργανισμός πρέπει να διασφαλίζει ότι η ασφάλεια και ο έλεγχος της ιδιωτικότητας εφαρμόζονται σωστά και λειτουργούν όπως προβλέπεται. Η μετάβαση σε ένα εξωτερικό συνεργάτη δημοσίου cloudcomputing περιβάλλοντος είναι από πολλές απόψεις μια έκθεση σε κίνδυνο. Η διαχείριση κινδύνου συνεπάγεται με τον προσδιορισμό και την αξιολόγηση του κινδύνου, και λαμβάνοντας τα μέτρα για τη μείωσή του σε ένα αποδεκτό επίπεδο. Η εκτίμηση και η διαχείριση των κινδύνων σε ένα cloud μπορεί να γίνει μια πρόκληση. Καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος, οι κίνδυνοι που εντοπίζονται πρέπει να εξισορροπούνται προσεκτικά κατά των ελέγχων ασφαλείας και ιδιωτικότητας που είναι διαθέσιμοι και με τα αναμενόμενα οφέλη που προκύπτουν από την χρήση τους. Πάρα πολλοί έλεγχοι μπορεί να είναι περίπλοκοι αναποτελεσματικοί, αν τα οφέλη υπερτερούν του κόστους και των συναφών κινδύνων. Οι ομοσπονδιακές υπηρεσίες και οι οργανισμοί θα πρέπει να εργαστούν για να διασφαλίσουν την κατάλληλη ισορροπία μεταξύ του αριθμού και της ισχύος των ελέγχων και των κινδύνων που σχετίζονται με λύσεις του cloudcomputing. Όπως διαπιστώνουμε, τόσο οι κίνδυνοι όσο και τα πλεονεκτήματα που προσφέρει το cloudcomputing είναι σημαντικά.

Το cloud είναι η εξέλιξη των σημερινών δικτύων και υπόσχεται πολύ σοβαρές αλλαγές, που θα μας λύσουν τα χέρια. Κάποιοι ίσως να μη το εμπιστεύονται – αν το καλοσκεφτούμε όμως έχει πάρα πολλά θετικά. Στη πραγματικότητα δεν είναι χειρότερο από τη σημερινή κλασική δικτυακή τεχνολογία. Το αντίθετο μάλλον συμβαίνει. Η μόνη διαφορά με τη παρούσα κλασική προσέγγιση δικτύων και ασφάλειας, είναι ότι θα προσφέρει νέες προκλήσεις και προβλήματα που θα πρέπει να λυθούν. Με την εξάπλωση της τεχνολογίας θα επιβιώσουν οι πάροχοι που έχουν προσέξει τον πελάτη και τον έχουν διασφαλίσει όσο το δυνατόν καλύτερα. Το

cloudμπορεί να μη θεωρείται ακόμα απόλυτα ασφαλές. Όσο όμως περνάει ο χρόνος, είναι πιθανό να αρθούν όλες οι επιφυλάξεις και τελικά το cloudcomputing να αποδειχθεί η πλέον ασφαλής πλατφόρμα λειτουργίας των πληροφοριακών υποδομών μιας επιχείρησης ή ενός οργανισμού [36].

Βιβλιογραφία

1)http://en.wikipedia.org/wiki/Ubiquitous_computing

2)http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf

3)http://cloudcomputing.sys-con.com/node/581838

4)https://en.wikipedia.org/wiki/Grid_computing

5)https://en.wikipedia.org/wiki/Utility_computing

6)http://computer.howstuffworks.com/server-virtualization2.htm

7)https://en.wikipedia.org/wiki/Virtualization

8)http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

9) Cloud security and privacy, Above the clouds(A Berkeley View Of Cloud Computing) Electrical engineering and Computer Sciences University of California at Berkeley.__

10)http://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

11)https://en.wikipedia.org/wiki/Cloud_computing

12)http://www.njvc.com/fathers-of-cloud-computing

13)https://en.wikipedia.org/wiki/Cloud_computing

14)http://www.cloud-lounge.org/clouds-in-IT-history.html

15)http://seattletimes.com/html/microsoftpri0/2011255515_steve_ballmer_speech_at_uw_were_all_in_for_cloud_c.html

16)http://www.metadosi-ischios.gr/article.php?ID=186

17)https://www.youtube.com/watch?v=xsQcQxI3HZgCloud Computing and Security (CSCAN | PlymUniInfoSec)

18) Cloud Security: A Live Technical Analysis
Microsoft TechEd North America

https://www.youtube.com/watch?v=GwgFcauwDXI

19)http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

20)Model for cloud computing security assessment based on AHP and FCEZhuRuo-xin; Xiao-jie Cui; Shi-jun Gong; Hong-kang Ren; KeChenComputer Science & Education (ICCSE), 2014 9th International Conference on

21)https://en.wikipedia.org/wiki/IPsec

22) http://www.networksorcery.com/enp/protocol/esp.htm

23)http://www.techopedia.com/definition/1504/encapsulating-security-payload-esp

24)Ασφάλεια Δικτύων ,ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ

25)http://el.wikipedia.org/wiki/SSL

26)http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%91%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82_%CE%95%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%CF%82

27) Secure Model for Virtualization Layer in Cloud Infrastructure
SinaManavi*, SadraMohammadalian, NurIzuraUdzir, Azizol Abdullah

28)**https://en.wikipedia.org/wiki/Intrusion_detection_system**

29)http://en.wikipedia.org/wiki/Honeypot_(computing)

30)**https://en.wikipedia.org/wiki/Intrusion_prevention_system**

31)**https://en.wikipedia.org/wiki/Cyclic_redundancy_check**

32) THE CHINESE WALL SECURITY POLICY
Dr. David F.C. Brewer and Dr. Michael J. Nash
GAMMA SECURE SYSTEMS LIMITED
9 Glenhurst Close, Backwater, Camberley, Surrey, GUI 7 9BQ, United Kingdom

33)https://en.wikipedia.org/wiki/Chinese_wall

34)ChineseWall Security Access Control in Cloud computing

SreeprasadGovindankutty
Committee Chair: Professor. Rajendra. K. Raj
Reader: Professor: Xumin Lu
Department of Computer Science
B. Thomas Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, New York
July 29, 2013

35) A Practical Chinese Wall Security Model in Cloud
Computing
Tien-Hao Tsai*, Yen-Chung Chen*†, Hsiu-Chuan Huang*†, Pei-Ming Huang* and Kuo-Sen Chou*
*Information & Communication Security Lab
Chunghwa Telecom Laboratories
Taoyuan, R.O.C.
{p1t1r,yzchen,pattyh,peiming,cksp}@cht.com.tw
†Institute of Computer Science and Engineering
National Chiao Tung University
Hsinchu, R.O.C.

36) NIST (National Institute of Standards and Technology) Guidelines on Security and Privacy in Public Cloud Computing, IT Professional.security

37)https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

38) https://en.wikipedia.org/wiki/Fingerprint#

39) http://www.biometrics.gov/Documents/FingerprintRec.pdf

40)http://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/

41) http://www.dataonline.gr/qr-codes.html