Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Μυστικότητα και Εμπιστευτικότητα σε Αρχιτεκτονικές Υπολογιστικού Σύννεφου (Cloud Computing)

Πολυξένη Σπανάκη

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μαϊος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μυστικότητα και Εμπιστευτικότητα σε Αρχιτεκτονικές Υπολογιστικού Σύννεφου (Cloud Computing)

Πολυξένη Σπανάκη

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μαϊος 2017

Περίληψη

Η εξέλιξη στην Τεχνολογία των Πληροφοριών, εισήγαγε το Cloud Computing ως μία νέα τεχνολογία η οποία αφορά την "εικονικοποίηση" (virtualization) των διαθέσιμων πόρων. Το Cloud Computing περιλαμβάνει την αποθήκευση και την πρόσβαση σε δεδομένα καθώς και την ανάπτυξη και διαχείριση εφαρμογών μέσω του διαδικτύου. Ανεξάρτητα από τα πολλά πλεονεκτήματα από την συγκεκριμένη τεχνολογία, όπως η διαθεσιμότητα των αποθηκευμένων δεδομένων, ο περιορισμός του κόστους και η επεκτασιμότητα, η Ασφάλεια και η Ιδιωτικότητα θεωρούνται κρίσιμοι παράγοντες.

Στην συγκεκριμένη μεταπτυχιακή διατριβή, οι βασικοί στόχοι είναι η παρουσίαση και η ανάλυση των ζητημάτων Ιδιωτικότητας και Εμπιστευτικότητας, στις Αρχιτεκτονικές του Υπολογιστικού Σύννεφου. Απειλές ασφάλειας που αφορούν την διαχείριση ευαίσθητων δεδομένων, οι ευπάθειες καθώς και η ασφάλεια του δικτύου, είναι μερικές από τις προκλήσεις που αντιμετωπίζονται.

Η μεθοδολογία που ακολουθείται γίνεται μέσω της χρήσης ενός εικονικού περιβάλλοντος. Με την χρήση εργαλείων αυτοματοποίησης, ακολουθείται μια συγκεκριμένη μεθοδολογία ώστε οι απομακρυσμένοι εξυπηρετητές να διαμορφωθούν κατάλληλα, μέσα στο Υπολογιστικό σύννεφο και τελικά να ασφαλιστούν.

Το **πρώτο κεφάλαιο** εισάγει την έννοια του Cloud Computing καθώς και μερικά ιστορικά στοιχεία, πλεονεκτήματα και μειονεκτήματα της χρήσης του καθώς και τα βασικά χαρακτηριστικά του.

Οι βασικοί στόχοι του **δεύτερου κεφαλαίου** είναι η παρουσίαση και ανάλυση των βασικών στοιχείων που αφορούν την ασφάλεια στις Αρχιτεκτονικές του Υπολογιστικού σύννεφου.

Στο **τρίτο κεφάλαιο** παρουσιάζεται η βασική μεθοδολογία καθώς και τα εργαλεία αυτοματοποίησης που χρησιμοποιήθηκαν.

Στο **τέταρτο κεφάλαιο** αναλύονται οι βασικές ευπάθειες που βρέθηκαν.

Η διατριβή ολοκληρώνεται με το **πέμπτο κεφάλαιο** που περιλαμβάνει τον επίλογο.

Summary

Evolution in Information Technology, has introduced Cloud Computing as a new technology that refers to resource virtualization. Cloud Computing involves storing and accessing data and developing and managing applications over the Internet. Despite the many advantages of the specific technology, such as the availability of stored data, cost and time saving and scalability, Security and Privacy are considered critical factors in Cloud Computing.

This Master's degree dissertation main targets, are to present and discuss privacy and confidentiality issues, in Cloud computing. Some of the many challenges faced are security threats regarding managing sensitive data and vulnerabilities in the virtualized environment and network security.

The methodology used, in order to demonstrate these issues, is by using a virtualized environment and software automation tools. The remote hosts are configured, within the cloud in order to be secured.

The **first chapter** introduces Cloud Computing as well as some evolution information, advantages and disadvantages and main characteristics.

The main target of the **second chapter** is the discussion of Cloud's Security main aspects.

In the **third chapter** the main methodology is introduced as well as the automation tools used.

The **fourth chapter** analyzes and discusses the main vulnerabilities found.

This dissertation ends with the **fifth chapter** which includes the conclusions.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Νικόλαο Σκλάβο για την πολύτιμη βοήθεια και την εξαιρετική συνεργασία μας.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου καθώς και τους φίλους μου για την στήριξη που μου παρείχαν.

Περιεχόμενα

1 Εισαγωγή 6

1.1 Υπολογιστικό σύννεφο 7

1.1.1 Ιστορικά Στοιχεία 10

1.1.2 Πλεονεκτήματα και μειονεκτήματα της χρήσης του Υπολογιστικού συννέφου 11

1.2 Αρχιτεκτονική του Υπολογιστικού σύννεφου 14

1.2.1 Software-as-a-Service 15

1.2.2 Platform-as-a-Service 16

1.2.3 Infrastructure-as-a-Service 16

1.3 Μοντέλα ανάπτυξης του Υπολογιστικού σύννεφου 17

1.4 Υπολογιστικό σύννεφο και εξέλιξη 20

2 Ασφάλεια στο Υπολογιστικό σύννεφο 22

2.1 Ευπάθειες εξειδικευμένες στο Υπολογιστικό σύννεφο 25

2.2 Ζητήματα ασφάλειας στο Υπολογιστικό σύννεφο 27

2.3 Γνωστές Επιθέσεις 29

3 Μεθοδολογία 33

3.1 Εργαλεία Αυτοματοποίησης 34

3.1.1 Vagrant by HashiCorp 35

3.1.2 Ansible 37

3.2 Δημιουργία Εικονικού Περιβάλλοντος Υπολογιστικού σύννεφου 41

3.3 Ρύθμιση και ασφάλιση του Εικονικού Περιβάλλοντος Υπολογιστικού σύννεφου 43

3.3.1 Απαραίτητα βήματα εξασφάλισης της ασφάλειας στο εικονικό περιβάλλον 46

4 Ανίχνευση Ευπαθειών 60

4.1 Nessus 63

4.2 OpenVas 66

5 Επίλογος 68

Δημοσίευση 76

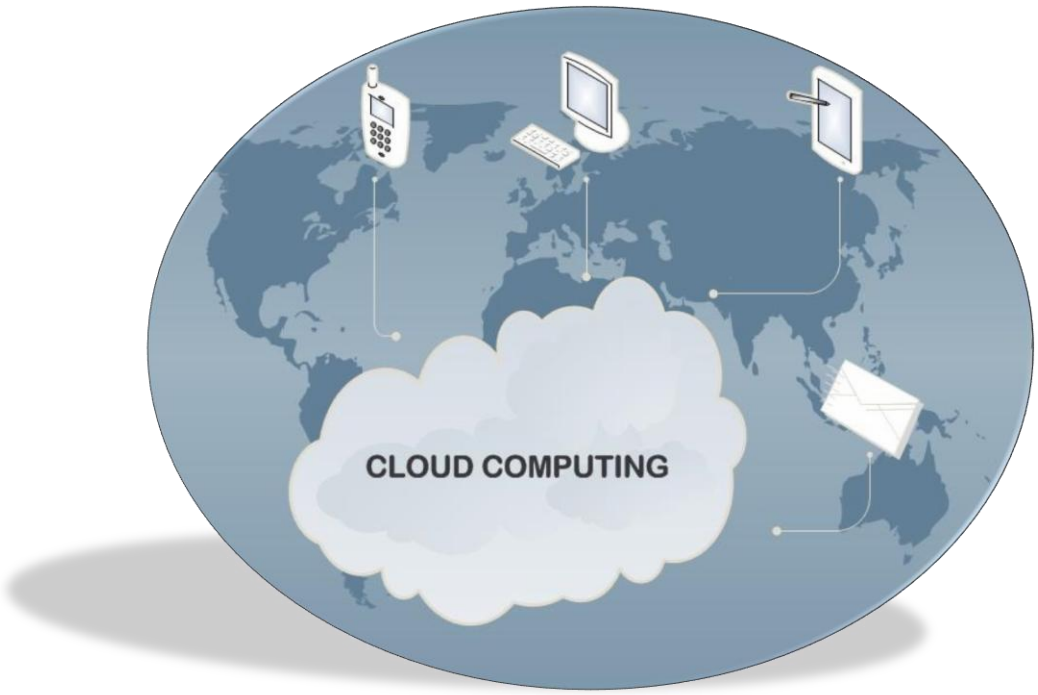
Βιβλιογραφία 77

Κεφάλαιο 1
Εισαγωγή

Η δημοτικότητα του Υπολογιστικού σύννεφου (Cloud Computing), κατά την διάρκεια των τελευταίων ετών, έχει αυξηθεί καθώς ο αριθμός των οργανισμών και εταιριών της Τεχνολογίας των Πληροφοριών (Information Technology- IT) που χρησιμοποιεί τέτοιου είδους πλατφόρμες, ολοένα και αυξάνεται.

Η ευρεία και αυξανόμενη χρήση του Υπολογιστικού σύννεφου απορρέει από το πλήθος των διάφορων υπηρεσιών που προσφέρονται, καθώς και από τα πολλά οφέλη της χρήσης του. Το Cloud, τα τελευταία χρόνια, έχει αποδεικτεί ως μία δημοφιλή περιοχή έρευνας, σχεδιασμού αλλά και ανάπτυξης πολλαπλών εφαρμογών [01], όπως βλέπουμε στην Εικόνα 1. Κάθε χρήστης προσφέρεται με τεράστιο αριθμό επεξεργαστικής ισχύος, με συνδυασμό ανεξάντλητο πλήθος πόρων, με ιδιαίτερα χαμηλό οικονομικό κόστος.

Το Cloud Computing έχει προσφέρει τεράστια αλλαγή, όσο αφορά τον τρόπο με τον οποίο οι υπηρεσίες παραδίδονται στους χρήστες. Αυτό το νέο μοντέλο προσφέρει στους καταναλωτές, λογισμικό, διαφορετικές πλατφόρμες καθώς και υποδομές με την μορφή υπηρεσιών μέσω του διαδικτύου, χωρίς ο ίδιος ο καταναλωτής να είναι ενήμερος για την ακριβή φυσική τοποθεσία όπου οι συγκεκριμένες υπηρεσίες εκτελούνται [02].



Εικόνα 1. Απεικόνιση του Υπολογιστικού σύννεφου.

Στόχοι αυτής της μεταπτυχιακής διατριβής, αποτελούν η παρουσίαση αλλα και η ανάλυση των ζητημάτων Ιδιωτικότητας και Εμπιστευτικότητας, στις Αρχιτεκτονικές του Υπολογιστικού Σύννεφου. Μερικές από τις προκλήσεις που αντιμετωπίζονται αποτελούν οι απειλές ασφάλειας που αφορούν την διαχείριση ευαίσθητων δεδομένων, οι ευπάθειες καθώς και η ασφάλεια του δικτύου.

Η μεθοδολογία που ακολουθείται γίνεται μέσω της χρήσης ενός εικονικού περιβάλλοντος. Με την χρήση εργαλείων αυτοματοποίησης, ακολουθείται μια συγκεκριμένη μεθοδολογία ώστε οι απομακρυσμένοι εξυπηρετητές να διαμορφωθούν κατάλληλα, μέσα στο Υπολογιστικό σύννεφο και τελικά να ασφαλιστούν.

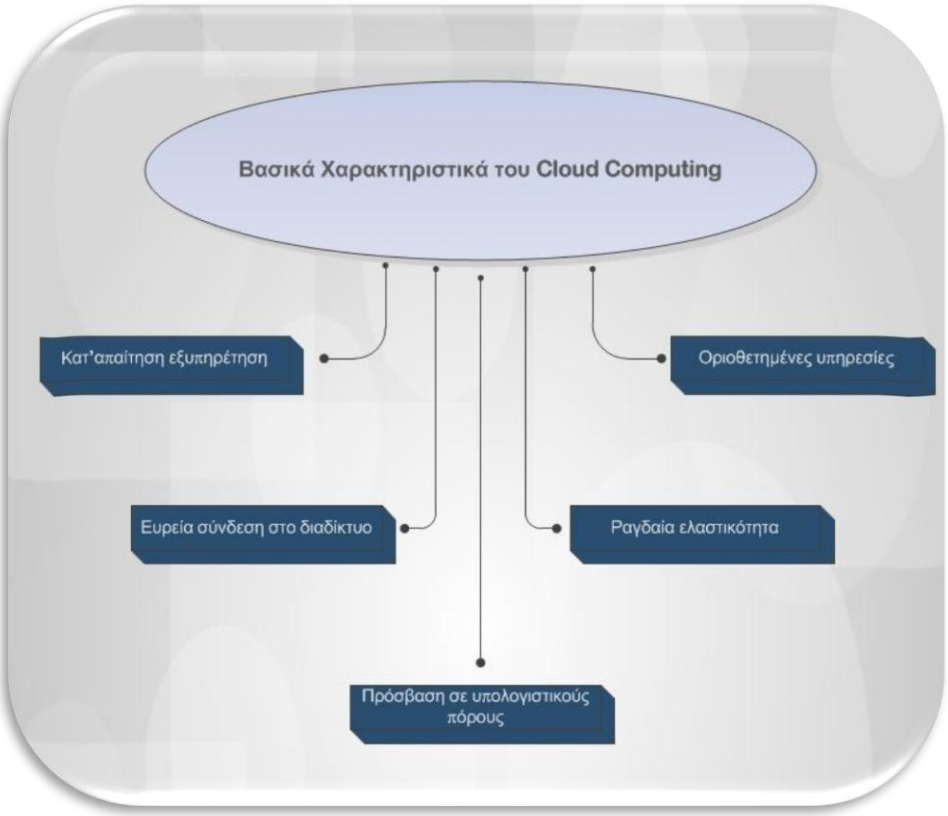
1.1 Υπολογιστικό Σύννεφο

Σύμφωνα με το Ινστιτούτο NIST (National Institute of Standards and Technology), το Υπολογιστικό σύννεφο αποτελεί ένα μοντέλο το οποίο παρέχει σταθερή, πρακτική καθώς και κατ'αίτηση πρόσβαση σε ένα μεγάλο πλήθος διαμοιραζόμενων πόρων. Οι πόροι αυτοί, μπορεί να αποτελούνται από δίκτυα, διακομιστές, αποθηκευτικό χώρο, εφαρμογές αλλά και υπηρεσίες που

παρέχονται μέσω διαδικτύου. Οι παραπάνω πόροι και υπηρεσίες μπορούν να προμηθευτούν στους καταναλωτές με ελάχιστη διαχειριστική προσπάθεια και κόστος [03].

Το Cloud Computing αποτελεί μία νέα αναδυόμενη τεχνολογία, η οποία συνδέεται με την έννοια του Grid Computing καθώς και με άλλες συναφή τεχνολογίες όπως το Utility και Distributed Computing [04].

Σύμφωνα με τον ορισμό του Ινστιτούτου NIST, το μοντέλο του Υπολογιστικού σύννεφου διαμορφώνεται από κάποια βασικά χαρακτηριστικά όπως η κατ'απαίτηση εξυπηρέτηση, η ευρεία σύνδεση στο διαδίκτυο, η εύκολη πρόσβαση σε ομάδες υπολογιστικών πόρων, η ραγδαία ελαστικότητα και οι οριοθετημένες διαθέσιμες υπηρεσίες [03], όπως απεικονίζεται στην Εικόνα 2.



Εικόνα 2. Χαρακτηριστικά του Υπολογιστικού σύννεφου.

1. Κατ'απαίτηση εξυπηρέτηση. Ο χρήστης της πλατφόρμας του Υπολογιστικού σύννεφου μπορεί ανεξάρτητα, να εφοδιαστεί με κάθε είδους παροχές όπως για παράδειγμα διαδικτιακό αποθηκευτικό χώρο, αυτόματα δίχως την ανθρώπινη αλληλεπίδραση μεταξύ αυτού και του προμηθευτή της υπηρεσίας.

2. Ευρεία σύνδεση στο διαδίκτυο. Όλες οι παροχές είναι διαθέσιμες μέσω του διαδικτύου με σύνδεση η οποία είναι εφικτή μέσω των τυπικών συσκευών διασύνδεσης όπως τα smartphones, tablets, φορητούς υπολογιστές και όλα τα είδη των σταθμών εργασίας.

3. Εύκολη πρόσβαση σε ομάδες υπολογιστικών πόρων. Οι πάροχοι των υπολογιστικών πόρων εξυπηρετούν πολλαπλούς χρήστες, χρησιμοποιώντας ένα μοντέλο "multi-tenant", με πλήθος διαφορετικών φυσικών αλλά και εικονικών πόρων. Οι παροχές αυτές διαθέτονται αλλά και αποσύρονται σύμφωνα με τις ανάγκες του κάθε χρήστη. Ο καταναλωτής δεν είναι απαραίτητο να γνωρίζει ή ακόμα και να διαθέτει κάποιο έλεγχο στην ακριβή φυσική τοποθεσία των διαθέσιμων πόρων , μπορεί όμως να κατέχει γνώση για την πιο ευρεία έννοια της τοποθεσίας στο επίπεδο της χώρας ή ακόμα και του datacenter. Οι διαθέσιμοι υπολογιστικοί πόροι συμπεριλαμβάνουν αποθηκευτικό χώρο, μνήμη καθώς και bandwidth.

4. Ραγδαία ελαστικότητα. Οι υπηρεσίες μπορούν να διατεθούν με μεγάλη ελαστικότητα ώστε να επεκταθούν ανάλογα με τις ανάγκες και απαιτήσεις του κάθε καταναλωτή. Από την προοπτική του χρήστη, οι διαθέσιμοι πόροι φαντάζουν ανεξάντλητοι και μπορούν να αποκτήσουν πρόσβαση σε αυτούς σε οποιαδήποτε χρονική στιγμή.

5. Οριοθετημένες διαθέσιμες υπηρεσίες. Οι παροχές του Υπολογιστικού σύννεφου μπορούν αυτόματα να βελτιστοποιηθούν και να χειρισθούν, επιδρώντας ανάλογα με τον κατάλληλο τύπο της υπηρεσίας που διατίθεται. Κάθε χρήση των πόρων παρακολουθείται αλλά και ελέγχεται, δίνοντας έτσι την αίσθηση της διαφάνειας τόσο για τον χρήστη όσο και για τον πάροχο.

Οι πιο γνωστοί πάροχοι πρόσβασης σε Cloud αποτελούν, η Microsoft Corporation με την πλατφόρμα Azure Services Platform, η Google με τις υπηρεσίες που παρέχονται μέσω του Google App Engine και η Amazon με τις υπηρεσίες που παρέχονται μέσω του Amazon Web Services (AWS) [05].

1. Azure Services Platform. Η συγκεκριμένη πλατφόρμα, η οποία προτάθηκε από τους προγραμματιστές της Microsoft Corporation, παρέχει τέσσερις βασικές υπηρεσίες. Η πρώτη αποτελεί την Windows Azure, η οποία παρέχει εφαρμογές δικτύου, η .NET Services η οποία χρησιμοποιείται για επίλυση συγκεκριμένων προβλημάτων σύνδεσης

διαφόρων υπηρεσιών καθώς και εκτέλεση ελέγχου πρόσβασης. Επίσης παρέχει τις υπηρεσίες SQL Services και Live Frameworks.

2. Google App Engine. Η Google App Engine παρέχει εφαρμογές δικτύου και ιστοσελίδων σε διακομιστές της Google. Με κάποιο λογαριασμό στην Google, υπάρχει η δυνατότητα χρήσης όλων αυτών των εφαρμογών, χωρίς δημιουργία ξεχωριστών λογαριασμών για κάθε μία από αυτές. Η πλατφόρμα App Engine διαθέτει ενσωματωμένες εφαρμογές με κάποιους περιορισμούς, κάποιοι εκ των οποίων αφορούν την γλώσσα προγραμματισμού που θα πρέπει να γνωρίζουν καθώς και τον διαθέσιμο αποθηκευτικό χώρο.

3. Amazon Web Services (AWS). Η πλατφόρμα που προσφέρεται από την Amazon, παρέχει μεγάλο πλήθος υπηρεσιών όπως αποθηκευτικό χώρο δεδομένων, δυνατότητα ενοικίασης εικονικών διακομιστών καθώς και άλλων ειδών υπηρεσίες. Αυτές αποτελούν τις Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) και Amazon Cloud Front.

1.1.1 Ιστορικά Στοιχεία

Αν και η έννοια του Cloud Computing θεωρείται σχετικά χρονολογικά νέα στον τομέα της Πληροφορικής, στην ουσία αποτελεί εξέλιξη του Utility και Grid Computing. Ο όρος "Cloud", αναφέρεται κυρίως στην διασύνδεση πολλών υπολογιστών για διαμοιρασμό και μεταφορά δεδομένων.

Το ARPANET (Advanced Research Agency Network), παρουσιάστηκε από τον J.C.R Licklider στην δεκαετία του 1960. Αποτέλεσε το πρώτο packet switching δίκτυο και τελικά την βάση για την διασύνδεση των υπολογιστικών συστημάτων. Μετά από συνεχή βελτίωση και αναβάθμιση το ARPANET οδήγησε στην εφεύρεση του διαδικτύου, οπότε σταδιακά στην εφεύρεση του Υπολογιστικού σύννεφου [06].

Το διαδίκτυο αποτέλεσε μία από τις πιο σημαντικές τεχνολογικές εφευρέσεις στο τέλος του προηγούμενου αιώνα, με αποτέλεσμα να κατέχει κυρίαρχο ρόλο σε όλους του τομείς των τηλεπικοινωνιών . Στα μέσα της δεκαετίας του ενενήντα ξεκίνησε η «επανάσταση» στον τομέα του διαδικτύου, όπου η χρήση του έγινε εμπορικά διαθέσιμη. Σύμφωνα με έρευνες, η χρήση του διαδικτύου το έτος 1993 για παγκόσμιες ανταλλαγές δεδομένων κυμαίνονταν γύρω στο 1%. Όμως, το έτος 2000 το ποσοστό αυτό αυξήθηκε δραματικά στο 51%, περί το έτος 2007 η χρήση

του διαδικτύου για μεταφορά και διαμοιρασμό των δεδομένων ανέβηκε στο 97% και τελικά την σημερινή εποχή έχει φτάσει στο 100% [07].

Όσο η χρήση των υπολογιστών γινόταν όλο και πιο δημοφιλής και το διαδίκτυο εισήγαγε πολλές διαφορετικές δραστηριότητες και υπηρεσίες, όπως τα μέσα κοινωνικής δικτύωσης, οικονομικές υπηρεσίες και πλήθος online εφαρμογών, η έννοια του Cloud Computing έγινε πραγματικότητα. [06].

Η εμφάνιση του όρου "cloud" ξεκίνησε ως μέρος συζήτησης το 2008 σε κάποιο από τα συνέδρια για την χρήση του διαδικτύου. Κατά την διάρκεια των συζητήσεων αυτών, ο όρος "cloud" χρησιμοποιήθηκε για πρώτη φορά από τον επικεφαλή της Google, Eric Schmidt, και τελικά καθιερώθηκε από τους επιστήμονες, τα μέσα ενημέρωσης και τους χρήστες [05].

Η έννοια αυτή αποτέλεσε καινοτομία στην διαδικασία της μεταφοράς και πρόσβασης σε μεγάλο πλήθος κοινόχρηστων πόρων μέσω του διαδικτύου. Ο παγκόσμιος διαμοιρασμός των πληροφοριών μέσω σύνδεσης στο διαδίκτυο, που ήταν οικονομικά προσιτή προς όλους, αποτέλεσε και τον λόγο για τον οποίο έγινε δυνατή η χρήση αλλά και η κυριαρχία του Υπολογιστικού σύννεφου [07].

Σήμερα οι περισσότερες εταιρίες του χώρου χρησιμοποιούν ενεργά πλατφόρμες Υπολογιστικού συννέφου, κάνοντας την έννοια αυτή ιδιαίτερα ανταγωνιστική στον χώρο της Τεχνολογίας των Πληροφοριών.

1.1.2 Πλεονεκτήματα και μειονεκτήματα χρήσης του Cloud Computing

Η επικράτηση του Cloud Computing, αποτελεί αποτέλεσμα από τα πολλά οφέλη που παρέχονται στις εταιρίες αλλα και στους απλούς καταναλωτές από την χρήση του. Η ανταγωνιστική φύση της έννοιας αυτής, θέτει την πρόκληση στους παρόχους να βελτιώνουν διαρκώς τις υπηρεσίες τους καθώς και να προσπαθούν για την επίλυση πιθανών προβλημάτων που μπορεί να εμφανιστούν. Μερικά από τα πολλά πλεονεκτήματα της χρήσης του Υπολογιστικού σύννεφου, όπως φαίνεται και στην Εικόνα 3., αποτελούν τα εξής [05-06] [08] :

1. Χαμηλό κόστος. Οι οργανισμοί με την χρήση του Cloud μπορούν να μειώσουν τις συνολικές δαπάνες τους, όπως το χρηματικό κόστος του εξοπλισμού αλλά και της συντήρησής του, ακόμα και στο ποσοστό της τάξης του 50%. Παράλληλα, και οι χρήστες

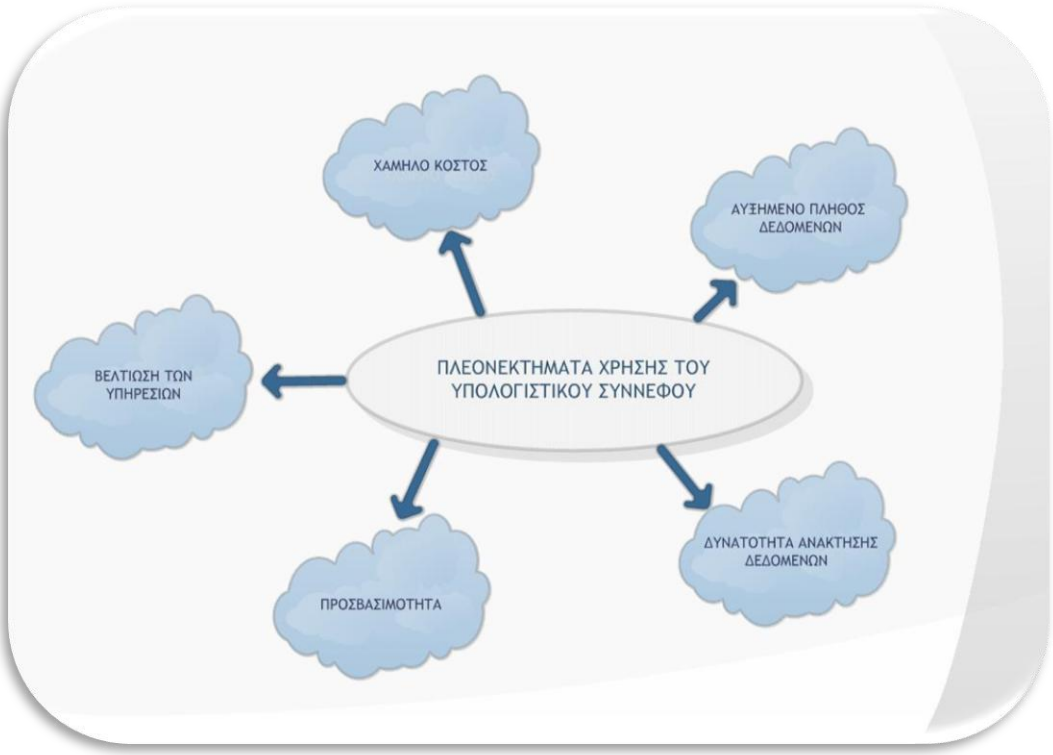
δεν είναι υποχρεωμένοι να κάνουν αγορές ακριβών υπολογιστών με μεγαλύτερη μνήμη ή δίσκο ώστε να συμβαδίζουν με τα τεχνολογικά άλματα. Η μείωση του κόστους, όσο αφορά τους καταναλωτές αλλά και τις εταιρίες αποτελεί ίσως και το μεγαλύτερο όφελος της χρήσης του Υπολογιστικού σύννεφου.

2. Αυξημένο πλήθος αποθηκευμένων δεδομένων. Ένα τεράστιο πλήθος δεδομένων και πληροφοριών είναι διαθέσιμο στους χρήστες μέσω του διαδικτύου. Σε σύγκριση με την αποθήκευση δεδομένων σε προσβάσιμους χώρους αποθήκευσης, το Υπολογιστικό σύννεφο παρέχει μεγαλύτερη ευελιξία και δίνει την δυνατότητα προσαρμογής στις ανάγκες του κάθε χρήστη. Με την αποθήκευση των δεδομένων στο cloud, απαλείφονται πιθανοί περιορισμοί που υπάρχουν με την χρήση των συμβατικών δίσκων.

3. Δυνατότητα ανάκτησης δεδομένων. Με την χρήση του Cloud Computing υπάρχει μία σταθερότητα στην απώλεια δεδομένων ή ακόμα και στην κλοπή του εξοπλισμού για την αποθήκευση των πληροφοριών. Οι υπηρεσίες που προσφέρουν οι πάροχοι στους καταναλωτές, υπόσχονται ανάκτηση των δεδομένων σε οποιαδήποτε περίπτωση απώλειας, καθώς οι πληροφορίες αποθηκεύνται σε αντίγραφα και διανέμονται σε πολλαπλούς διακομιστές οι οποίοι δεν βρίσκονται απαραίτητα στην ίδια γεωγραφική περιοχή.

4. Προσβασιμότητα. Κάθε χρήστης με συσκευή η οποία έχει την δυνατότητα σύνδεσης στο διαδίκτυο, μπορεί οποιαδήποτε στιγμή να έχει πρόσβαση σε πλήθος πληροφοριών και αποθηκευμένων δεδομένων. Το Υπολογιστικό σύννεφο παρέχει υπηρεσίες συμβατές με οποιοδήποτε υπολογιστικό σύστημα καθιστώντας έτσι την πρόσβασή του εφικτή προς όλους. Χρήστες συστήματος Unix, έχουν την δυνατότητα διαμοιρασμού δεδομένων με χρήστες πλατφόρμας Windows ή και αντίθετα, χωρίς κανένα περιορισμό ή πρόβλημα.

5. Βελτίωση των υπηρεσιών. Οι πάροχοι Cloud Computing διαθέτουν στους χρήστες τους συνεχώς βελτιωμένες υπηρεσίες, αυξάνοντας έτσι την ικανοποίηση των καταναλωτών καθώς και την παραγωγικότητά τους. Ένα παράδειγμα βελτίωσης των παρεχόμενων υπηρεσιών, αποτελεί η συνεχής αναβάθμιση των εφαρμογών και προγραμμάτων που διαθέτονται προς χρήση μέσω του cloud.



Εικόνα 3. Πλεονεκτήματα χρήσης του Υπολογιστικού σύννεφου.

Παράλληλα από τα πολλά οφέλη που παρουσιάζονται με την χρήση του Υπολογιστικού σύννεφου, υπάρχουν και κάποια μειονεκτήματα που δημιουργούν κάποιους περιορισμούς αλλά και προβλήματα.

Ένα από αυτά αποτελεί το πρόβλημα της προσβασιμότητας, καθώς σε περιπτώσεις αδυναμίας σύνδεσης στο διαδίκτυο ή σε περιπτώσεις αργής σύνδεσης, η πρόσβαση καθιστάται δύσκολη ή ακόμα και αδύνατη. Το Cloud Computing χρειάζεται πάντα διαδικτυακή σύνδεση για να δώσει την δυνατότητα στους χρήστες να χρησιμοποιήσουν τα προγράμματα, τις εφαρμογές και όλες τις υπόλοιπες παρεχόμενες υπηρεσίες. Αυτό ίσως, αποτελεί και ένα από τα πιο μεγάλα επιχειρήματα που χρησιμοποιούνται κατά της χρήσης του Cloud, χωρίς να υπάρχει μεγάλη βάση πάνω σε αυτό, καθώς η χρήση του διαδικτύου ειναι καθημερινή, παγκόσμια και πλέον αποτελεί βασική ανάγκη [05].

Ένα μεγάλο θέμα στην χρήση του Υπολογιστικού σύννεφου είναι τα ζητήματα ασφάλειας που προκύπτουν. Αν και, οπως αναφέρθηκε, τα οφέλη του Cloud Computing είναι πολλά, με κύρια να αποτελούν τη μείωση του κόστους και την προσβασιμότητα σε τεράστιο πλήθος δεδομένων, τα ζητήματα που προκύπτουν όσο αφορά την ασφάλεια κάνουν αρκετούς οργανισμούς να απέχουν από την χρήση του. Καθώς δεν υπάρχει τεχνολογία με την οποία να υπάρχει μέγιστη και

απόλυτη ασφάλεια της εμπιστευτικότητας των δεδομένων, κάποιος κακόβουλος χρήστης έχοντας πρόσβαση σε τόσο μεγάλο πλήθος δεδομένων θα καταφέρει να επιτεθεί επιτυχημένα, παραβιάζοντας έτσι τα τρία βασικά χαρακτηριστικά της ασφάλειας που αποτελούν η εμπιστευτικότητα, η ακεραιότητα καθώς και η διαθεσιμότητα των δεδομένων.

Μέσα στο περιβάλλον του Cloud, εμφανίζονται πολλές προκλήσεις που αφορούν την ασφάλεια. Οι απειλές ασφάλειας αφορούν δεδομένα, ευαίσθητες και απόρρητες πληροφορίες, δίκτυα και πλήθος ευπαθειών. Οι ευπάθειες αυτές μπορούν εύκολα να εκμεταλλευθούν από κακόβουλους χρήστες και να αποτελέσουν σοβαρό ζήτημα σε οργανισμούς και καταναλωτές.

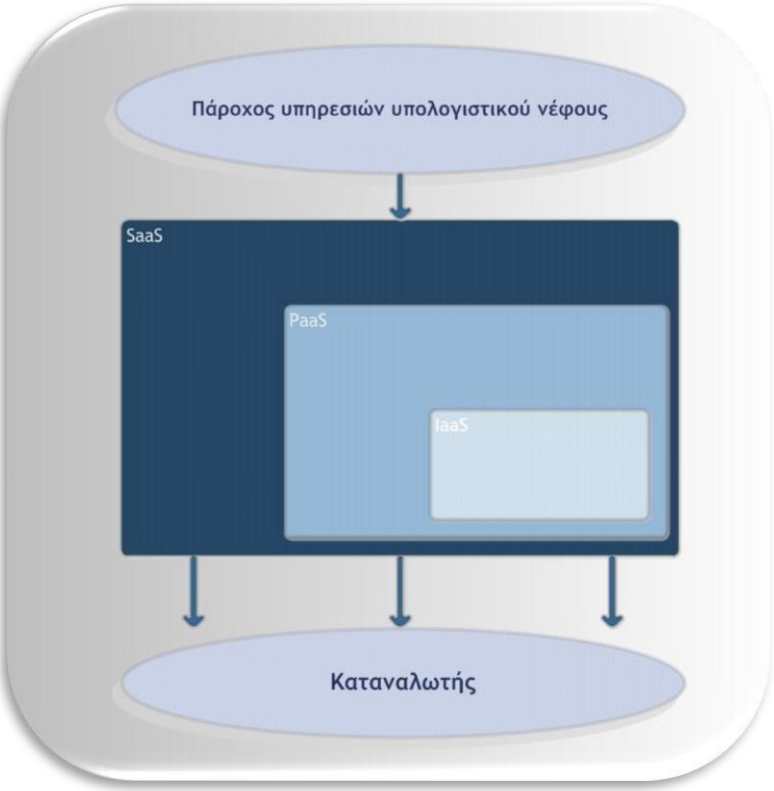
1.2 Αρχιτεκτονική του Υπολογιστικού Σύννεφου

Σύμφωνα με τον οργανισμό NIST (National Institute of Standards and Technology), το Cloud Computing αποτελείται από μία ομάδα μοντέλων παροχής υπηρεσίων. Αυτά τα μοντέλα έχουν σχεδιαστεί ώστε να μπορούν να επιλεχθούν και να τροποποιηθούν ώστε να καλύπτουν τις ανάγκες των οργανισμών και των χρηστών [06]. Όλες οι ανάγκες του κάθε οργανισμού καλύπτονται μέσω της διαδικασίας της "εικονικοποίησης". Σύμφωνα με την συγκεκριμένη διαδικασία, δημιουργείται εικονική έκδοση των πόρων του Cloud και παράλληλα διαχωρίζονται σε πολλαπλά περιβάλλοντα.

Η διαδικασία αυτή, του διαχωρισμού της παροχής των υπηρεσιών μέσω των διάφορων μοντέλων, πέρα από την ευελιξία που μπορεί να προσφέρει, υπόσχεται και πολλά οικονομικά οφέλη.

Τα μοντέλα υπηρεσιών του Υπολογιστικού σύννεφου αποτελούν τα Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) και Infrastructure-as-a-Service (IaaS).

Οι βασικές διακρίσεις των μοντέλων υπηρεσιών του Cloud Computing, περιγράφονται αναλυτικά στα υποκεφάλαια 1.2.1, 1.2.2 και 1.2.3 αλλα και στην Εικόνα 4 και 5 [03] [06] [08-10].



Εικόνα 4. Μοντέλα υπηρεσιών του Υπολογιστικού σύννεφου.

1.2.1 Software-as-a-Service (SaaS)

Οι πάροχοι υπηρεσιών δίνουν την δυνατότητα σε χρήστες και οργανισμούς να χρησιμοποιήσουν υπηρεσίες και εφαρμογές που εκτελούνται σε κάποια δομή Cloud, η οποία είναι διαθέσιμη μέσω διάφορων συσκευών εύκολα προσβάσιμων σε κάθε καταναλωτή, με απλή χρήση ενός web browser ή κάποιου άλλου προγράμματος [05].

Οι δομές αυτές αποτελούνται από το hardware αλλά και το λογισμικό στο οποίο τίθενται σε εφαρμογή τα πέντε βασικά χαρακτηριστικά του Cloud Computing. Οι δομές του Υπολογιστικού σύννεφου περιέχουν το φυσικό αλλά και το αφαιρετικό επίπεδο.

Το φυσικό επίπεδο, περιλαμβάνει όλο τον διαθέσιμο εξοπλισμό ο οποίος χρησιμοποιείται για να υποστηρίξει τις υπηρεσίες που παρέχονται μέσω του Υπολογιστικού Σύννεφου, όπως οι διακομιστές, ο αποθηκευτικός χώρος που χρειάζεται καθώς και οποιαδήποτε δομικά στοιχεία απαραίτητα για την σύνδεση στο διαδίκτυο. Παράλληλα, το αφαιρετικό επίπεδο συμπεριλαμβάνει το λογισμικό το οποίο αξιοποιεί το φυσικό επίπεδο [03].

Στο μοντέλο SaaS, ο χρήστης δεν είναι υποχρεωμένος να διαθέσει χρόνο ή πόρους για συντήρηση ή και αναβάθμιση, καθώς δεν είναι αυτός υπεύθυνος για την συγκεκριμένη πλατφόρμα, την εφαρμογή ή την υπηρεσία που χρησιμοποιεί.

Μερικά παραδείγματα παρόχων SaaS cloud αποτελούν οι IBM , Oracle, SalesForce, Microsoft και Cisco [09].

1.2.2 Platform-as-a-Service (PaaS)

Με το μοντέλο PaaS, δίνεται η δυνατότητα στον κάθε χρήστη να χρησιμοποιεί εφαρμογές, οι οποίες έχουν δημιουργηθεί μέσω γλωσσών προγραμματισμού, υπηρεσιών και εργαλείων διαθέσιμων από τον πάροχο υπηρεσιών Cloud. Πλατφόρμες οι οποίες χρησιμοποιούν το μοντέλο αυτό, περιέχουν τα εργαλεία τα οποία χρησιμοποιούνται για την δημιουργία, δοκιμή αλλα και χρήση εφαρμογών, υπηρεσιών και προγραμματιστικών περιβαλλόντων [05].

Το μοντέλο που βασίζεται το PaaS, δίνει την δυνατότητα να γίνεται πλήρης αξιοποίηση των υπολογιστικών πόρων ανάλογα με το κόστος της χρήσης του.

Ο καταναλωτής δεν μπορεί να ελέγξει ή να διαχειριστεί την υποδομή του Cloud η οποία περιλαμβάνει, όπως αναφέρθηκε, τα λειτουργικά συστήματα, τους διακομιστές, το δίκτυο και τον αποθηκευτικό χώρο αλλά μπορεί να έχει τον έλεγχο στην χρήση των εφαρμογών και πιθανώς στις ρυθμίσεις τους για το περιβάλλον στο οποίο χρησιμοποιούνται [03].

Κάποια παραδείγματα για το μοντέλο PaaS αποτελούν τα Google App Engine, Microsoft Azure και Heroku [06].

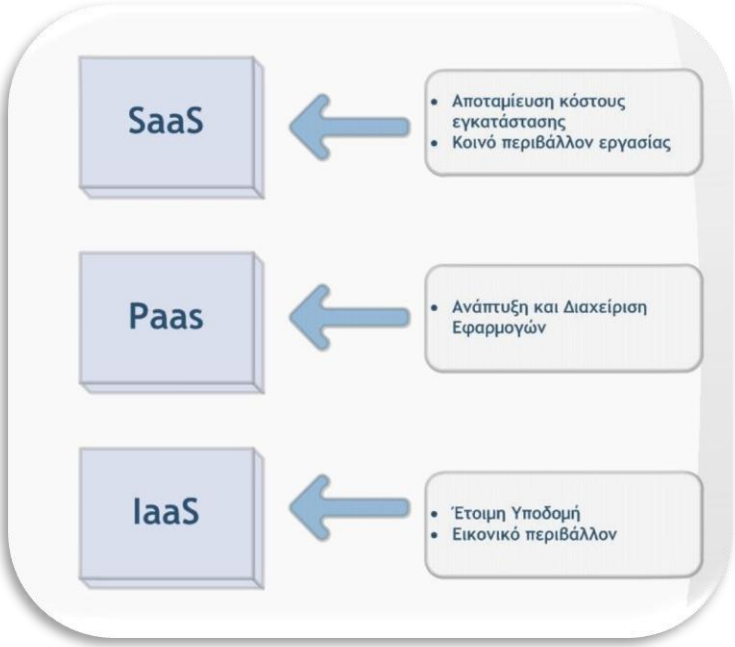
1.2.3 Infrastructure-as-a-Service (IaaS)

Ο καταναλωτής προμηθεύεται με αποθηκευτικό χώρο, δίκτυο και άλλους θεμελιώδεις υπολογιστικούς πόρους όπου, ο ίδιος έχει την δυνατότητα να χρησιμοποιήσει και να τρέξει εφαρμογές αλλά και λειτουργικά συστήματα. Το μεγαλύτερο πλεονέκτημα του IaaS είναι η μεταφορά εικονικών μηχανών από οποιοδήποτε οργανισμό ή και ιδιώτη στο Υπολογιστικό σύννεφο, με ελάχιστο κόπο και κατανάλωση πόρων.

Ο έλεγχος αλλά και η διαχείριση του βασικού φυσικού και εικονικού περιβάλλοντος του Cloud, το οποίο συμπεριλαμβάνει δίκτυο, διακομιστές και κάποια ήδη λειτουργικών συστημάτων γίνεται από τον πάροχο υπηρεσιών, χωρίς να λαμβάνει μέρος ο καταναλωτής.

Ο χρήστης έχει την δυνατότητα να ελέγξει και να χρησιμοποιήσει λειτουργικά συστήματα, αποθηκευτικό χώρο, συγκεκριμένες εφαρμογές και κάποια δομικά στοιχεία δικτύου σε μικρό βαθμό, όπως για παράδειγμα τα host firewalls.

Κάποια παραδείγματα Infrastructure-as-a-Service σαν υπηρεσίες μοντέλου Cloud αποτελούν η Amazon C2, Eucalyptus, Rackspace και Nimbus [06].



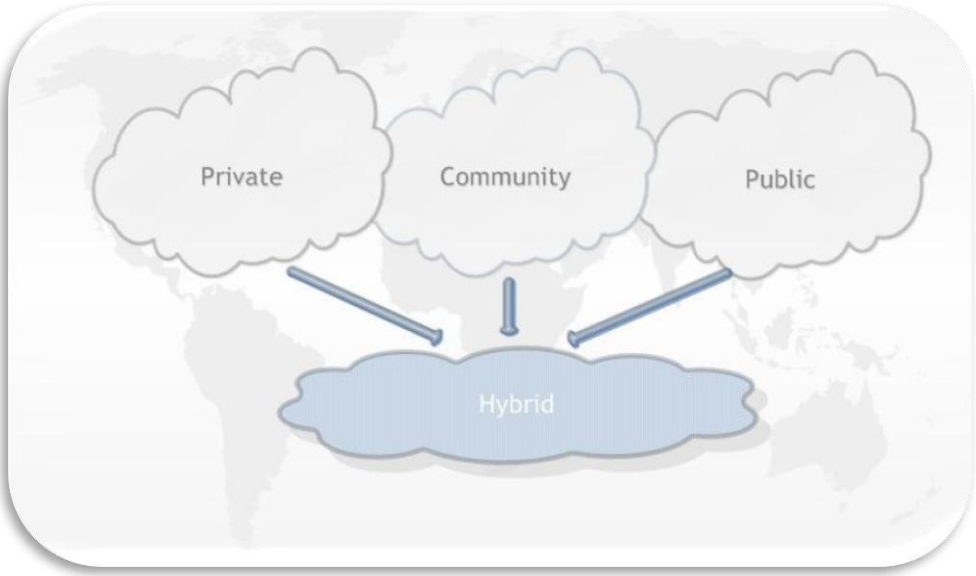
Εικόνα 5. Χαρακτηριστικά μοντέλων παροχής υπηρεσιών του Υπολογιστικού σύννεφου.

1.3 Μοντέλα ανάπτυξης του Υπολογιστικού σύννεφου

Οι υπηρεσίες που περιγράφηκαν μπορούν να χρησιμοποιηθούν σε ένα ή και περισσότερα μοντέλα ανάπτυξης του Υπολογιστικού σύννεφου, σύμφωνα με τον οργανισμό NIST. Κάθε μοντέλο έχει την δυνατότητα να μεταβάλει τον τρόπο σύνδεσης των συστημάτων ή τον τρόπο και μέγεθος της εργασίας που γίνεται σε κάθε οργανισμό.

Με την χρήση κάθε ενός από τα μοντέλα ανάπτυξης υπηρεσιών, υπάρχει η δυνατότητα βελτίωσης των εφαρμογών, πλατφόρμων, υποδομής και οποιονδήποτε άλλων πόρων και υπηρεσιών που χρησιμοποιούνται μέσα στο Cloud [09].

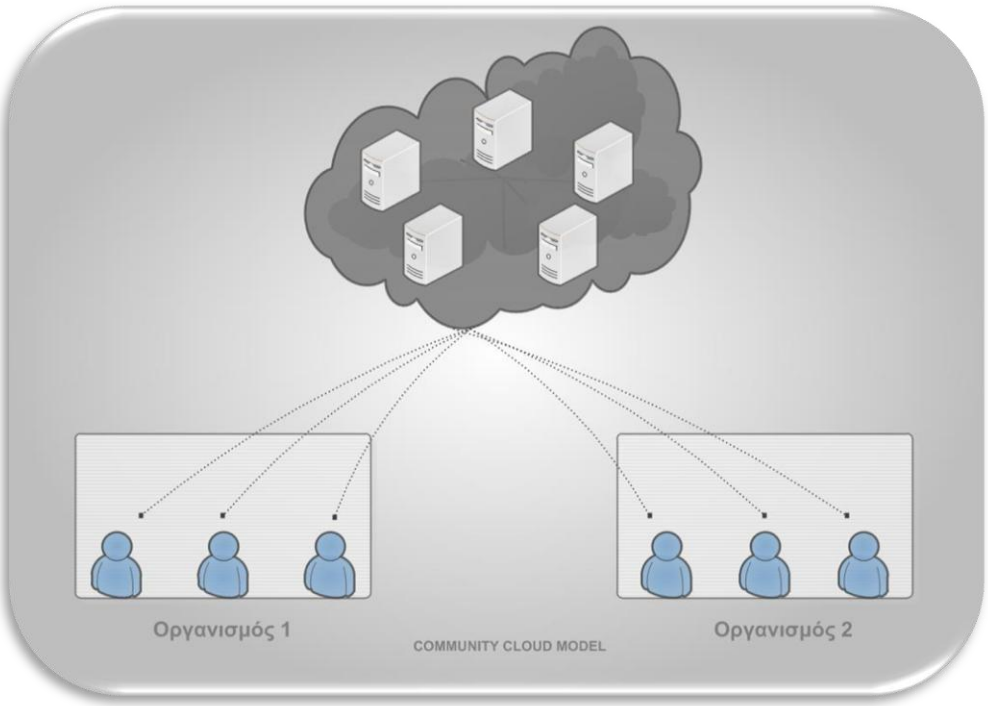
Σύμφωνα με τον οργανισμό NIST, τα τέσσερα μοντέλα ανάπτυξης υπηρεσιών που συνθέτουν το Υπολογιστικό σύννεφο είναι το Private Cloud, Public Cloud, Community και Hybrid Cloud [03] [10], όπως παρουσιάζεται και στην Εικόνα 6.



Εικόνα 6. Μοντέλα ανάπτυξης υπηρεσιών Υπολογιστικού σύννεφου.

1. Private Cloud. Το Private Cloud αποτελείται από την υποδομή Cloud που περιλαμβάνει ένα σύνολο υπολογιστικών πόρων, που προσφέρονται σε κάποιο συγκεκριμένο οργανισμό, ο οποίος αποτελείται από πολλαπλούς καταναλωτές. Οι πόροι αυτοί, προσφέρονται με συγκεκριμένο τρόπο ώστε να μπορούν σχεδιάζονται, να ελέγχονται και να ανήκουν στον συγκεκριμένο οργανισμό, κάποιο τρίτο οργανισμό ή και στους δύο ταυτόχρονα και μπορούν να υπάρχουν εντός ή και εκτός των εγκαταστάσεων του οργανισμού. Ένα σημαντικό μειονέκτημα του Private Cloud αποτελεί το υψηλό κόστος για την απόκτηση, λειτουργία αλλά και την συντήρησή του. Καθώς το μοντέλο αυτό εφαρμόζεται σε κάποιο ήδη υπάρχον data center, στα πλαίσια κάποιου οργανισμού, παρέχει ίσως μεγαλύτερη ασφάλεια στα ευαίσθητα προσωπικά δεδομένα. Ένα μικρό κομμάτι του Private Cloud αποτελεί το Virtualization, το οποίο βοηθά στην αναβάθμιση και βελτιστοποίηση της απόδοσης του hardware στα data centers κάθε οργανισμού.

2. Community Cloud. Το Community Cloud αποτελείται από την υποδομή Cloud που περιλαμβάνει ένα σύνολο υπολογιστικών πόρων, που διατίθενται για ιδιωτική χρήση από συγκεκριμένη ομάδα καταναλωτών, από οργανισμούς με κοινούς στόχους, ενδιαφέροντα και προβληματισμούς, όπως απαιτήσεις ασφάλειας και πολιτικές της εταιρίας, όπως φαίνεται στην Εικόνα 7. Μπορεί να ανήκει, να ελεγχθεί και να διαχειριστεί από τους ίδιους τους οργανισμούς, κάποιο τρίτο οργανισμό ή και από τους δύο ταυτόχρονα και μπορεί να υπάρχει εντός ή εκτός των εγκαταστάσεων του οργανισμού.



Εικόνα 7. Μοντέλο Community Cloud.

3. Public Cloud. Η υποδομή του Cloud, στο μοντέλο αυτό, παρέχεται για δημόσια και ανοικτή χρήση. Το σύνολο των πόρων που παρέχονται, διατίθενται μέσω του διαδικτύου και ανήκει, ελέγχεται και διαχειρίζεται από κάποια επιχείρηση, ακαδημαϊκό ή κυβερνητικό οργανισμό καθώς και μπορεί να υπάρχει μόνο στις εγκαταστάσεις του παρόχου Cloud. Το Public Cloud, χαρακτηρίζεται από αρκετά πλεονεκτήματα για τους καταναλωτές, όπως η ασφάλεια της διάθεσης των υπηρεσιών, η διαθεσιμότητα και η ευελιξία τους.

4. Hybrid Cloud. Η υποδομή του Cloud, στο μοντέλο Hybrid, είναι δομημένη από δύο ή και περισσότερα μοντέλα, όπως αναφέρθηκαν παραπάνω συνδυάζοντας τους πόρους που παρέχονται από κάθε ένα ξεχωριστά. Αν και διατηρούν, το κάθε ένα όλα τα

χαρακτηριστικά τους και παραμένουν ξεχωριστές οντότητες, ουσιαστικά είναι αλληλοεξαρτώμενα και δεμένα μεταξύ τους, με συγκεκριμένη τεχνολογία. Το Hybrid Cloud καθιστά δυνατή την φορητότητα των δεδομένων και των εφαρμογών. Καθώς το μοντέλο αυτό είναι συνδυαστικό, διαθέτει αρκετά πλεονεκτήματα και προσφέρει στους χρήστες ασφάλεια, ευελιξία, δυνατότητα επεκτασιμότητας και σημαντική μείωση του κόστους. Προσφέρει ασφάλεια, καθώς ως στοιχείο του υβριδικού μοντέλου, το Private Cloud, εκπληρώνει τις απαιτήσεις για ασφάλιση των ευαίσθητων δεδομένων καθώς και τις απαιτήσεις ασφάλειας της χρήσης του. Η ευελιξία των πόρων δίνει την δυνατότητα βελτίωσης και επεκτασιμότητας των οργανισμών και τέλος τα Public Clouds, ως στοιχείο του υβριδικού μοντέλου, παρέχουν εξοικονόμιση κόστους χρήσης και διαχείρισης των υπηρεσιών.

1.4 Υπολογιστικό σύννεφο και εξέλιξη

Η δημοτικότητα του Υπολογιστικού σύννεφου, είναι αρκετά υψηλή καθώς ο αριθμός των οργανισμών και εταιριών της Τεχνολογίας των Πληροφοριών (Information Technology- IT) που το χρησιμοποιεί, ολοένα και αυξάνεται. Η ευρεία χρήση του απορρέει από το πλήθος των διαφόρων υπηρεσιών που προσφέρονται, καθώς και από τα πολλά οφέλη που λαμβάνει ο κάθε καταναλωτής. Το Cloud, τα τελευταία χρόνια, έχει αποδεικτεί ως μία δημοφιλή περιοχή έρευνας σχεδιασμού αλλά και ανάπτυξης πολλών εφαρμογών καθώς και προσφέρει τεράστια αλλαγή, όσο αφορά τον τρόπο με τον οποίο οι υπηρεσίες παραδίδονται στους χρήστες.

Η ευρεία χρήση και εξέλιξή του αποτελεί γεγονός. Παρόλο το γεγονός, ότι αποτελεί σχετικά καινούργια έννοια στον χώρο της Τεχνολογίας των Πληροφοριών, και βρίσκεται στα αρχικά σχετικά στάδια της, οδηγεί σε μία νέα κατεύθυνση ανάπτυξης των παρεχόμενων υπηρεσιών [05].

Το Cloud Computing, πέρα από τα πολλά οφέλη χαρακτηρίζεται και από αρκετές αδυναμίες στην χρήση του ή ακόμα και στην ασφάλεια του. Η ανταγωνιστική φύση του αλλά και η πλέον ευρεία και διαδεδομένη χρήση του, θέτει ως πρωταρχικό στόχο την διαρκή βελτίωση των υπηρεσιών του.

Κάποιες προβλέψεις, όσο αφορά την εξέλιξη του Υπολογιστικού σύννεφου αποτελούν [11]:

1. Το Global Cloud Computing Market Forecast 2015-2020, περιμένει αύξηση της τάξεως του 30% του Compound Annual Growth Rate (CAGR), στην παγκόσμια αγορά του Υπολογιστικού σύννεφου. Έχοντας ως αποτέλεσμα, να φτάσει τα 270 δισσεκατομμύρια δολλάρια μέχρι το έτος 2020.

2. Μέχρι το έτος 2019, προβλέπεται ο παγκόσμιος ρυθμός data traffic από κινητά τηλέφωνα που αντιπροσωπεύονται μέσω εφαρμογών στο Cloud, να φτάσει στο 90%.

3. Ο όγκος εργασίας σε μοντέλα υπηρεσιών Software-as-a-Service, προβλέπεται να αυξηθεί στο ποσοστό του 59% μέχρι το έτος 2018, από το 41% που κατείχε το 2013.

Κεφάλαιο 2
Ασφάλεια στο Υπολογιστικό Σύννεφο

Το Υπολογιστικό σύννεφο, όπως έχει αναφερθεί, αποτελείται από μεγάλης κλίμακας διαμοιρασμένη υποδομή, η οποία παραδίδει στους χρήστες τεράστιο πλήθος καθώς και δυναμικά επεκτάσιμους πόρους. Οι πόροι αυτοί αποτελούν τον αποθηκευτικό χώρο, τις πλατφόρμες χρήσης καθώς και όλες τις διαθέσιμες δικτυακές εφαρμογές και υπηρεσίες [12].

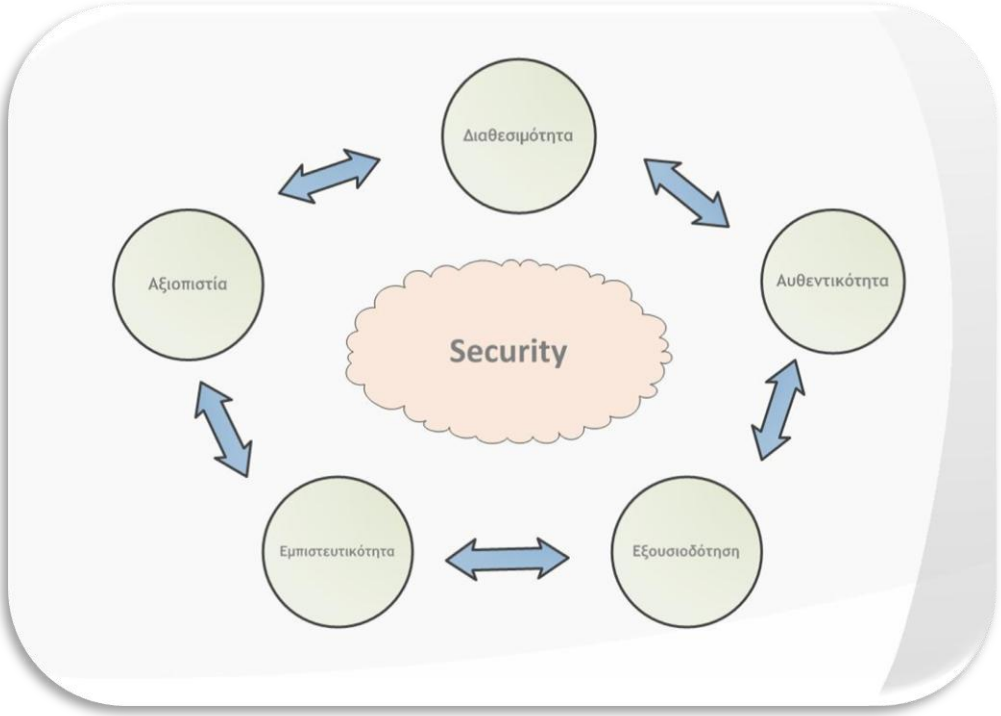
Ανεξάρτητα από τα πολλά οφέλη που το χαρακτηρίζουν, η ύπαρξη απειλών και ζητημάτων ασφάλειας είναι ιδιαίτερα αισθητή. Αυτό αποτελεί κυρίως αποτέλεσμα της εξάρτησης της λειτουργίας του από το διαδίκτυο.

Στην περίπτωση που κάποιος οργανισμός ή εταιρία αποφασίσει την χρήση του Cloud, όλα τα ευαίσθητα και σημαντικά δεδομένα καθώς και η διαχείριση και η ευθύνη για την ασφάλειά τους, αποτελεί λειτουργία του πάροχου υπηρεσιών. Συνεπώς, είναι ιδιαίτερη σημαντική η εμπιστοσύνη μεταξύ των πάροχων υπηρεσιών Cloud με τον κάθε οργανισμό που κάνει χρήση των υπηρεσιών τους. Ειναι απαραίτητος λοιπόν, ο έλεγχος και η ύπαρξη στρατηγικών για εξασφάλιση της ασφάλειας, απο μεριάς του κάθε πάροχου πριν την απόφαση για χρήση του Cloud [11].

Σύμφωνα με την έρευνα IDC Asia/Pacific Cloud Survey, που έλαβε μέρος το 2009, ο βασικός προβληματισμός στο περιβάλλον του Υπολογιστικού σύννεφου αποτελεί το ζήτημα της ασφάλειας [12].

Ένα σημαντικό παράδειγμα παραβίασης της ασφάλειας σε πλατφόρμες Υπολογιστικού σύννεφου τα τελευταία χρόνια αποτελεί η διαρροή μεγάλου αριθμού δεδομένων στους χρήστες, από την Google τον Μάρτιο του 2009. Επίσης, τραντακτά παραδείγματα αποτελούν η παύση λειτουργίας της πλατφόρμας Microsoft Azure για 22 ώρες καθώς και οι διακοπές της λειτουργίας της Amazon EC2, τον Απρίλιο του 2011 [13]. Αυτές, αν και αποτελούν μεμονωμένες περιπτώσεις παραβίασης της ασφάλειας και προβλημάτων των πλατφόρμων Υπολογιστικού σύννεφου δείχνουν την σοβαρότητα και την ανάγκη για εύρεση λύσεων για βελτιστοποίηση των υπηρεσιών Cloud.

Η ασφάλεια των υπολογιστών αποτελείται από τις υπηρεσίες που παρέχονται σε κάποιο αυτοματοποιημένο πληροφοριακό σύστημα προκειμένου να προφυλαχθούν οι αρχές διατήρησης της ασφάλειας, που αποτελούν την αξιοπιστία, την διαθεσιμότητα, την αυθεντικότητα, την εξουσιοδότηση καθώς και την εμπιστευτικότητα των πληροφοριών και δεδομένων όπως φαίνεται και στην Εικόνα 8.



Εικόνα 8. Αρχές ασφάλειας Υπολογιστών.

Οι περισσότεροι προβληματισμοί για ζητήματα ασφάλειας στο Υπολογιστικό σύννεφο, αποτελούν τα αποτελέσματα από την έλλεψη φυσικής δομής του χρήστη ή του οργανισμού καθώς δεν μπορούν να γνωρίζουν την ακριβή τοποθεσία αποθήκευσης των δεδομένων τους. Επίσης σημαντικά ζητήματα δημιουργούνται από την έλλειψη ασφάλειας στα προγράμματα περιήγησης αλλά και πολλά άλλα που θα αναφερθούν αργότερα στα πλαίσια της διατριβής.

Εμφανίζεται λοιπόν, η ανάγκη για ύπαρξη συγκεκριμένων προτύπων για την αύξηση της ασφάλειας και της διαλειτουργικότητας των πλατφόρμων Cloud. Παρόλο το γεγονός ότι τα πρότυπα αυτά βρίσκονται σε πρώιμο στάδιο, η γρήγορη ανάπτυξη τους αποτελεί γεγονός [13].

Κάποιοι παγκόσμιοι οργανισμοί, ήδη έχουν αναπτύξει πρότυπα, οδηγίες και διαδικασίες ασφάλειας και λειτουργικότητας του Υπολογιστικού σύννεφου με τους σπουδαιότερους να αποτελούν οι [11]:

1. National Institute of Standards and Technology (NIST).
2. Cloud Standards Customer Council (CSCC).
3. The European Telecommunications Standards Institute (ETSI).
4. Distributed Management Task Force (DMTF).
5. European Union Agency for Network and Information Security (ENISA).
6. Global Inter—Cloud Technology Forum (GICF).
7. Association for Retail Technology Standards (ARTS).
8. International Telecommunications Union (ITU).
9. Open Cloud Consortium (OCC).
10. Storage Networking Industry Association (SNIA).
11. Object Management Group (OMG).

12. Organization for the Advancement of Structured Information Standards (OASIS).

13. Open Grid Forum (OGF).

14. Enterprise Cloud Leadership Council (ECLC).

2.1 Ευπάθειες εξειδικευμένες στο Υπολογιστικό σύννεφο

Στην ασφάλεια των υπολογιστών, ευπάθεια αποτελεί μία αδυναμία ή ελάττωμα στο υπολογιστικό σύστημα που επιτρέπει σε κάποιον πιθανό κακόβουλο χρήστη να την εκμεταλλευθεί και έτσι να καταφέρει να παραβιάσει κάποια από τις βασικές αρχές ασφάλειας, που αναφέρθηκαν παραπάνω.

Όσο αφορά το Cloud Computing, κάποια ευπάθεια είναι εξειδικευμένη στο Υπολογιστικό σύννεφο όταν ικανοποιούνται συγκεκριμένες προυποθέσεις όπως [14]:

1. Παρατηρείται συχνά σε κάποια από τις βασικές τεχνολογίες του Υπολογιστικού σύννεφου.

2. Αναφέρεται σε ένα ή και περισσότερα από τα χαρακτηριστικά του Υπολογιστικού σύννεφου που έχουν αναπτυχθεί, σύμφωνα με τον οργανισμό NIST.

3. Δημιουργεί όλο και περισσότερα προβλήματα στην υλοποίηση των καινοτομιών καθώς και στους ελέγχους ασφάλειας από τους πάροχους υπηρεσιών.

4. Είναι κυρίαρχη στις καθιερωμένες προσφορές υπηρεσιών Cloud.

Κάποιος πιθανός κακόβουλος χρήστης, με την εκμετάλλευση κάποιας εξειδικευμένης ευπάθειας στο Υπολογιστικό σύννεφο, μπορεί να ξεκινήσει επίθεση με πολύ σημαντικές και επικίνδυνες συνέπειες στο περιβάλλον λειτουργίας. Κάποια χαρακτηριστικά που μπορεί να εκμεταλλευτεί, όπως έχει αναφερθεί αποτελούν τα εξής [14] [15]:

1. Κατ'απαίτηση εξυπηρέτηση.

2. Ευρεία σύνδεση στο διαδίκτυο.

3. Εύκολη πρόσβαση σε ομάδες υπολογιστικών πόρων.

4. Ραγδαία ελαστικότητα.

5. Οριοθετημένες διαθέσιμες υπηρεσίες.

Κάθε περιβάλλον Υπολογιστικού σύννεφου θα πρέπει να διαθέτει συγκεκριμένα χαρακτηριστικά ώστε να θεωρηθεί ασφαλές περιβάλλον εργασίας και χρήσης. Είναι απαραίτητη η διαφύλαξη της αξιοπιστίας, της διαθεσιμότητας, αυθεντικότητας , εξουσιοδότησης καθώς και της εμπιστευτικότητας των πληροφοριών και δεδομένων. Οι πληροφορίες κάθε οργανισμού όχι μόνο αποτελούν ανταγωνιστικό προσόν, αλλά αρκετές φορές περιέχουν ευαίσθητες πληροφορίες για πελάτες αλλά και εργαζόμενους κάνοντας έτσι την ανάγκη για προστασία τους κρίσιμη [16].

Για κάθε οργανισμό, η διαδικασία ασφάλισης των δεδομένων αποτελεί οικονομική επένδυση καθώς και διασφαλίζει τον περιορισμό των δαπανών που χρησιμοποιούνται για επιδιόρθωση λαθών σε περιπτώσεις παραβίασης του συστήματος [17]. Το προσωπικό υπεύθυνο για την ασφάλεια, πρέπει να είναι εκπαιδευμένο ειδικά ώστε να μπορεί να εντοπίσει επιθέσεις αποκλειστικά στοχευμένες στο Υπολογιστικό σύννεφο. Η ευθύνη της προστασίας των υπολογιστικών συστημάτων πρέπει να ανατεθεί σε άτομο με μεγάλη εμπειρία και εξειδίκευση στο τομέα της ασφάλειας. Το μεγαλύτερο προσόν που θα πρέπει να διαθέτει είναι η ικανότητα να σχεδιάζει, να ρυθμίζει αλλά και να μπορεί να εισέρχεται επιτυχώς σε οποιοδήποτε σύστημα παραβιάζοντας την ασφάλειά του [10].

Καθώς κάθε χρήστης είναι υποχρεωμένος να κρυπτογραφήσει τα δεδομένα του πριν κάνει οποιαδήποτε διαδικασία αποθήκευσής τους στο Cloud, οι πάροχοι υπηρεσιών Cloud θα πρέπει να διαχειριστούν όλες τις διαδικασίες ώστε η διαδικασία κρυπτογράφησης-αποκρυπτογράφησης να απλοποιηθεί όσο το δυνατόν περισσότερο.

Στις πλατφόρμες Υπολογιστικού σύννεφου, όλα τα αποθηκευμένα δεδομένα βρίσκονται σε data centers που χωρίς την ύπαρξη του Cloud θα βρίσκονταν στους ιδιωτικούς υπολογιστές του ιδιώτη ή κάποιου άλλου είδους συσκευές. Το χαρακτηριστικό αυτό κάνει ιδιαίτερα σημαντική την διαδικασία ασφάλειας για τα προσωπικά δεδομένα του κάθε χρήστη ή οργανισμού.

Στα δημόσια Cloud, η ανάγκη για μέτρα προστασίας αποτελεί ανάγκη για την διασφάλιση της αυθεντικότητας των δεδομένων αλλα και της σωστής εξουσιοδότησης. Στα περιβάλλοντα Private Cloud, υπάρχει η δυνατότητα χειρισμού και διαχείρισης χρηστών που χρησιμοποιούν λανθασμένα στοιχεία εισόδου με σκοπό την είσοδο τους σε συστήματα. Στις περιπτώσεις πολλαπλών υπηρεσιών Υπολογιστικού σύννεφου, απαραίτητη προυπόθεση αποτελεί η διαδικασία του single sign-on [16].

2.2 Ζητήματα ασφάλειας στο Υπολογιστικό σύννεφο

Αρκετές φορές κάποια από περιστατικά που αναφέρονται ως περιστατικά ασφάλειας, αποτελούν διαδεδομένα και κλασικά προβλήματα διαδικτυακών εφαρμογών. Η ασφάλεια στο Υπολογιστικό σύννεφο, αν και βασίζεται στις βασικές αρχές της ασφάλειας των υπολογιστών, απειλείται από διαφορετικού είδους απειλές και χρίζει μεγάλης προσοχής [18].

Μερικά από τα πιο σημαντικά ζητήματα ασφάλειας που μπορούν να συναντηθούν σε περιβάλλοντα Υπολογιστικού σύννεφου αποτελούν, όπως φαίνεται και στην Εικόνα 9, τα εξής [02] [11] [19]:

Εικόνα 9. Ζητήματα ασφάλειας στο Υπολογιστικό σύννεφο.

1. Έλεγχος πρόσβασης. Όλα τα ευαίσθητα δεδομένα και πληροφορίες που επεξεργάζονται εκτός του οργανισμού ή του χώρου του ιδιώτη παρουσιάζουν μεγάλο ρίσκο στην διασφάλιση της ασφάλειας τους. Κάποιοι εξωτερικοί χρήστες ή ακόμα και υπηρεσίες μπορούν να παρακάμψουν όλους τους φυσικούς και λογικούς ελέγχους ώστε να παραβιάσουν το σύστημα.

2. Ανάκτηση δεδομένων. Καθώς τα δεδομένα δεν βρίσκονται αποθηκευμένα στις εγκαταστάσεις του οργανισμού ή του χρήστη, η ύπαρξη τους αλλά και η διαθεσιμότητα τους σε περίπτωση καταστροφής, αμφισβητείται. Θεωρείται λοιπόν, υποχρέωση του κάθε παρόχου να παρέχει στρατηγικές ανάκτησης και διαφύλαξης των δεδομένων σε περίπτωση οποιουδήποτε κινδύνου.

3. Ασφάλεια των δεδομένων. Η ασφάλεια των δεδομένων αφορά τις βασικές αρχές διασφάλισης των δεδομένων και των πληροφοριών. Η αξιοπιστία, εμπιστευτικότητα και διαθεσιμότητα των δεδομένων μπορεί να αποτελέσει σημαντικό ζήτημα όσο αφορά την ασφάλεια. Αποτελεί ευθύνη κάθε παρόχου αλλά και κάθε χρήστη ξεχωριστά, να διασφαλίσει την προστασία των αποθηκευμένων δεδομένων από παραβιάσεις ασφάλειας, λόγω ευπαθειών σε υπηρεσίες ή εφαρμογές ή ακόμα και από επιθέσεις κακόβουλων χρηστών.

4. Συμμόρφωση χρηστών στις καθορισμένες ρυθμίσεις. Αποτελεί υποχρέωση των πελατών να ασφαλίζουν και να κρυπτογραφούν τα δικά τους δεδομένα και πληροφορίες, ακόμα και αν είναι αποθηκευμένα σε κάποιο data center που βρίσκεται στην δικαιοδοσία του παρόχου υπηρεσιών Cloud.

5. Τοποθεσία των δεδομένων. Οι πάροχοι υπηρεσιών Υπολογιστικού σύννεφου πρέπει να εξασφαλίζουν την ασφάλεια των δεδομένων καθώς οι ίδιοι οι πελάτες δεν μπορούν να γνωρίζουν την ακριβή φυσική τοποθεσία τους. Οι οργανισμοί από την μεριά τους, θα πρέπει να είναι ενημερωμένοι για τους κανονισμούς και νόμους που ισχύουν, πριν αποφασίσουν να μεταφέρουν τις υπηρεσίες τους στο Cloud.

6. Ανασφαλή Interfaces και API (Application Programming Interfaces). Η λειτουργία, διαχείριση, ο έλεγχος και η ρύθμιση των υπηρεσιών παρέχονται στον καταναλωτή με την μορφή Software Interfaces και Application Programming Interfaces. Αυτά αποτελούν την

βάση για την διαχείριση της ασφάλειας των παρόχων, οπότε το οποιοδήποτε πρόβλημα σε αυτά δημιουργεί ζητήματα ασφάλειας.

7. Ζητήματα κοινόχρηστων τεχνολογιών. Οι υπηρεσίες που διαμοιράζονται μεταξύ χρηστών, αποτελεί ένα από τα μεγαλύτερα πλεονεκτήματα χρήσης του Cloud αλλά και ταυτόχρονα ένα από τα κυριότερα ζητήματα εγγύησης της ασφάλειας των πληροφοριών.

2.3 Γνωστές Επιθέσεις

Πολλές από τις πιο γνωστές και σημαντικές επιθέσεις σε περιβάλλοντα Υπολογιστικού σύννεφου αποτελούν επιθέσεις που προυπήρχαν σε περιβάλλοντα μη χρήσης του Cloud. Ο συνδυασμός των πρόσφατων τεχνολογιών, όπως το διαδίκτυο και το "virtualization" που συνιστούν, μαζί με άλλες υπηρεσίες και εφαρμογές του Cloud, οδηγούν στο γεγονός ότι κάθε είδους ευπάθεια που μπορεί να υπάρξει σε αυτές τις τεχνολογίες αποτελεί απειλή σε περιβάλλοντα χρήσης ή μη του Υπολογιστικού σύννεφου [15].

Μπορούν να παρατηρηθούν, βέβαια συγκεκριμένες επιθέσεις που είναι δυνατόν να συμβούν κατά κύριο λόγο σε περιβάλλοντα χρήσης του Υπολογιστικού σύννεφου.

Κάποιες από τις πιο συχνές επιθέσεις σε Cloud, αποτελούν [15] :

1. Distributed Denial of Service Attack (DDos). Η DDos επίθεση είναι η σκόπιμη πράξη κάπου κακόβουλου χρήστη, που έχει σκοπό την υποβάθμιση της ποιότητας και της διαθεσιμότητας των υπηρεσιών που προσφέρονται από κάποιο πληροφοριακό σύστημα. Η διαδικασία της επίθεσης αυτής, συμπεριλαμβάνει την κατανάλωση του bandwidth και του επεξεργαστικού χρόνου [20] του στόχου. Σε μία DDos επίθεση, ο κακόβουλος χρήστης εκμεταλλεύεται πλήθος μηχανών που ονομάζονται bots, με σκοπό την παρεμπόδιση ενός υπολογιστή ή δικτύου να παρέχει υπηρεσίες, μπλοκάροντας την είσοδο σε αυτές. Με την επίθεση αυτή αναλώνονται όλοι οι υπολογιστικοί πόροι του "θύματος" όπως το bandwidth, η μνήμη και το δίκτυο. Η επιτυχία μίας DDos επίθεσης, εξαρτάται από το τύπο και όγκο του traffic στην διάρκεια της επίθεσης καθώς και από την επεξεργαστική ισχύ του υπολογιστή του στόχου της επίθεσης [20]. Οι συγκεκριμένες επιθέσεις μπορούν να στοχοποιηθούν συγκεκριμένα σε μηχανές Cloud, καθώς κάποιος κακόβουλος χρήστης μπορεί να εκμεταλλευθεί εικονικές μηχανές ως εσωτερικά bots με

σκοπό την παρεμπόδιση των υπηρεσιών. Η προστασία των υπηρεσιών Cloud ενάντια σε τέτοιου είδους επιθέσεις γίνεται με την χρήση Intrusion Detection Systems (IDSs) [21]. Για την προστασία των χρηστών ενάντια σε τέτοιες επιθέσεις το Computer Emergency Response Team Coordination Center (CERT/CC), δημοσίευσε το "Home Network Security" τον Ιούλιο του 2001 [20].

2. VM Denial of Service Attacks (VM Dos). Η επίθεση VM Denial of Service, προκύπτει όταν κάποιος χρήστης, που είναι ιδιοκτήτης ενός εικονικού μηχανήματος, εκμεταλλεύεται μία ευπάθεια με απώτερο σκοπό να καταναλώσει όσο το δυνατόν περισσότερους υπολογιστικούς πόρους, όπως και η DDos επίθεση που αναφέρθηκε παραπάνω, στο φυσικό μηχάνημα στο οποίο λειτουργεί το εικονικό μηχάνημα (Virtual Machine-VM). Η συγκεκριμένη επίθεση μπορεί να λάβει μέρος σε οποιοδήποτε περιβάλλον το οποίο χρησιμοποιεί την τεχνολογία της "εικονικοποίησης" (virtualization). Μετά την εύρεση ενός κακόβουλου VM, που αποτελεί σχετικά απλή διαδικασία, μία από τις τεχνικές που ακολουθούνται για την αποτροπή επόμενης Denial of Service επίθεσης σε κάποιο από τα άλλα εικονικά μηχανήματα που ίσως διαθέτονται στο φυσικό μηχάνημα, είναι η επανεκκίνηση του κακόβουλου VM.

3. Keystroke Timing Attacks. Τέτοιου είδους επιθέσεις λαμβάνουν μέρος, όταν κάποιος χρήστης προσπαθεί να υποκλέψει απόρρητες πληροφορίες του "θύματος" όπως για παράδειγμα κωδικούς πρόσβασης, με παρατήρηση του τρόπου πληκτρολόγησής του. Οι πληροφορίες που μπορεί να λαμβάνονται από την πληκτρολόγηση του χρήστη μπορεί να δίνουν πληροφορίες για την αλληλουχία των πλήκτρων που χρησιμοποιούνται. Έτσι ο κακόβουλος χρήστης μετράει την χρονική διάρκεια μεταξύ συνεχόμενων πληκτρολόγησεων κατά την διάρκεια που ίσως το πιθανό "θύμα", πληκτρολογεί κάποιον κωδικό πρόσβασης [19]. Στα περιβάλλοντα Cloud η διαδικασία της συγκεκριμένης επίθεσης παραμένει η ίδια. Σε περίπτωση που η επίθεση γίνεται στον ίδιο χώρο με το πιθανό στόχο υπάρχει η δυνατότητα να λάβει μέρος και σε πραγματικό χρόνο, με πολύ πιο επικίνδυνα και σοβαρά αποτελέσματα. Σε περιβάλλοντα Υπολογιστικού σύννεφου, πέρα από την αποφυγή ύπαρξης στον ίδιο χώρο μεταξύ κακόβουλου χρήστη και στόχου, δεν υπάρχουν άλλα γνωστά αντίμετρα αυτής της επίθεσης.

4. Side-Channel Attacks. Τα περιβάλλοντα Cloud, δίνουν την δυνατότητα λειτουργίας πολλαπλών εικονικών μηχανημάτων ταυτόχρονα στο ίδιο το φυσικό μηχάνημα. Η πιθανότητα κάποιος χρήστης να βρίσκεται στον ίδιο διακομιστή με κάποιον πιθανό

κακόβουλο χρήστη είναι μεγάλη, επιτρέποντας τον επιτιθέμενο να εισχωρήσει στο εικονικό μηχάνημα του στόχου παραβιάζοντας έτσι την ασφάλεια του. Τέτοιου είδους επιθέσεις απαρτίζονται από δύο βήματα, την τοποθέτηση του κακόβουλου μηχανήματος και την εξαγωγή των πληροφοριών. Μόλις ο επιτιθέμενος τοποθετήσει το κακόβουλο μηχάνημά του στο φυσικό μηχάνημα του στόχου τότε μπορεί να εξάγει και να υποκλέψει πληροφορίες για αυτόν μέσω Cross-VM επιθέσεων. Ένα παράδειγμα Cross-VM επιθέσεων αποτελεί, η διαρροή πληροφοριών λόγω του διαμοιρασμού των πόρων, όπως για παράδειγμα δεδομένων από την CPU cache. Η Side-Channel κρυπτανάλυση αποτελεί αρκετά πιο εξειδικευμένη διαδικασία και αρκετές φορές αρκετά πιο ισχυρή από την κλασική κρυπτανάλυση [22].

5. Hypervisor Attacks. Ο Hypervisor (επόπτης) αποτελείται από το λογισμικό και το hardware το οποίο είναι υπεύθυνο για την δημιουργία και υλοποίηση των εικονικών μηχανημάτων. Σύμφωνα με την Hypervisor επίθεση, ο διαχειριστής του Υπολογιστικού σύννεφου που διαθέτει εξουσιοδοτημένη πρόσβαση στον Hypervisor, μπορεί να εισχωρήσει στο εικονικό μηχάνημα του χρήστη ακόμα και χωρίς να διαθέτει εξουσιοδότηση για είσοδο στο συγκεκριμένο μηχάνημα.

6. Cloud Malware Injection Attacks. Στις επιθέσεις Cloud Malware Injection, ο επιτιθέμενος προσπαθεί να εισχωρήσει κακόβουλο εικονικό μηχάνημα σε κάποιο περιβάλλον Cloud, με απώτερο σκοπό να επιτεθεί σε μηχανήματα μέσα σε αυτό [23]. Για να θεωρηθεί η επίθεση επιτυχημένη, θα πρέπει το κακόβουλο μηχάνημα να είναι έτσι σχεδιασμένο ώστε να θεωρεί από το περιβάλλον ως έγκυρο μηχάνημα [24].

7. Fraudulent Resource Consumption Attacks. Στην συγκεκριμένη επίθεση σε περιβάλλοντα Cloud, ο βασικός στόχος του επιτιθέμενου είναι η εκμετάλλευση ευπαθειών στο οικονομικό μοντέλο του περιβάλλοντος αυτού. Η διαδικασία της επίθεσης έχει αρκετές ομοιότητες με την Denial of Service επίθεση. Ο σκοπός του κακόβουλου χρήστη αποτελείται από την στέρηση των μακροχρόνιων οικονομικών προνομίων του στόχου, καταναλώνοντας τους πόρους του χρήστη. Η βασική διαφορά των δύο αυτών επιθέσεων, δηλαδή της DDos και της Fraudulent Resource Consumption (FRC), είναι ότι η FRC επίθεση στοχεύει στην οικονομική αστάθεια των πόρων του Cloud του "θύματος", ενώ η DDos αποσκοπεί στην κατανάλωση μεγάλου μέρους των πόρων του Υπολογιστικού σύννεφου. Η ανίχνευση μίας FRC επίθεσης μπορεί να αποδεικτεί δύσκολη, διότι η διαδικασία της επίθεσης (απαιτήσεις δικτυακών πόρων), μπορεί να

θεωρηθεί ως πράξη αποδεκτή, όπως αυτή οποιουδήποτε άλλου χρήστη, με την διαφορά της ύπαρξης της κακόβουλης πρόθεσης του επιτιθέμενου [24].

8. Phishing. Η επίθεση Phising αποτελεί ένα είδος επίθεσης υποκλοπής ευαίσθητων και απόρρητων πληροφοριών μέσω τεχνικών Social Engineering. Κοινή τακτική αποτελεί η διαδικασία αποστολής συνδέσμων ιστοσελίδων ή ακόμα και επισυναπτόμενων αρχείων μολυσμένων με κακόβουλο λογισμικό ή ευπαθειών, μέσω email ή μηνυμάτων. Οι συγκεκριμένες επιθέσεις μπορούν να λάβουν μέρος σε ιστοσελίδες παρόχων Υπολογιστικού σύννεφου χρησιμοποιώντας τις υπηρεσίες του Cloud και της τεχνικής του Social Engineering [25].

9. Ransomware. Η συγκεκριμένη επίθεση, επιτρέπει στον επιτιθέμενο να λάβει τον έλεγχο κάποιων δεδομένων και εφαρμογών ή ακόμα και ολόκληρου του μηχανήματος του στόχου. Από την μεριά του περιβάλλοντος του Υπολογιστικού σύννεφου, εφόσον ο χρήστης αποθηκεύσει τα αρχεία του σε κάποιον φάκελο στο Cloud, σε περίπτωση που πέσει θύμα τέτοιου είδους επίθεσης, υπάρχει η πιθανότητα να χάσει το μεγαλύτερο μέρος ή ακόμα και όλα τα αποθηκευμένα δεδομένα του [25].

Κεφάλαιο 3
Μεθοδολογία

Οι απειλές ασφάλειας, που αφορούν την διαχείριση των ευαίσθητων και απόρρητων δεδομένων καθώς και των ευπαθειών που μπορεί να παρατηρηθούν σε κάποιο εικονικό περιβάλλον και στην ασφάλεια δικτύου, αποτελούν κάποιες από τις προκλήσεις που αντιμετωπίζουν χρήστες σε περιβάλλοντα Υπολογιστικού σύννεφου ή μη.

Αποτελεί βασική ανάγκη, για την ασφάλεια των δεδομένων και πληροφοριών του κάθε χρήστη ξεχωριστά αλλά και κάθε οργανισμού ή εταιρίας που χρησιμοποιεί περιβάλλοντα Cloud Computing, η εξασφάλιση της ασφάλειας από τον κάθε πάροχο αλλά και από τον ίδιο τον οργανισμό ή χρήστη.

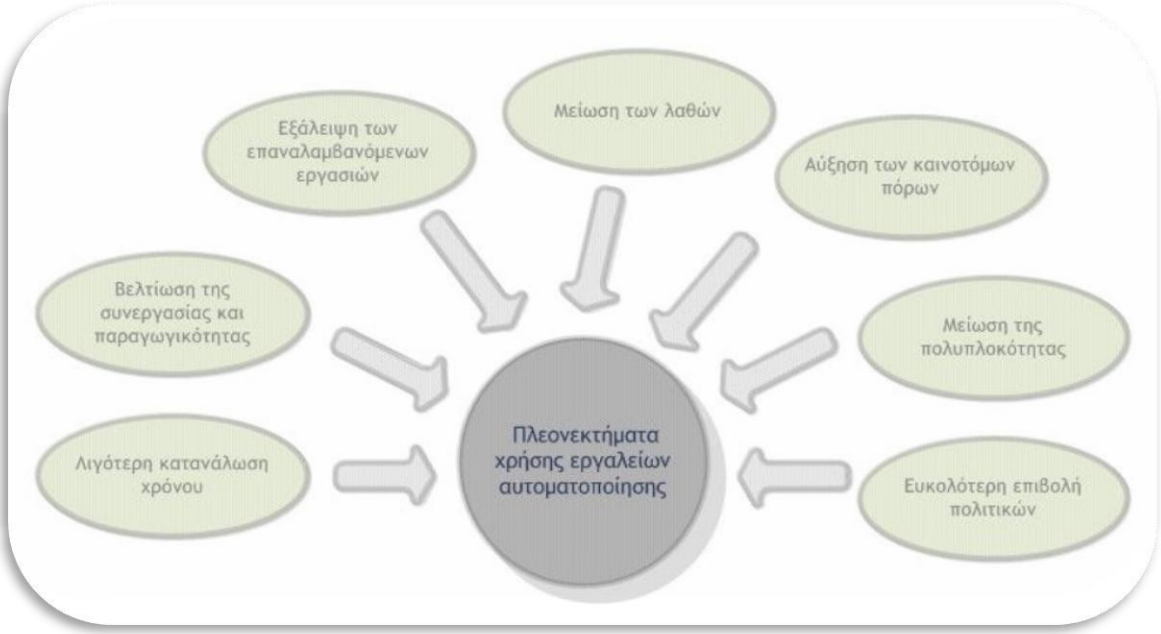
Κάθε περιβάλλον Υπολογιστικού σύννεφου θα πρέπει να διαθέτει συγκεκριμένα χαρακτηριστικά ώστε να θεωρηθεί ασφαλές περιβάλλον εργασίας και χρήσης. Είναι απαραίτητη η διαφύλαξη της αξιοπιστίας, της διαθεσιμότητας, αυθεντικότητας , εξουσιοδότησης καθώς και της εμπιστευτικότητας των πληροφοριών και δεδομένων.

Στην συνέχεια της διατριβής, θα παρουσιαστούν τρόποι εγγύησης της ασφάλειας ενός περιβάλλοντος Υπολογιστικού σύννεφου με την χρήση εργαλείων αυτοματοποίησης. Η μεθοδολογία που ακολουθείται γίνεται μέσω της χρήσης ενός εικονικού περιβάλλοντος. Με την χρήση εργαλείων αυτοματοποίησης, ακολουθείται μια συγκεκριμένη μεθοδολογία ώστε οι

απομακρυσμένοι εξυπηρετητές να διαμορφωθούν κατάλληλα, μέσα στο Υπολογιστικό σύννεφο και τελικά να ασφαλιστούν.

3.1 Εργαλεία Αυτοματοποίησης

Η χρήση της διαδικασίας της αυτοματοποίησης συμπεριλαμβάνει όλες τις τεχνικές με τις οποίες οι υπηρεσίες διαθέτονται αυτόματα από το υπολογιστικό σύστημα χωρίς την συμβολή του χρήστη ή οργανισμού. Η μεθοδολογία που ακολουθείται στην συγκεκριμένη διατριβή, αποτελείται από την χρήση εργαλείων αυτοματοποίησης για την δημιουργία ενός εικονικού περιβάλλοντος Υπολογιστικού σύννεφου καθώς και για την ρύθμιση και ασφάλιση των απομακρυσμένων χρηστών που συγκροτούν το συγκεκριμένο περιβάλλον. Μερικά από τα πολλά οφέλη της χρήσης εργαλείων αυτοματοποίησης, όπως φαίνεται και στην Εικόνα 10, αποτελούν τα εξής:



Εικόνα 10. Πλεονεκτήματα χρήσης εργαλείων αυτοματοποίησης.

1. Λιγότερη κατανάλωση χρόνου από την μεριά του κάθε χρήστη αλλά και οργανισμού.

2. Βελτίωση της συνεργασίας και της παραγωγικότητας μεταξύ των μελών που χρησιμοποιούν πλατφόρμες Υπολογιστικού σύννεφου, που έχουν ρυθμιστεί και διαχειριστεί μέσω εργαλειών αυτοματοποίησης.

3. Εξάλειψη των πιθανών επαναλαμβανόμενων διαδικασιών.

4. Μείωση των λαθών.

5. Μείωση της πολυπλοκότητας των διαδικασιών.

6. Αύξηση των καινοτόμων πόρων.

7. Ευκολότερη επιβολή των διάφορων πολιτικών οργανισμών ή εταιριών.

3.1.1 Vagrant by HashiCorp

Για την διαδικασία της δημιουργίας ενός Εικονικού περιβάλλοντος Υπολογιστικού σύννεφου, είναι αναγκαία η χρήση του κατάλληλου εργαλείου. Υπάρχουν αρκετές επιλογές ανοιχτού κώδικα, που μπορούν να χρησιμοποιηθούν για την δημιουργία εικονικών περιβάλλοντων, όπως για παράδειγμα το Docker, αλλά το βασικό ενδιαφέρον της συγκεκριμένης διατριβής αποτελεί το Vagrant της HashiCorp (https://www.vagrantup.com/).

Το Vagrant αποτελεί εργαλείο που χρησιμοποιείται για την δημιουργία ολοκληρωμένων περιβαλλόντων ανάπτυξης, με μεγάλη εξοικονόμηση χρόνου εγκατάστασής του. Το συγκεκριμένο project ξεκίνησε τον Ιανουάριο του 2010 από τον Mitchell Hashimoto.

Το εργαλείο αυτό χρησιμοποιείται για την δημιουργία και ρύθμιση φορητών και ελαφριών εικονικών περιβαλλόντων ανάπτυξης, τα οποία μπορούν εύκολα να αναπαραχθούν οποιαδήποτε στιγμή. Το πρόγραμμα αυτό, μπορεί να χρησιμοποιηθεί στα περισσότερα λειτουργικά συστήματα και είναι γραμμένο στην προγραμματιστική γλώσσα Ruby, όμως μπορεί να υποστηρίξει την ανάπτυξή του σε οποιαδήποτε σχεδόν, βασική γλώσσα.

Το Vagrant διαχειρίζεται όλες τις σημαντικές ρυθμίσεις, με σκοπό την αποφυγή του χρόνου δημιουργίας και εγκατάστασης καθώς και συντήρησης του περιβάλλοντος. Η ροή της εργασίας που ελέγχει το δημιουργημένο περιβάλλον βοηθά στην αύξηση και μεγιστοποίηση της παραγωγικότητας και ελαστικότητας. Το συγκεκριμένο εργαλείο είναι σχεδιασμένο να τρέχει σε οποιοδήποτε πρόγραμμα εικονικών μηχανημάτων, όπως για παράδειγμα το VirtualBox και VM ware, παρόλα αυτά προεπιλεγμένη υποστήριξη παρέχεται μόνο για το VirtualBox. Για οποιοδήποτε άλλο η εγκατάσταση plugins είναι απαραίτητη για την ομαλή λειτουργία και συντήρηση.

Για τους προγραμματιστές, το Vagrant αποτελεί χρήσιμο και πρακτικό εργαλείο για την απομόνωση και διαχώριση των dependency αρχείων που είναι απαραίτητα για την εγκατάσταση και ρύθμιση χρήσιμων εφαρμογών, στο ίδιο το περιβάλλον. Σημαντικό προτέρημα αποτελεί η διαχώριση του από οποιοδήποτε άλλο εργαλείο που ίσως χρησιμοποιηθεί στο project ανάπτυξης, όπως για παράδειγμα προγράμματα περιήγησης και επεξεργασίας. Ανεξάρτητα από το λειτουργικό σύστημα που χρησιμοποιεί κάθε μέλος του project (Windows, Mac OS X ή Linux), οι απαραίτητες λειτουργίες συμβαίνουν στο συγκεκριμένο πρόγραμμα και ρυθμίζονται κατά τον ίδιο τρόπο [26].

Για τους μηχανικούς, το συγκεκριμένο εργαλείο καθιστά εφικτή την δημιουργία προσωρινών και εύκολα προσβάσιμων και διαθέσιμων περιβαλλόντων καθώς και μίας σταθερής ροής εργασιών για την δημιουργία και τον έλεγχο υποδομής για ανάπτυξη και διαχείριση scripts. Ο έλεγχος αυτός γίνεται πολύ εύκολα, με μεγάλη εξοικονόμηση χρόνου και πόρων στο εικονικό περιβάλλον ανάπτυξης [26].

Όσο αφορά τους designers, το συγκεκριμένο πρόγραμμα παρέχει το κατάλληλο περιβάλλον που είναι απαραίτητο για την δημιουργία μίας εύκολης και απλής διαδικασίας σχεδιασμού. Με το τρόπο αυτό, η εργασία κάποιου designer γίνεται λιγότερο πολύπλοκη με αποτέλεσμα την αύξηση της παραγωγικότητας [26].

Η διαδικασία της εγκατάστασης και ρύθμισης του εργαλείου αυτού αποτελεί εξαιρετικά απλή διαδικασία, όπως θα αναφερθεί και στην συνέχεια. Η βάση της διαδικασίας της ρύθμισης του περιβάλλοντος ανάπτυξης αποτελεί το αρχείο Vagrantfile. Το αρχείο αυτό συμπεριλαμβάνει όλες τις επιλογές ρύθμισης που μπορεί να χρειαστούν για το περιβάλλον Vagrant, και είναι γραμμένο σε γλώσσα Ruby. Παρέχει την δυνατότητα εγκατάστασης των απαραίτητων αρχείων καθώς και την επιλογή για αλλαγές στις αρχικές ρυθμίσεις.

Το εργαλείο Vagrant, επίσης δίνει την δυνατότητα χρήσης των Vagrant Boxes, τα οποία αποτελούν πακέτα διαμόρφωσης που χρησιμοποιούνται για την δημιουργία περιβαλλόντων Vagrant. Τα Vagrant Boxes μπορούν να χρησιμοποιηθούν από οποιοδήποτε χρήστη και οργανισμό για την δημιουργία όμοιων εικονικών περιβαλλόντων που μπορούν εύκολα να αναβαθμιστούν και να βελτιωθούν. Υπάρχει διαθέσιμος δημόσιος κατάλογος προς όλους τους χρήστες και οργανισμούς, όμως κάθε χρήστης μπορεί να χρησιμοποιήσει δικό του μηχάνημα προσαρμοσμένο αποκλειστικά στις ανάγκες του.

Τέλος, το Vagrant δίνει την δυνατότητα καθορισμού και διαχείρισης πολλαπλών εικονικών μηχανημάτων κάτι που δίνει την δυνατότητα δημιουργίας ενός αλληλένδετου και αλληλοεξαρτόμενου περιβάλλοντος με πολλαπλά μηχανήματα. Το χαρακτηριστικό αυτό, χρησιμοποιήθηκε στην συγκεκριμένη διατριβή για την δημιουργία του εικονικού περιβάλλοντος Υπολογιστικού σύννεφου.

Κάποια ενδιαφέροντα χαρακτηριστικά που παρουσιάζονται στο εργαλείο Vagrant αποτελούν τα εξής:

1. Η ύπαρξη μεγάλου δημόσια διαθέσιμου καταλόγου Vagrant Boxes.

2. Η δυνατότητα ανάκτησης του κάθε μηχανήματος σε κάποιο αρχείο Vagrant box για μελλοντική χρήση και ανάπτυξη.

3. Η δυνατότητα προσαρμογής ρυθμίσεων στα εικονικά μηχανήματα.

4. Η εισαγωγή των Vagrantfiles, που παρέχουν την δυνατότητα εγκατάστασης των απαραίτητων πακέτων καθώς και την δυνατότητα αλλαγής των αρχικών ρυθμίσεων.

5. Η αλληλοεξάρτηση και ενσωμάτωση διάφορων εργαλείων διαχείρισης των ρυθμίσεων όπως το Puppet, Chef και Ansible.

3.1.2 Ansible

Όπως αναφέρθηκε, μαζί με την χρήση του εργαλείου Vagrant δίνεται η δυνατότητα χρήσης εργαλείων διαχείρισης (Puppet, Chef και Ansible) των απαραίτητων ρυθμίσεων που μπορεί να είναι απαραίτητες σε κάποιο περιβάλλον. Τα συγκεκριμένα Configuration Management tools είναι σε συνεργασία με το εργαλείο Vagrant της Hashicorp και μπορούν εύκολα να χρησιμοποιηθούν για οποιαδήποτε διαχείριση και ρύθμιση μπορεί να χρειαστεί.

Στην συγκεκριμένη διατριβή, το εργαλείο που θα παρουσιαστεί για την διαχείριση του εικονικού περιβάλλοντος όσο αφορά την ασφάλισή του, αποτελεί το Ansible (https://www.ansible.com/).

Το εργαλείο Ansible αποτελεί μια μηχανή IT αυτοματοποίησης, που χρησιμοποιείται κυρίως για την απλοποίηση της διαδικασίας της διάταξης και ρύθμισης του κάθε περιβάλλοντος καθώς και της σύνθεσης των υπηρεσιών και εφαρμογών που παρέχονται.

Η διαδικασία εγκατάστασης του συγκεκριμένου εργαλείου είναι εξαιρετικά απλή και η χρήση του απαιτεί περιορισμένο αριθμό δαπανών και υπολογιστικών πόρων. Η διαδικασία της αυτοματοποίησης γίνεται σε γλώσσα εύκολα αναγνώσιμη από τους χρήστες και χρειάζονται ελάχιστες ικανότητες και γνώσεις προγραμματιστικών γλωσσών. Οι διαδικασίες που λαμβάνουν μέρος στην διαδικασία της αυτοματοποίησης εκτελούνται σε ειδική σειρά, καθιστώντας έτσι εύκολη την αύξηση της παραγωγικότητας και εξοικονόμησης χρόνου και κόπου [27].

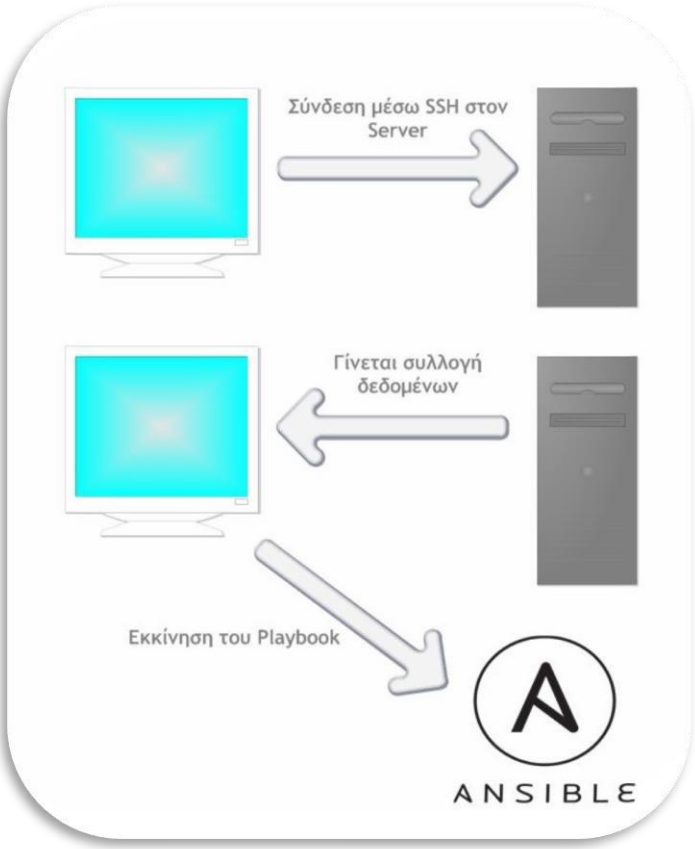
Το Ansible αποτελεί ένα εξαιρετικά απλό αλλά και ισχυρό εργαλείο που αποτελείται από ανεξάρτητη αρχιτεκτονική, κάτι που συμβάλει εξαιρετικά στην προστασία του περιβάλλοντος που δημιουργήθηκε καθώς δεν επιτρέπει σε εξωτερικούς διαχειριστές να εκμεταλλευθούν ευπάθειες ή να συμβάλλουν σε άλλες διαδικασίες. Απαραίτητα στοιχεία για να ξεκινήσει η διαδικασία διαχείρισης και ρύθμισης μέσω του προγράμματος Ansible, αποτελούν η προγραμματιστική γλώσσα Python καθώς και το Open SSH [27].

Η διαδικασία εκκίνησης του Ansible, όπως φαίνεται παρακάτω και στην Εικόνα 11, αποτελείται από τα εξής απλά βήματα:

1. Αρχικά ο διαχειριστής του συστήματος, με χρήση του πρωτοκόλλου SSH, συνδέεται στον διακομιστή.

2. Στην συνέχεια ο διαχειριστής του συστήματος συγκεντρώνει απαραίτητες πληροφορίες και δεδομένα από τον διακομιστή, όπως για παράδειγμα το λειτουργικό σύστημα και όλα τα εγκαταστημένα προγράμματα.

3. Τέλος μετά την συγκέντρωση όλων των απαραίτητων πληροφορίων από τον διακομιστή, το Ansible εκτελεί το Playbook.



Εικόνα 11. Στάδια εκκίνησης του Ansible.

Το Playbook αποτελεί ένα απλό και εύχρηστο configuration αρχείο, γραμμένο σε σύνταξη YAML, που αποτελεί γλώσσα αναγνωρίσιμη τόσο στους χρήστες όσο και στις μηχανές. Τα αρχεία αυτά συμπεριλαμβάνουν όλα τα απαραίτητα βήματα για την ανάπτυξη των ρυθμίσεων και αποτελούν την βάση για την ανάπτυξη περιβαλλόντων, ακόμα και με πολλαπλά μηχανήματα κάτι με το οποίο ασχολείται και η συγκεκριμένη διατριβή [28].

Τα Playbooks αποτελούν πολυτμηματικά αρχεία και μπορούν να περιλαμβάνουν μεταβλητές και πολλαπλά tasks και modules, όπως θα αναφερθεί και παρακάτω, για την διαχείριση των βημάτων των απαραίτητων ρυθμίσεων του περιβάλλοντος. Ο πελάτης με την χρήση του Playbook, μπορεί να τρέξει διαφορετικά tasks όπως για παράδειγμα την διαδικασία αντιγραφής αρχείων, να χρησιμοποιήσει διάφορα modules, να αντικαταστήσει μεταβλητές και να αναθέσει διαφορετικά Roles, όπως για παράδειγμα την εγκατάσταση του firewall [28].

Πιο αναλυτικά, μερικά από τα πιο σημαντικά στοιχεία που δημιουργούν και συνθέτουν το Ansible αποτελούν τα εξής:

1. Host Inventory. Στο αρχείο αυτό γίνεται η καταγραφή των εξυπηρετητών καθώς και των διακομιστών, οι οποίοι έχουν ανατεθεί για την διαχείριση και ρύθμιση με την χρήση του Ansible. Με την χρήση του Host Inventory, η λίστα των εξυπηρετητών μπορεί να οργανωθεί σε ομάδες καθώς και να ανατεθούν μεταβλητές για κάθε έναν από αυτούς, όπως για παράδειγμα τα κατάλληλα ports [29].

2. Plays, Tasks και Modules. Κάθε Playbook αποτελείται από ένα ή και περισσότερα Plays σε μία λίστα. Σκοπός του κάθε Play αποτελεί να αναθέσει σε κάθε εξυπηρετητή, διακομιστή ή και ομάδα μία σειρά από Tasks που με την σειρά τους καλούν τα Modules. Τα Modules χρησιμοποιούνται ώστε να τροποποιήσουν ή και να διαχειριστούν διάφορες ρυθμίσεις που συμβαίνουν στον διακομιστή. Οι αλλαγές που γίνονται μέσω των Modules είναι στατικές. Τα Modules χρησιμοποιούνται για την εγκατάσταση προγραμμάτων, την εκτέλεση εντολών, αντιγραφή αρχείων, διαχείριση υπηρεσιών και πλήθος άλλων ρυθμίσεων. Υπάρχει πληθώρα modules που παρέχονται στους χρήστες από την Ansible, με έτοιμες εντολές για διάφορα είδη ρυθμίσεων αλλά δίνεται και η δυνατότητα δημιουργίας νέου από την μεριά του χρήστη ή οργανισμού (http://docs.ansible.com/ansible/modules_by_category.html).

3. Handlers. Τα Handlers αποτελούν συγκεκριμένου είδους Tasks τα οποία εκτελούνται έπειτα από συγκεκριμένο έναυσμα. Τα Handlers εκτελούνται στο τέλος κάθε Play και για μόνο μία φορά. Μπορούν επίσης να χρησιμοποιηθούν για την επανεκκίνηση ορισμένων ρυθμίσεων ώστε να ενεργήσουν συγκεκριμένες αλλαγές που μπορεί να έχουν λάβει μέρος στο σύστημα.

4. Variables, Templates και Facts. Η εφαρμογή των Variables γίνεται ώστε να επιτρέψουν την αλλαγή κάποιων ρυθμίσεων σε πολλά και διαφορετικά περιβάλλοντα. Με τα Templates επιτρέπεται με την χρήση μεταβλητών, να γίνει αντιγραφή κάποιων αρχείων ρύθμισης διάφορων εργαλείων και προγραμμάτων καθώς και αλλαγή και ανάπτυξη συγκεκριμένων σημείων τους. Τέλος, τα Facts αποτελούν πληροφορίες που έχουν συλλεγεί για κάθε διακομιστή, όπως για παράδειγμα IP διευθύνσεις, μνήμη και χώρος δίσκου. Τα Facts χρησιμοποιούνται κυρίως για την βελτίωση της επικοινωνίας με τον διακομιστή.

5. Roles. Τα Roles αποτελούν ένα ειδικό είδος Playbook. Η χρήση τους γίνεται κυρίως για την καλύτερη οργάνωση και λειτουργία των Tasks. Η δομή κάθε Role περιλαμβάνει

έτοιμους καταλόγους από Tasks, Variables, Templates ρύθμισης και άλλα απαραίτητα αρχεία. Τα Roles συμπεριλαμβάνουν αρχεία τα οποία συνδυάζονται μεταξύ τους ώστε να απαλοιφούν περιττά βήματα, χρόνος αλλά και κόπος για την διαχείριση των ρυθμίσεων.

Τέλος, το Ansible δίνει την δυνατότητα χρήσης έτοιμων Roles, μέσω του Ansible Galaxy που αποτελεί κοινότητα διαμοιρασμού Roles (https://galaxy.ansible.com/).

3.2 Δημιουργία Εικονικού Περιβάλλοντος Υπολογιστικού σύννεφου

Όπως έχει αναφερθεί, για την δημιουργία ενός εικονικού περιβάλλοντος Υπολογιστικού σύννεφου υπάρχει πληθώρα εργαλειών αλλά και προγραμμάτων ανοιχτού κώδικα που μπορούν να χρησιμοποιηθούν, όμως στα πλαίσια της συγκεκριμένης διατριβής χρησιμοποιήθηκε το Vagrant της Hashicorp. Το Vagrant μπορεί να δημιουργήσει πολλά μηχανήματα στο ίδιο περιβάλλον και κάθε εντολή να εκτελείται ταυτόχρονα σε όλα τα υπάρχοντα μηχανήματα του περιβάλλοντος.

Αρχικά πρέπει να επιλεγεί το κατάλληλο Vagrant Box, από την δημόσια διαθέσιμη λίστα μηχανημάτων. Υπάρχει βέβαια, όπως έχει αναφερθεί και η δυνατότητα δημιουργίας μηχανήματος ανεξάρτητα από την προεπιλεγμένη λίστα που παρέχεται. Διατίθεται μεγάλη ποικιλία εικονικών μηχανημάτων που έχουν την δυνατότητα να χρησιμοποιηθούν με μεγάλο αριθμό λειτουργικών συστημάτων σε διαφορετικές εκδόσεις, όπως για παράδειγμα Ubuntu, OpenSuse, CentOS, Fedora, Debian, OpenBSD, Solaris και Kali Linux. Για τις ανάγκες της συγκεκριμένης διατριβής, χρησιμοποιήθηκε μηχάνημα λειτουργικού συστήματος Ubuntu.

Ανεξάρτητα του επιλεγμένου εικονικού μηχανήματος, η διαδικασία δημιουργίας ενός ή πολλαπλών απομακρυσμένων χρηστών είναι η ίδια. Με την απλή εντολή *$ vagrant init* και την ονομασία του εικονικού Vagrant Box που επιλέχθηκε καθώς και με την εντολή *$ vagrant up* το εικονικό μηχάνημα είναι έτοιμο για χρήση. Για την είσοδο μέσω του Vagrant στο εικονικό μηχάνημα, χρησιμοποιείται το SSH πρωτόκολλο με την εντολή *$ vagrant ssh* και την ονομασία του εικονικού μηχανήματος.

Με χρήση της εντολής *$ vagrant status* γίνεται η ενημέρωση, κάθε χρονική στιγμή, της κατάστασης του μηχανήματος και η διαδικασία σταματάει με την εντολή *$ vagrant destroy*.

Με την δημιουργία ενός εικονικού μηχανήματος, δημιουργείται και το Vagrantfile. Όλες οι απαραίτητες ρυθμίσεις καταγράφονται στο συγκεκριμένο αρχείο, όπως για παράδειγμα η εσωτερική μνήμη του κάθε μηχανήματος ή η δημιουργία του συστήματος πολλαπλών διασυνδεδεμένων μηχανημάτων.

Για την δημιουργία του εικονικού περιβάλλοντος Cloud Computing, εισάγονται στο Vagrantfile οι παρακάτω γραμμές κώδικα:

```
N = 4
(1.4). each do |i|
config.vm.define "node-#{i}" do |node|
node.vm.hostname = "node-#{i}"
node.vm.network "public_network", auto_config: "false", bridge: ENV['VAGRANT_INTERFACE']
```

Σύμφωνα με τα παραπάνω, το N εκπροσωπεί τον αριθμό των μηχανημάτων που θα δημιουργηθούν. Επίσης τέθηκε η ονομασία κάθε μηχανήματος καθώς και το είδος του δικτύου και το interface που χρησιμοποιείται για σύνδεση στο διαδίκτυο. Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε environmental μεταβλητή η οποία καλέσθηκε στο αρχείο Vagrantfile για χρήση.

Για την ανάθεση σταθερών διευθύνσεων IP σε κάθε χρήστη είναι απαραίτητη η εισαγωγή των παρακάτω, στο αρχείο Vagrantfile:

```
node.vm.provision "shell", run: "always", inline: "ifconfig eth1 192.168.1.#{i+104} netmask 255.255.255.0 up"
```

Κάθε χρήστης θα πρέπει να καθοριστεί σε κάποιο Host Inventory αρχείο, ώστε να επιλέγεται αυτόματα όταν ξεκινά η διαδικασία των απαραίτητων ρυθμίσεων και διαχείρισης του περιβάλλοντος με την εγκατάσταση και χρήση του Ansible. Μέσα στο αρχείο ρύθμισης του Ansible (ansible.cfg) καθορίζουμε το αρχείο που περιέχει την λίστα των απομακρυσμένων χρηστών.

Για να γίνει εφικτή η σύνδεση του εργαλείου Vagrant, για την δημιουργία του περιβάλλοντος και του Ansible για την διαχείριση των ρυθμίσεων, πρέπει να γίνουν κάποιες αλλαγές στο

Vagrantfile. Οι αλλαγές αυτές γίνονται, ώστε να είναι εφικτή η χρήση του Ansible Playbook το οποίο περιέχει όλες τις απαραίτητες ενέργειες και όλα τα βήματα για την ρύθμιση και διαχείριση των χρηστών.

Πιο συγκεκριμένα, το αρχείο Vagrantfile στο σημείο που αναφέρεται η σύνδεσή του με το εργαλείο Ansible πρέπει να είναι της μορφής:

```
config.vm.provision "shell", inline: <<-SHELL
apt-get update ; apt-get upgrade -y
SHELL

#Run ansible
  if i == N
   node.vm.provision:ansible do |ansible|
    ansible.limit = "all"
    ansible.playbook = "playbook.yml"
    ansible.sudo = true
```

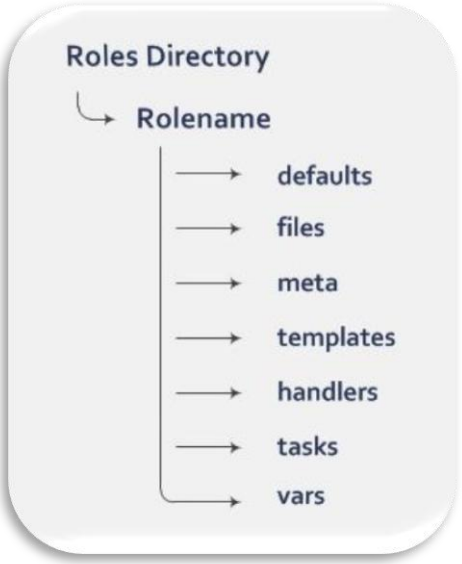
Με την διαδικασία που αναφέρθηκε, δημιουργήθηκε το εικονικό περιβάλλον καθώς και η διασύνδεση πολλαπλών χρηστών για την εξομοίωση του περιβάλλοντος Υπολογιστικού σύννεφου. Με την χρήση του εργαλείου αυτοματοποίησης των διαδικασιών ρύθμισης και διαχείρισης των χρηστών Ansible, ξεκινάει η διαδικασία ασφάλισης των απομακρυσμένων χρηστών.

3.3 Ρύθμιση και ασφάλιση του Εικονικού Περιβάλλοντος Υπολογιστικού σύννεφου

Ανεξάρτητα από το γεγονός ότι κάθε λειτουργικό σύστημα χρησιμοποιεί διαφορετικά εργαλεία αλλά και εντολές, τα βασικά βήματα για την διαδικασία της ασφάλισης πολλαπλών απομακρυσμένων χρηστών με την χρήση του Ansible, είναι τα ίδια.

Το Ansible όπως αναφέρθηκε, χρησιμοποιεί Roles τα οποία αποτελούν ειδικό είδος Playbook και περιλαμβάνουν Tasks, Variables, Templates, Handlers και άλλα απαραίτητα αρχεία, όπως φαίνεται και στην Εικόνα 12. Τα αρχεία αυτά συνδυάζονται μεταξύ τους για την απαλοιφή

περιττών βημάτων, χρόνου αλλά και κόπου για την διαχείριση των απαραίτητων ρυθμίσεων. Για την δημιουργία Role γίνεται απλή χρήση της εντολής *$ ansible-galaxy init Rolename* στον επιλεγμένο και δημιουργημένο φάκελο του Role με Rolename την επιλεγμένη ονομασία του κάθε Role.



Εικόνα 12. Δομή Role.

Κάθε δημιουργημένο Role, μπορεί να αποτελείται από πολλά διαφορετικά Tasks με παρόμοια λειτουργία για καλύτερη οργάνωση, με την διαδικασία διαχώρισης του σε μικρότερα κομμάτια όσο αφορά τα βήματα για τις απαραίτητες ρυθμίσεις. Δίνεται η δυνατότητα ύπαρξης μεγάλου αριθμού Roles για την διευκόλυνση της οργάνωσης των βημάτων. Ο καταμερισμός και η κατανομή των Roles είναι καθαρά υποκειμενική απόφαση και οργανώνεται σύμφωνα με τις ανάγκες και επιθυμίες κάθε προγραμματιστή.

Ο τρόπος γραφής των διάφορων tasks, handlers και άλλων αρχείων είναι συγκεκριμένος και οργανωμένος με τέτοιο τρόπο ώστε να είναι εύκολος στην κατανόηση και από χρήστες που δεν διαθέτουν μεγάλη εμπειρία σε παρόμοιου είδους προγράμματα. Η διαδικασία κατανόησης του συγκεκριμένου τρόπου γραφής αποτελεί απλή διαδικασία και έπειτα από συγκεκριμένες δοκιμές γίνεται εμφανής η διευκόλυνση που παρέχει στην οργάνωση και ανάγνωση των εντολών.

Όπως αναφέρθηκε, υπάρχουν αρκετά Modules, ώστε να απλοποιείται η διαδικασία της ρύθμισης με έτοιμες εντολές που παρέχονται μέσω του Ansible. Μέσα σε κάθε φάκελο Role, στους υποφακέλους των Tasks που έχουν ανατεθεί για κάθε λειτουργία, δίνεται η δυνατότητα χρήσης των παρεχόμενων Modules για εξοικονόμηση κόπου και χρόνου.

Μετά την εγκατάσταση και την εκκίνηση των Vagrant Boxes, το Ansible εκτελεί το Playbook το οποίο με την σειρά του εκτελεί όλα τα επιπλέον Roles που δημιουργήθηκαν για την διαδικασία της ασφάλισης των πολλαπλών μηχανημάτων που δημιουργήθηκαν μέσω του Vagrant.

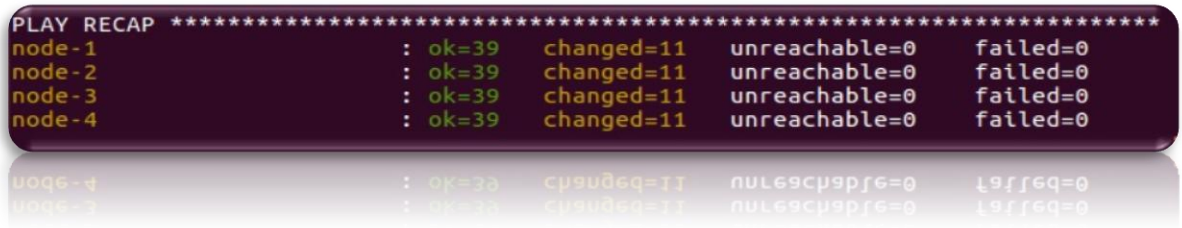
Παράδειγμα αρχείου Playbook αποτελεί το παρακάτω:

```
- hosts: all
  become: true
  roles:
    -role 1
    -role 2
    -role 3
```

Σύμφωνα με το παράδειγμα, το συγκεκριμένο Playbook αναφέρεται σε όλους τους χρήστες που έχουν καταγραφεί στο Host Inventory, παρόλα αυτά δίνεται η δυνατότητα επιλογής ενός ή ακόμα και μίας ή περισσότερων ομάδων, αρκεί αυτοί να έχουν καθοριστεί στο αρχείο αυτό. Όσο αφορά τις ονομασίες των Roles (role 1, role 2, role 3) αυτές καθορίζονται αποκλειστικά βάσει των επιθυμιών κάθε προγραμματιστή και των λειτουργιών που σκοπεύουν να ανατεθούν. Πιθανές ονομασίες, όπως χρησιμοποιήθηκαν και στην διατριβή αυτή αποτελούν τα: Firewall, Intrusion, Monitoring, Setup κ.α.

Έπειτα από την εκκίνηση λειτουργίας των πολλαπλών μηχανημάτων, μέσω του Vagrant και της εντολής *$ vagrant up*, ξεκινάει η διαδικασία εκκίνησης του Ansible και όλων των ρυθμίσεων που έχουν ανατεθεί, όπως θα παρουσιαστεί στην συνέχεια.

Η επιτυχημένη εκκίνηση και λειτουργία του Vagrant και του Ansible Playbook, παρουσιάζεται στην παρακάτω εικόνα. Στην συγκεκριμένη εικόνα οι ονομασίες node-1, node-2 κτλ αποτελούν τις ονομασίες που δόθηκαν, όπως αναλύθηκε στο Vagrantfile για κάθε απομακρυσμένο χρήστη που αποτελεί μέλος του εικονικού Περιβάλλοντος Υπολογιστικού σύννεφου.



Εικόνα 13. Επιτυχημένη εκκίνηση και λειτουργία.

Έπειτα από την επιτυχημένη εκκίνηση και ρύθμιση του περιβάλλοντος, η σύνδεση με κάθε απομακρυσμένο χρήστη για επιπλέον λειτουργίες γίνεται μέσω SSH και πιο συγκεκριμένα με την εντολή *$ ssh hostname@IP,* όπου hostname αποτελεί η ονομασία που δόθηκε σε κάθε χρήστη μέσω του Vagrantfile καθως και IP η διεύθυνση που ανατέθηκε σε κάθε έναν από αυτούς.

3.3.1 Απαραίτητα βήματα εξασφάλισης της ασφάλειας του Εικονικού Περιβάλλοντος

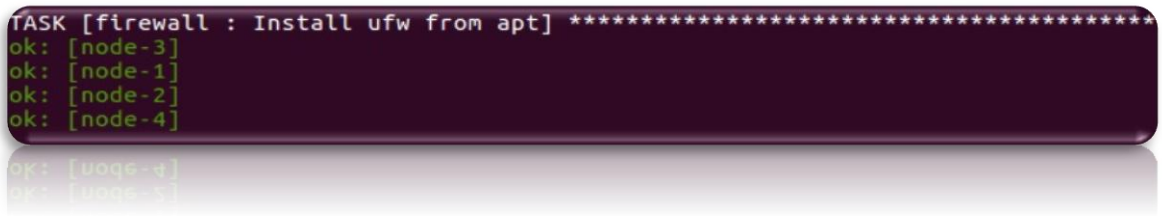
Κατά την διαδικασία της δημιουργίας και ρύθμισης ενός περιβάλλοντος Υπολογιστικού σύννεφου είναι απαραίτητο και εξαιρετικά σημαντικό να ληφθεί υπόψη η ασφάλεια και η ιδιωτικότητα των δεδομένων. Είναι αναγκαίο να μελετηθούν σοβαρά τα ζητήματα ασφάλειας που μπορεί να υπάρχουν, οι πολιτικές καθώς και τα μοντέλα ασφάλειας που βασίζονται στα Security Standards [08].

Τα ζητήματα ασφάλειας όπως έχει αναφερθεί, στα περιβάλλοντα Cloud αποτελούν τα εξής:

1. Έλεγχος πρόσβασης.
2. Ανάκτηση δεδομένων.
3. Ασφάλεια των δεδομένων.
4. Συμμόρφωση χρηστών στις καθορισμένες ρυθμίσεις.
5. Τοποθεσία των δεδομένων.
6. Ανασφαλή Interfaces και API (Application Programming Interfaces).
7. Ζητήματα κοινόχρηστων τεχνολογιών.

Οι στρατηγικές και τα βήματα ασφάλειας είναι απαραίτητο να αναβαθμίζονται ανά τακτά χρονικά διαστήματα καθώς νέες τεχνολογίες ανακαλύπτονται συνεχώς καθώς και νέοι τρόποι καταπάτησης των βασικών αρχών ασφάλειας. Συνεπώς, η ασφάλεια αποτελεί μία διαρκώς αναβαθμιζόμενη διαδικασία.

Για την ασφάλιση των απομακρυσμένων χρηστών μέσω του Ansible, κυρίως για ζητήματα που αφορούν τον έλεγχο πρόσβασης, την ασφάλεια των δεδομένων και τα ζητήματα κοινόχρηστων τεχνολογιών, ακολουθήθηκαν τα βήματα που θα αναλυθούν παρακάτω. Δημιουργήθηκαν συγκεκριμένα Tasks που βρίσκονται σε καθορισμένους φακέλους ανά κάθε δημιουργημένο Role, ανάλογα με το είδος τους, για την καλύτερη οργάνωση των ρυθμίσεων. Επιτυχημένη χρήση των Tasks παρουσιάζεται στην Εικόνα 14 και 15. Όπως αναφέρθηκε κάθε Role δημιουργείται με την εντολή *$ ansible-galaxy init Rolename*. Επίσης, με την εκτέλεση του Playbook, όλα τα βήματα ανατέθηκαν σε όλους τους απομακρυσμένους χρήστες, καθώς τα Host Inventories των εργαλείων Vagrant και Ansible είναι διασυνδεδεμένα και οι χρήστες επιλέγονται αυτόματα με την εκκίνηση των συγκεκριμένων προγραμμάτων.



Εικόνα 14. Επιτυχημένη χρήση Task.

Εικόνα 15. Επιτυχημένη χρήση Task.

Πιο συγκεκριμένα τα βήματα διασφάλισης των χρηστών που ακολουθήθηκαν είναι τα παρακάτω:

1. Updates και Upgrades. Η διασφάλιση των συχνών αναβαθμίσεων των συστημάτων αποτελεί ίσως και το σημαντικότερο μέτρο ασφάλειας που μπορεί να ληφθεί για την ασφάλιση οποιουδήποτε λειτουργικού συστήματος. Οι αναβαθμίσεις software μπορούν να αποτελούν είτε λογισμικά ενημέρωσης για μεγάλες ευπάθειες ασφάλειας που μπορεί να ανακαλυφθούν είτε επιδιορθώσεις για μικρά σφάλματα που μπορεί να παρουσιαστούν. Καθώς διαρκώς εμφανίζονται νέες εκδόσεις λειτουργικών συστημάτων και εφαρμογών, οι υπολογιστές δεν λαμβάνουν όλες τις απαραίτητες ενημερώσεις και επιδιορθώσεις ασφάλειας, οπότε είναι ιδιαίτερα σημαντικές οι συνεχείς ενημερώσεις και αναβαθμίσεις [30].

Έπειτα από την ανάθεση του συγκεκριμένου βήματος στο κατάλληλο Role ανάλογα με το είδος (στην περίπτωση της συγκεκριμένης διατριβής χρησιμοποιήθηκε ένα Role με την ονομασία setup που συμπεριλαμβάνει όλες τις βασικές ρυθμίσεις), το αρχείο του Task που δημιουργήθηκε είναι της μορφής:

```
- name: Update APT package cache
  apt:
    update_cache: yes
- name: Run apt-get upgrade
  apt:
    upgrade: full
```

Το apt που εμφανίζεται στην παραπάνω μορφή Task, αποτελεί έτοιμο Module που χρησιμοποιείται για την εγκατάσταση πακέτων σε συστήματα Linux.

2. Δημιουργία λογαριασμών με κρυπτογραφημένους κωδικούς ασφάλειας. Πολύ σημαντικό βήμα για την διασφάλιση της ασφάλειας, αποτελεί η ανάθεση των λογαριασμών χρηστών για κάθε μηχάνημα με κρυπτογραφημένα κλειδιά. Τα κλειδιά κρυπτογραφούνται ώστε να αποφυγεί και να δυσκολευτεί η αποκρυπτογράφησή τους από πιθανούς κακόβουλους χρήστες. Για να διευκολυνθεί η διαδικασία ανάθεσης λογαριασμών ανά εικονικό μηχάνημα, είναι αναγκαία η δημιουργία ενός επιπλέον φακέλου μέσα στο περιβάλλον που εκτελείται το Vagrant, που περιλαμβάνει αρχείο μεταβλητών (οι μεταβλητές σε όλα τα υπόλοιπα αρχεία συμβολίζονται ως εξής: "{{ μεταβλητή }}"), για κάθε λογαριασμό με τον αντίστοιχο κρυπτογραφημένο κωδικό ασφάλειας. Για την δημιουργία των κρυπτογραφημένων κωδικών χρησιμοποιήθηκε η εντολή *$ mkpasswd –method=sha-512.* Κάθε αρχείο, για κάθε ένα μηχάνημα ξεχωριστά είναι της μορφής:

```
user: username
password:
$6$JwvqQTg21Ib$NijLJFoV3NOvZZvzImBVg1y9zmBeO64iI23KCAb3VSxihoBBfhOSfpCU
cErsXG0n766BhMuRpgRKfEhtlAM.C8JB/
```

Μέσα στο καθορισμένο Role που επιλέγεται στο κεντρικό αρχείο του Task καταγράφεται η σειρά των εντολών για την δημιουργία αλλά και την ανάθεση των κωδικών χρήσης. Οι

ονομασίες και τα κλειδιά αναθέτονται από τα αρχεία που δημιουργήθηκαν, όπως αναφέρθηκε παραπάνω.

```
- user:
    name: "{{ user }}"
    password: "{{ password }}"
    state: present
```

3. Δημιουργία SSH κλειδιών για κάθε ένα λογαριασμό. Καλή πρακτική ασφάλισης των απομακρυσμένων χρηστών αποτελεί η δημιουργία κρυπτογραφικού ζεύγους κλειδιών για την SSH πρόσβαση, καθώς ασφαλίζει το σύστημα και καθιστά την Brute-Force επίθεση για ανάκτηση πληροφοριών, πιο δύσκολη. Τα SSH κλειδιά συμπεριλαμβάνουν περισσότερα bits δεδομένων, εξασφαλίζοντας έτσι σε μεγαλύτερο βαθμό ότι μία Brute-Force επίθεση, που απειλεί την ασφάλεια των δεδομένων καθώς και την πρόσβαση στο σύστημα, θα είναι αποτυχημένη. Τα SSH κλειδιά αποτελούν ζεύγος δημόσιου και ιδιωτικού κλειδιού, που χρησιμοποιούνται για την πιστοποίηση της αυθεντικότητας για είσοδο σε κάποιο σύστημα. Το δημόσιο κλειδί μπορεί να διαμοιραστεί με όλους, σε αντίθεση με το ιδιωτικό κλειδί που αποτελεί κρυφό στοιχείο από τον χρήστη. Όταν κάποιος χρήστης επιχειρεί είσοδο στο σύστημα, χρησιμοποιεί το ιδιωτικό κλειδί του ώστε να διασφαλίσει την αυθεντικότητα του. Τότε ο διακομιστής, επιτρέπει στον χρήστη να συνδεθεί στο σύστημα καθώς έχει διασφαλιστεί η ταυτότητά του.
   Στον φάκελο του Role που ανατέθηκε το συγκεκριμένο βήμα ασφάλειας είναι απαραίτητη η δημιουργία υποφακέλου, μέσα στον οποίο δημιουργούνται τα ζευγάρια δημοσίου-ιδιωτικού κλειδιού για κάθε χρήστη. Τα κλειδιά αυτά δημιουργούνται με την εντολή *$ ssh_keygen –t rsa –f userfile,* όπου userfile είναι η ονομασία του αρχείου που θα χρησιμοποιηθεί. Το δημόσιο δημιουργημένο κλειδί καλείται μέσω του Module lookup, όπως παρατηρείται στην συνέχεια.

```
- authorized_key:
    user: "{{ user }}"
    key: "{{ lookup('file', './userfile/{{ user }}.pub') }}"
```

4. Εγκατάσταση SSL πιστοποιητικών. Τα ζεύγη κλειδιών που χρησιμοποιούνται για την κρυπτογράφηση της κίνησης επιπέδου εφαρμογών, χρησιμοποιούν συνδέσεις Secure Socket Layer (SSL) ή και Transport Layer Security (TLS). Το πιστοποιητικό SSL, αποτελεί

μέθοδο διανομής του δημοσίου κλειδιού σε χρήστες και οργανισμούς στο επίπεδο αυτό. Τα πιστοποιητικά αυτά, υπογράφονται ψηφιακά από κάποια Certification Authority (CA), που αποτελεί μία αμερόληπτη τρίτη οντότητα που επιβεβαιώνει ότι οι πληροφορίες που ανταλλάσονται είναι ακριβείς και ελεγμένες.

Για την δημιουργία του συγκεκριμένου Task είναι αναγκαία η δημιουργία ενός αρχείου μεταβλητών οι οποίες θα καλούνται από το κεντρικό αρχείο ώστε να γίνει η εγκατάσταση και χρήση των πιστοποιητικών SSL. Καθώς καλή πρακτική στην ρύθμιση της ασφάλειας μέσω του Ansible, είναι η χρήση των μεταβλητών και όχι η χρήση hardcoded πληροφοριών, για λόγους ασφάλειας, είναι απαραίτητη η δημιουργία του αρχείου αυτού. Μέσα στο αρχείο των μεταβλητών αποθηκεύονται πληροφορίες όπως: τα πεδία του πιστοποιητικού (χώρα, περιοχή, οργανισμός, μέρες ισχύος), ονομασία του πιστοποιητικού, τοποθεσία του αρχείου με το SSL πιστοποιητικό, ιδιοκτήτης του πιστοποιητικού (στην περίπτωση της συγκεκριμένης διατριβής ο χρήστης του κάθε μηχανήματος), τοποθεσία του ιδιωτικού κλειδιού, τοποθεσία της Certificate Signing Request (CSR) και το μήκος του κάθε κλειδιού. Οι πληροφορίες αυτές θα χρησιμοποιηθούν από το κεντρικό αρχείο του συγκεκριμένου Task..

Το Task αρχείο για την εγκατάσταση και χρήση των self-signed πιστοποιητικών SSL, ξεκινά με την εγκατάσταση του OpenSSL με την apt Module που αναφέρθηκε παραπάνω. Στην συνέχεια δημιουργείται φάκελος, χρησιμοποιώντας το file Module, στον οποίο καθορίζεται η τοποθεσία του πιστοποιητικού καθώς και ο ιδιοκτήτης, χρησιμοποιώντας το αρχείο μεταβλητών που δημιουργήθηκε:

```
- name: Ensure SSL folder exists
  file:
    path: "{{ ssl_certs_path }}"
    state: directory
    owner: "{{ ssl_certs_path_owner }}"
    mode: "{{ ssl_certs_mode }}"
```

Έπειτα γίνεται η δημιουργία του πιστοποιητικού, της CSR καθώς και του self-sighed πιστοποιητικού χρησιμοποιώντας την command Module καθώς και καλώντας τα απαραίτητα στοιχεία από το αρχείο των μεταβλητών. Πιο συγκεκριμένα:

```
- name: Generate RSA key
```

```
  command: openssl genrsa -out "{{ ssl_certs_privkey_path }}" "{{ ssl_certs_key_size }}" creates="{{ ssl_certs_privkey_path }}"

- name: Generate CSR
  command: openssl req -new -sha256 -subj "{{ ssl_certs_fields }}" -key "{{ ssl_certs_privkey_path }}" -out "{{ ssl_certs_csr_path }}" creates="{{ ssl_certs_csr_path }}"

 - name: Generate self-signed SSL certificate
  command: openssl req -nodes -x509 -days "{{ ssl_certs_days }}" -in "{{ ssl_certs_csr_path }}" -key "{{ ssl_certs_privkey_path }}" -out "{{ ssl_certs_cert_path }}" -extensions v3_ca creates="{{ ssl_certs_cert_path }}"
  when: true
```

Τέλος, και για τα τρία βήματα δημιουργίας SSL πιστοποιητικών που περιγράφηκαν με την βοήθεια του file Module καθορίζεται η ιδιοκτησία κάθε ενός κλειδιού, πιστοποιητικού και CSR.

5. Εγκατάσταση και ρύθμιση Firewall. Υπάρχουν αρκετά Security Firewalls ανοιχτού κώδικα για λειτουργικά συστήματα Linux, όπως για παράδειγμα τα Ip Tables, Ufw, IPCop Firewall, ShoreWall και IpFire. Το πιο κατάλληλο, ανάλογα με τις ανάγκες κάθε χρήστη και την συμβατότητα της κάθε έκδοσης λειτουργικού συστήματος, πρέπει να επιλεγεί ώστε να προστατευτεί κάθε σύστημα από επιθέσεις Denial of Service (Dos) καθώς και οποιαδήποτε άλλη ανεπιθύμητη εισχώρηση στο σύστημα. Η χρήση σωστού Firewall αποτρέποντας την πιθανή ανεπιθύμητη ανταλλαγή δεδομένων, παρέχει υψηλό επίπεδο ασφάλειας στα λειτουργικά συστήματα.

   Με την χρήση του Ansible, επιλέχθηκε το Ufw Firewall για την ασφάλιση των απομακρυσμένων χρηστών, με δημιουργία νέου Role με την ονομασία Firewall. Στο αρχείο task που χρησιμοποιήθηκε, δεν αναγράφεται καμμία πληροφορία hardcoded αλλά δημιουργείται αρχείο μεταβλητών που συμπεριλαμβάνει αριθμό πορτών ή και διευθύνσεις IP, που ίσως χρειαστούν στην διαδικασία ασφάλισης μέσω του firewall. Ο ρόλος που ανατίθεται για την εγκατάσταση και ρύθμιση του firewall, καλεί όλες τις μεταβλητές που θα χρειαστούν από τα δημιουργημένα αρχεία μεταβλητών. Επίσης είναι απαραίτητη η χρήση αρχείου Handler ώστε να επανεκκινείται η υπηρεσία αυτή κάθε φορά που το κάθε μηχάνημα χρησιμοποιείται.

Αρχικά γίνεται η εγκατάσταση του Ufw Firewall μέσω του Apt Module και στην συνέχεια ξεκινάει η διαδικασία ρύθμισης των κανόνων για αποφυγή Dos και πιθανών άλλων κακόβουλων επιθέσεων:

```
 - ufw:
    rule: limit
    port: "{{ item }}"
    proto: tcp
   with_items:
    - "{{ http_port }}"
    - "{{ https_port }}"
    - ssh
```

Στο συγκεκριμένο βήμα γίνεται οριοθέτηση των συνδέσεων σε συγκεκριμένες πόρτες. Πιο συγκεκριμένα το Ufw θα αρνηθεί συνδέσεις από κάποια IP διεύθυνση, εφόσον έχει επιχειρήσει την εκκίνηση 6 ή και περισσότερων συνδέσεων στα τελευταία 30 δευτερόλεπτα. Χρησιμοποιείται το with_items, το οποίο αποτελεί εύκολο βήμα οργάνωσης όταν χρειάζεται η ανάθεση των ίδιων εντολών σε παραπάνω από μία τιμή.
Στην συνέχεια, με την ίδια διαδικασία που περιγράφηκε παραπάνω οριοθετήθηκε και το πλήθος των πακέτων που εισέρχονται στο σύστημα ανά IP διεύθυνση.
Τέλος, όπως αναφέρεται παρακάτω ενεργοποιείται το Ufw καθώς και το Ufw logging και γίνεται ανάθεση του Handler με την εντολή notify.

```
 - ufw:
    logging: on
   notify:
    - restart ufw

 - ufw:
    state: enabled
```

Το αρχείο Handler θα είναι της μορφής:

```
- name: Restart ufw
  service:
    name: ufw
```

```
    state: restarted
```

6. Απενεργοποίηση πρωτοκόλλου IPV6. Κάποιος πιθανός επιτιθέμενος μπορεί να στείλει κακόβουλο λογισμικό μέσω του Internet Protocol version 6 (IPV6), καθώς δεν παρακολουθείται πάντα εκτενώς από τους διαχειριστές. Αν δεν αποτελεί αναγκαία συνθήκη για κάποια δικτυακή ρύθμιση, καλή πρακτική αποτελεί η απενεργοποίησή του ή η ρύθμιση Firewall για το πρωτόκολλο IPV6. Στα πλαίσια της συγκεκριμένης διατριβής θα ακολουθηθεί η τακτική της απενεργοποίησης.
   Με την χρήση της with_items λειτουργίας για πολλαπλή ανάθεση τιμών και ρυθμίζοντας τις sysctl εισαγωγές (δίνοντας την τιμή 1 για απενεργοποίηση των items που αναφέρονται), το Task αρχείο θα είναι της μορφής:

```
- name: Disable IPv6
  sysctl:
    name: "{{ item }}"
    value: 1
    state: present
  with_items:
    - net.ipv6.conf.all.disable_ipv6
    - net.ipv6.conf.default.disable_ipv6
    - net.ipv6.conf.lo.disable_ipv6
```

7. Αποφυγή IP Spoofing. Το IP Spoofing αποτελεί τεχνική συγκάλυψης κάποιας IP διεύθυνσης με κάποια ψεύτικη, ώστε ο κακόβουλος χρήστης να μπορεί να αποκρύψει την ταυτότητα του, κάνοντας τον στόχο του να θεωρεί ότι η κίνηση προέρχεται από κάποιον άλλον υπολογιστή.
   Η διαδικασία που ακολουθείται στο συγκεκριμένο Task ουσιαστικά αποτελεί μια απλή επεξεργασία κάποιου αρχείου ρύθμισης ώστε να μην επιτρέπεται η συγκεκριμένη κακόβουλη πράξη. Αρκεί λοιπόν, η πρόσθεση μίας επιπλέον γραμμής στο αρχείο των hosts με χρήση του έτοιμου Module, Line_in_file:

```
 - lineinfile:
    dest: /etc/host.conf
    line: 'nospoof on'
    state: present
```

8. Απενεργοποίηση του Irqbalance. Το Irqbalance χρησιμοποιείται για την διανομή διακοπών του hardware σε όλα τα πολλαπλά CPUs, με σκοπό την αύξηση της απόδοσης του κάθε συστήματος. Καλή τακτική ασφάλισης των συστημάτων, αποτελεί η απενεργοποίηση του Irqbalance ώστε να αποφυγεί οποιαδήποτε ανεπιθύμητη διακοπή hardware.
   Το Task αρχείο που ικανοποιεί το συγκεκριμένο βήμα είναι της μορφής:

   ```
   - replace:
       name: /etc/default/irqbalance
       regexp: '^ENABLED="1"$'
       replace: '^ENABLED="0"$'
   ```

   Το συγκεκριμένο βήμα, απενεργοποίησης του Irqbalance, γίνεται με το Replace Module που χρησιμεύει στην αντικατάσταση και μεταποίηση κάποιας εντολής σε κάποιο αρχείο ρύθμισης, στην συγκεκριμένη περίπτωση του αρχείου ρύθμισης του Irqbalance.

9. Ασφάλιση κοινόχρηστης μνήμης. Απαραίτητο βήμα ασφάλισης των απομακρυσμένων χρηστών, αποτελεί η διασφάλιση της καλής λειτουργίας μεταξύ όλων των χρηστών του Cloud περιβάλλοντος καθώς και επίλυση όλων των ζητημάτων που αφορούν τις κοινόχρηστες τεχνολογίες. Η κοινόχρηστη μνήμη μπορεί να χρησιμοποιηθεί σε κάποια επίθεση που αφορά ανοιχτές και σε λειτουργία υπηρεσίες (running services), httpd ή apache2, οπότε θεωρείται σωστό βήμα η ρύθμιση για την ασφάλισή της.
   Στο Role το οποίο έχει ανατεθεί η λειτουργία αυτή, στην περίπτωσή μας με ονομασία Setup, μέσω του έτοιμου Module Line_in_file θα γίνει εισαγωγή ρύθμισης στο αρχείο fstab που αφορά την κοινόχρηστη μνήμη. Πιο συγκεκριμένα:

   ```
    - name: Secure Shared Memory
      lineinfile:
       dest: /etc/fstab
       line: 'tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0'
       state: present
   ```

   Τέλος, είναι απαραίτητη η επανεκκίνηση του συστήματος ή η χρήση της εντολής mount για την διασφάλιση της σωστής λειτουργίας της αλλαγής αυτής. Στους καταλόγους του

Ansible υπάρχει έτοιμο Module Mount, το οποίο και χρησιμοποιήθηκε και στην συγκεκριμένη περίπτωση.

Στην συνέχεια ακολουθεί σειρά ρυθμίσεων που αφορούν την παρακολούθηση και ανίχνευση πιθανών ευάλωτων στοιχείων του συστήματος, με την εγκατάσταση και ρύθμιση εργαλείων παρακολούθησης. Για τις ανάγκες της πιο οργανωμένης διαδικασίας δημιουργήθηκε νέο Role με την ονομασία Monitoring που συμπεριλαμβάνει όλα τα απαραίτητα Tasks για κάθε ένα καθορισμένο βήμα.

10. Καθορισμός ανοιχτών και σε λειτουργία υπηρεσιών και συνδέσεων. Κάθε πιθανός επιτιθέμενος για να ξεκινήσει την διαδικασία επίθεσης σε κάποιο σύστημα, καταγράφει την ανεύρεση πιθανών ευπαθειών στο σύστημα. Για τον λόγο αυτό είναι αναγκαία η καταγραφή των υπηρεσιών και συνδέσεων, χρησιμοποιώντας κάποιο εργαλείο ανάλογα το λειτουργικό σύστημα και τις ανάγκες, από μεριά του χρήστη. Σε περίπτωση εύρεσης ανοιχτής σύνδεσης από κάποια μη αναγνωρίσιμη IP διεύθυνση ή πόρτα, είναι αναγκαία η λήψη περισσότερων μέτρων ασφάλειας και χρήσης εργαλείων ανάλυσης των μεταφορών δεδομένων.
    Για τις ανάγκες της συγκεκριμένης διατριβής, χρησιμοποιήθηκε το εργαλείο Netstat το οποίο αποτελεί μέλος του Net-tools, υπάρχουν όμως αρκετές επιλογές εργαλείων όπως το tcpdump, top, vmstat κ.α. Μετά από την διαδικασία της εγκατάστασης του εργαλείου χρησιμοποιώντας το Apt Module, το Task αρχείο για την ρύθμιση του συγκεκριμένου βήματος ασφάλειας είναι το εξής:

```
- name: Open processes using netstat
  shell: netstat -tunlp
  delegate_to: 127.0.0.1
  become: no
  register: results

- name: Get results from netstat
  debug:
   var: results
```

    Πιο αναλυτικά, η εντολή που χρησιμοποιείται μέσω της Shell Module $netstat –tunlp:
    t → tcp

u→ udp

n →shows IP addresses

l→ shows listening sockets

p→shows the Process Identifier and name of each program.

Με την χρήση την Delegate_to η εντολή εκτελείται στο μηχάνημα το οποίο εκτελεί το Ansible (IP 127.0.0.1) και αφορά όλους τους απομακρυσμένους χρήστες που έχουν δημιουργηθεί. Τέλος, η εμφάνιση των αποτελεσμάτων γίνεται κατά την διάρκεια εκτέλεσης του Playbook και όλων των επιπλέον Plays χρησιμοποιώντας το Module debug.

11. Καθορισμός ανοιχτών πορτών. Όπως αναλύθηκε παραπάνω, πιθανοί κακόβουλοι χρήστες εκμεταλλεύονται ευπάθειες ώστε να εκτελέσουν επιτυχημένες επιθέσεις σε κάποιο σύστημα. Εφόσον υπάρχουν ανοιχτές και εύκολα προσβάσιμες δημόσιες πόρτες, οποιοσδήποτε επιτιθέμενος μπορεί να ανακαλύψει πιθανές υπηρεσίες που λειτουργούν σε ανοιχτές πόρτες και έτσι να σχεδιάσει καλύτερα την επίθεσή του. Οπότε αποτελεί βασική ανάγκη η εύρεση πιθανών ανοιχτών πορτών από μεριά του κάθε χρήστη, ώστε να μπορούν να αποφευχθούν τέτοιου είδους ενέργειες.
    Το εργαλείο για καθορισμό ανοιχτών πορτών που χρησιμοποιήθηκε αποτελεί το nmap και χρησιμοποιήθηκε το Module Command για την εκτέλεση των απαραίτητων εντολών, η εντολή Delegate_to για εκτέλεση της εντολής στο μηχάνημα λειτουργίας του Ansible καθώς και το Module Debug για εμφάνιση και ανάλυση των αποτελεσμάτων. Οι εντολές που εκτελέστηκαν είναι οι εξής (όπου καλέσθηκαν οι μεταβλητές των IP διευθύνσεων κάθε μηχανήματος όπως καθορίστηκαν παραπάνω):

    $ nmap -v -sT '{{ IP }}' → TCP connect scan
    $ nmap -v -sS '{{ IP }}' → TCP SYN scan για πιο λεπτομερή αποτελέσματα.

12. Εγκατάσταση και ρύθμιση εργαλείου παρακολούθησης του συστήματος. Οι εφαρμογές και υπηρεσίες κατά την χρήση τους, δημιουργούν διάφορα αρχεία (Log files) για την παρακολούθηση της κινητικότητας και των δραστηριοτήτων που λαμβάνουν μέρος οποιαδήποτε στιγμή. Τα αρχεία αυτά παίζουν ιδιαίτερα σημαντικό ρόλο στην κατανόηση και ανάλυση γεγονότων που μπορεί να συνέβησαν και αφορούν την απόδοση αλλά και την ανάκτηση μέρους ή και ολόκληρου πλήθους δεδομένων που μπορεί να χάθηκαν. Τέλος, συμβάλουν ενεργά στην αντιμετώπιση μελλοντικών γεγονότων καθώς και στην

οργάνωση πιθανών στρατηγικών για τροποποιήσεις των συστημάτων. Αποτελεί σημαντικό βήμα η εγκατάσταση και χρήση τέτοιων εργαλείων, για καλύτερη παρακολούθηση και ανάλυση των δεδομένων για πιθανά ζητήματα ασφαλείας. Καθώς τα αρχεία log αποτελούν εξαιρετικά λεπτομερή και με μεγάλο πλήθος περιττών πληροφοριών αρχεία, είναι απαραίτητη η χρήση εργαλείων για την καλύτερη ανάλυσή τους. Υπάρχει μεγάλη ποικιλία εργαλείων για την συγκεκριμένη χρήση, όπως το Logwatch, Graylog2, Logstash και Logcheck, όμως στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε το Logwatch.

Μετά την εγκατάσταση του εργαλείου Logwatch με χρήση της Apt Module, πρέπει να γίνουν κάποιες τροποποιήσεις στο αρχείο ρύθμισης του Logwatch ώστε να αποστέλλεται ηλεκτρονικό μήνυμα στον διαχειριστή με επιλεγμένο ποσοστό λεπτομερειών και χρονικής περιόδου. Με την Replace Module, γίνονται όλες οι απαραίτητες μετατροπές στο αρχείο ρύθμισης του Logwatch ώστε να αποστέλλεται ηλεκτρονικό μήνυμα στον κατάλληλο χρήστη, καλώντας το με αρχείο μεταβλητής που δημιουργήθηκε στο συγκεκριμένο Role, λεπτομέρειας του log αρχείου καθώς και το εύρος της χρονικής περιόδου. Ένα παράδειγμα αποτελεί το εξής:

```
- name: Configure Logwatch
  replace:
    name: /usr/share/logwatch/default.conf/logwatch.conf
    regexp: 'Detail = Low'
    replace: 'Detail = Med'
```

13. Αναζήτηση Rootkits. Το Rootkit αποτελεί κακόβουλη συλλογή εφαρμογών και προγραμμάτων που έχουν σχεδιαστεί ώστε να επιτρέπουν μη εξουσιοδοτημένη είσοδο σε κάποιο υπολογιστή ή δίκτυο. Κάποιος πιθανός επιτιθέμενος εγκαθιστεί ένα Rootkit αποκτώντας πρόσβαση επιπέδου χρήστη. Η εγκατάσταση αυτή πραγματοποιείται με εκμετάλλευση κάποιας γνωστής ευπάθειας ή με αποκρυπτογράφηση κάποιου κωδικού εισόδου στο σύστημα. Όταν η διαδικασία της εγκατάστασης τελειώσει, ο επιτιθέμενος αποκτά πρόσβαση με επιπλέον προνόμια, κάτι που αποτελεί μεγάλη παραβίαση της ασφάλειας στο σύστημα. Ανάμεσα στα πολλά open-source προγράμματα αναζήτησης Rootkits, όπως για παράδειγμα το Rkhunter, επιλέχθηκε και χρησιμοποιήθηκε το Chkrootkit.

    Η διαδικασία ξεκινάει με την εγκατάσταση του Chkrootkit χρησιμοποιώντας το Apt Module, όπως και στα προηγούμενα παραδείγματα. Στην συνέχεια θα χρησιμοποιηθεί η

Template Module η οποία χρησιμοποιείται για την αντικατάσταση και αναβάθμιση ορισμένων αρχείων ρύθμισης, έπειτα από την εγκατάσταση κάποιου προγράμματος. Με την χρήση του Module αυτού, καλείται κάποιο αρχείο Template που έχει δημιουργηθεί ώστε να αντικαταστήσει κάποιο άλλο αρχείο ρύθμισης. Πιο συγκεκριμένα:

```
- name: Update Chkrootkit configuration
  template:
    src: chkrootkit.conf.j2
    dest: /etc/chkrootkit/chkrootkit.conf
    owner: root
    group: root
    mode: 0644
```

Στο Template αρχείο που δημιουργήθηκε αναφέρονται σημαντικοί τομείς της ρύθμισης του συγκεκριμένου εργαλείου, όπως η ηλεκτρονική διεύθυνση αποστολής των αποτελεσμάτων εύρεσης κάποιου κακόβουλου προγράμματος και η συχνότητα αποστολής των ηλεκτρονικών μηνυμάτων.

14. Intrusion Detection System (IDS). Τελευταίο και πολύ σημαντικό βήμα στην διαδικασία της ασφάλισης των απομακρυσμένων χρηστών μέσω του Ansible, αποτελεί η εγκατάσταση κάποιου Intrusion Detection System (IDS). Τα εργαλεία αυτά αποτελούν λογισμικό που παρακολουθεί τους χρήστες ή και τα δίκτυα για παραβιάσεις ασφάλειας και κακόβουλης δραστηριότητας. Οποιαδήποτε ύποπτη δραστηριότητα καταγραφεί, αναφέρεται στον διαχειριστή του συστήματος. Υπάρχει μεγάλη ποικιλία open-source Intrusion Detection εργαλείων όπως το Snort, AIDE, Suricata, Bro, Kismet κ.α. Για τις ανάγκες της συγκεκριμένης διατριβής χρησιμοποιήθηκε το εργαλείο Psad.
    Μετά την εγκατάσταση του με την Apt Module, στο νέο δημιουργημένο Role Intrusion, χρησιμοποιείται η Template Module για την αναβάθμιση του αρχείου ρύθμισης του psad. Τέλος, χρησιμοποιείται αρχείο Handler για την επανεκκίνηση του εργαλείου αυτού, για την εξασφάλιση της σωστής λειτουργίας του.
    Το αρχείο Template το οποίο χρησιμοποιήθηκε για την λειτουργία του εργαλείου αυτού, πρέπει να περιλαμβάνει πληροφορίες για τον χρήστη καθώς και την διεύθυνση ηλεκτρονικού ταχυδρομείου (που καλούνται ως μεταβλητές από το Ansible), πληροφορίες για τα επίπεδα επικινδυνότητας καθώς και πληροφορίες για το ελάχιστο

επίπεδο επικινδυνότητας που πρέπει να επιτευχθεί ώστε να γίνει ενημέρωση του διαχειριστή. Για παράδειγμα:

```
# Danger levels.

DANGER_LEVEL1       5;
DANGER_LEVEL2       15;
DANGER_LEVEL3       150;
DANGER_LEVEL4       1500;
DANGER_LEVEL5       10000;

# Controls psad logging and email alerts.

MIN_DANGER_LEVEL        1;

# Apllies only for email alerts.

EMAIL_ALERT_DANGER_LEVEL  1;
```

Κεφάλαιο 4
Ανίχνευση Ευπαθειών

Στην συγκεκριμένη διατριβή η μεθοδολογία που ακολουθήθηκε, όπως αναλύθηκε παραπάνω, ήταν η παρουσίαση τρόπων διασφάλισης της ασφάλειας ενός εικονικού περιβάλλοντος Υπολογιστικού σύννεφου με την χρήση εργαλείων αυτοματοποίησης, ώστε οι απομακρυσμένοι εξυπηρετητές να διαμορφωθούν κατάλληλα, μέσα στο Υπολογιστικό σύννεφο και τελικά να ασφαλιστούν. Για τις ανάγκες της εργασίας, χρησιμοποιήθηκε για την δημιουργία του εικονικού περιβάλλοντος το εργαλείο Vagrant και το εργαλείο Ansible για τα βήματα ασφάλισης του περιβάλλοντος αυτού.

Κάθε περιβάλλον Υπολογιστικού σύννεφου θα πρέπει να διαθέτει συγκεκριμένα χαρακτηριστικά ώστε να θεωρηθεί ασφαλές περιβάλλον εργασίας και χρήσης. Είναι απαραίτητη η διαφύλαξη της αξιοπιστίας, της διαθεσιμότητας, αυθεντικότητας , εξουσιοδότησης καθώς και της εμπιστευτικότητας των πληροφοριών και δεδομένων.

Κάθε πιθανός κακόβουλος χρήστης μπορεί να εντοπίσει με διάφορες τεχνικές, σοβαρές ή μη ευπάθειες ώστε να τις εκμεταλλευτεί και να καταφέρει να οργανώσει μία επίθεση και στο χειρότερο σενάριο να καταφέρει να την θέσει σε εφαρμογή.

Όπως αναφέρθηκε στην μεθοδολογία, εγκαταστάθηκαν αρκετά εργαλεία monitoring ώστε ο διαχειριστής κάθε συστήματος να μπορεί να εντοπίζει μόνος του πιθανά κενά σημεία στην προστασία του συστήματος του αλλά και εργαλεία ανίχνευσης πιθανών επιθέσεων.

Πολύ σημαντικό βήμα αποτελεί η καταγραφή των υπηρεσιών και συνδέσεων που λαμβάνουν μέρος και βρίσκονται σε λειτουργία οποιαδήποτε στιγμή, χρησιμοποιώντας κάποιο κατάλληλο εργαλείο. Σε περίπτωση εύρεσης ανοιχτής σύνδεσης από κάποια μη αναγνωρίσιμη IP διεύθυνση ή πόρτα, είναι αναγκαία η λήψη περισσότερων μέτρων για την εγγύηση της ασφάλειας του συστήματος.

Εφόσον υπάρχουν ανοιχτές και εύκολα προσβάσιμες δημόσιες πόρτες, οποιοσδήποτε κακόβουλος χρήστης, έχει την δυνατότητα να ανακαλύψει εύκολα πιθανές υπηρεσίες που λειτουργούν σε ανοιχτές πόρτες και έτσι να σχεδιάσει καλύτερα την επίθεση του. Αν οποιαδήποτε υπηρεσία παρουσιάσει κάποια οποιαδήποτε ευπάθεια που μπορεί να ανακαλυφθεί και να χρησιμοποιηθεί κατάλληλα για την οργάνωση κάποιας επίθεσης, η συγκεκριμένη επίθεση θα λάβει μέρος στην πόρτα στην οποία έχει ανατεθεί. Αποτελεί λοιπόν, βασική ανάγκη η εύρεση πιθανών ανοιχτών πορτών ώστε να αποφυγούν τέτοιου είδους ενέργειες.

Για τις ανάγκες της συγκεκριμένης διατριβής χρησιμοποιήθηκαν τα εργαλεία Netstat για την εύρεση υπηρεσιών και συνδέσεων και το nmap για την καταγραφή των ανοιχτών πορτών. Παραδείγματα χρήσης τους σε έναν από τους απομακρυσμένους χρήστες που συντελούν το εικονικό περιβάλλον Υπολογιστικού σύννεφου, παρουσιάζονται στις Εικόνες 15 και 16.

Οποιαδήποτε πληροφορία αντληθεί από κακόβουλους χρήστες, που αφορούν τα παραπάνω μπορεί να χρησιμοποιηθεί κακόβουλα και να δημιουργήσει ζητήματα ασφάλειας που αφορούν τα Ανασφαλή Interfaces και API, τις Κοινόχρηστες Τεχνολογίες που παρέχει το Υπολογιστικό σύννεφο καθώς και την Ασφάλεια των Δεδομένων και Πληροφοριών.

Η ασφάλεια των δεδομένων, όπως έχει αναφερθεί αφορά τις βασικές αρχές διασφάλισης των δεδομένων και των πληροφοριών που αφορούν την αξιοπιστία, εμπιστευτικότητα, εξουσιοδότηση, αυθεντικότητα και διαθεσιμότητα των δεδομένων. Αποτελεί ευθύνη κάθε παρόχου αλλά και κάθε χρήστη ξεχωριστά, να διασφαλίσει την προστασία των αποθηκευμένων δεδομένων από παραβιάσεις ασφάλειας, λόγω ευπαθειών σε υπηρεσίες ή εφαρμογές ή ακόμα και από επιθέσεις κακόβουλων χρηστών. Οι παραβιάσεις αυτές μπορεί να είναι αποτέλεσμα του

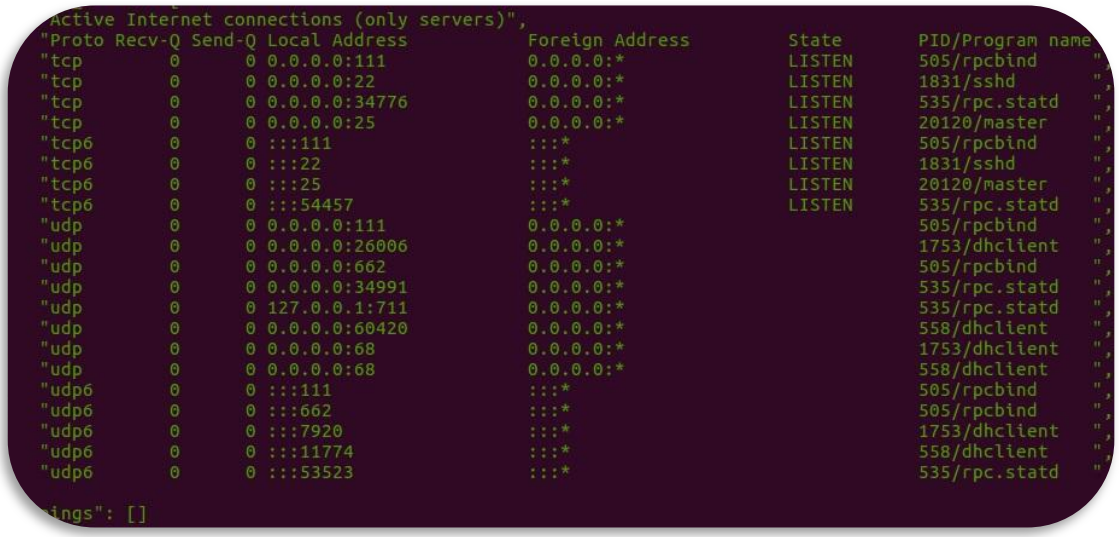
καθορισμού των ανοικτών πορτών καθώς και των εν λειτουργία υπηρεσιών, όπου κάποιος κακόβουλος χρήστης μπορεί να εκμεταλλευτεί για καλύτερη οργάνωση της διαδικασίας επίθεσής του.

Τα Software Interfaces και Application Programming Interfaces καθώς αποτελούν την βάση για την διαχείριση των διαθέσιμων υπηρεσιών εκ μέρους των παρόχων, οποιοδήποτε πρόβλημα σε αυτά δημιουργεί σοβαρά ζητήματα ασφάλειας.

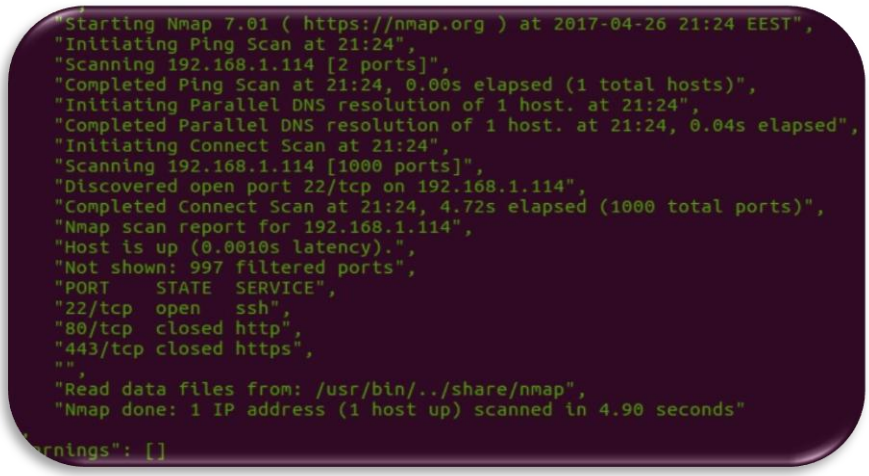
Τέλος, ενώ οι υπηρεσίες που διαμοιράζονται μεταξύ χρηστών, ως χαρακτηριστικό του Υπολογιστικού Σύννεφου, αποτελούν ένα από τα μεγαλύτερα πλεονεκτήματα χρήσης του Cloud ταυτόχρονα αποτελούν και ένα από τα κυριότερα ζητήματα εγγύησης της ασφάλειας των πληροφοριών και δεδομένων.

Στην συνέχεια, κάθε ένας απομακρυσμένος χρήστης του εικονικού Cloud περιβάλλοντος σαρώθηκε και εξετάστηκε από δύο προγράμματα ανίχνευσης ευπαθειών για εύρεση πιθανών ύποπτων αδυναμιών που χρήζουν προσοχής.

Τα προγράμματα που εφαρμόστηκαν αποτελούν το Nessus και OpenVas και χρησιμοποιήθηκαν σε κάθε έναν από τους απομακρυσμένους χρήστες του υλοποιημένου εικονικού περιβάλλοντος Υπολογιστικού σύννεφου. Παρ'όλα αυτά, τα αποτελέσματα τα οποία θα παρουσιαστούν υλοποιήθηκαν σε έναν απομακρυσμένο χρήστη που αντιπροσωπεύει το υλοποιημένο αυτό περιβάλλον.



Εικόνα 16. Χρήση του εργαλείου netstat.



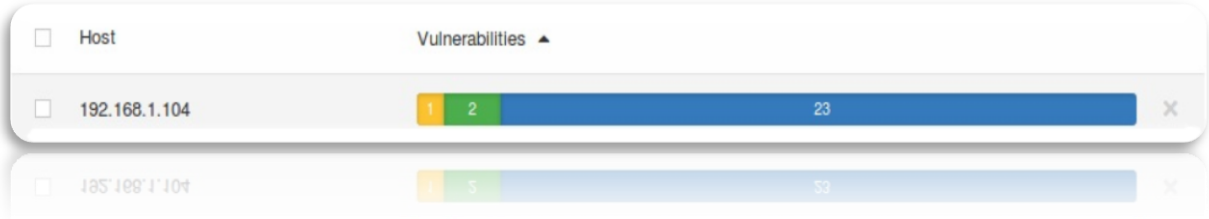
Εικόνα 17. Χρήση του εργαλείου nmap.

4.1 Nessus

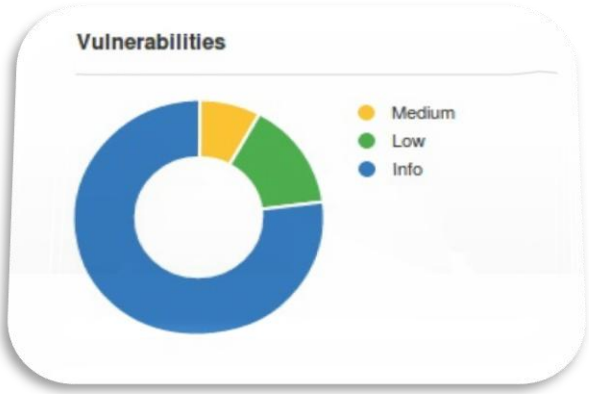
Το εργαλείο Nessus (https://www.tenable.com/products/nessus-vulnerability-scanner) αποτελεί εργαλείο ανίχνευσης και διαχείρισης ευπαθειών και πιθανών επιθέσεων. Καλή πρακτική για χρήστες αλλά και οργανισμούς είναι η χρήση τέτοιου είδους εργαλείων, ώστε να αποφεύγονται επιθέσεις από κακόβουλους χρήστες, που αφορούν την Ασφάλεια και την Ανάκτηση των δεδομένων καθώς και τις Κοινόχρηστες τεχνολογίες που διαθέτονται μέσω του περιβάλλοντος Υπολογιστικού σύννεφου.

Έπειτα από την εγκατάσταση του Nessus, το εργαλείο αυτό εφαρμόστηκε στο υλοποιημένο περιβάλλον Cloud. Το Nessus δίνει την δυνατότητα διάφορων μορφών σάρωσης του συστήματος δίνοντας βάση στο ποσοστό της λεπτομέρειας των αποτελεσμάτων. Για τις ανάγκες της συγκεκριμένης εργασίας, υλοποιήθηκε ένα αρκετά λεπτομερές σύστημα σάρωσης του συστήματος (Advance Network Scan για κάθε απομακρυσμένο χρήστη).

Όπως παρουσιάζεται και στις Εικόνες 18 και 19, οι ευπάθειες που μπορεί να ανακαλυφθούν διαχωρίζονται από επίπεδο σοβαρότητας και κινδύνου στο σύστημα. Στην περίπτωση του υλοποιημένου περιβάλλοντος παρατηρούνται: μία ευπάθεια με μεσαίο επίπεδο σοβαρότητας, δύο με χαμηλό επίπεδο σοβαρότητας και 23 αναφορές και πληροφορίες που αφορούν το σύστημα. Κάθε μία από αυτές τις παρατηρήσεις αποτελούν πληροφορίες και ευπάθειες που μπορεί να χρησιμοποιηθούν από οποιονδήποτε που έχει την δυνατότητα και θέληση για επίθεση, με σοβαρά και επικίνδυνα αποτελέσματα.



Εικόνα 18. Υλοποίηση Nessus Scan για πιθανές ευπάθειες.



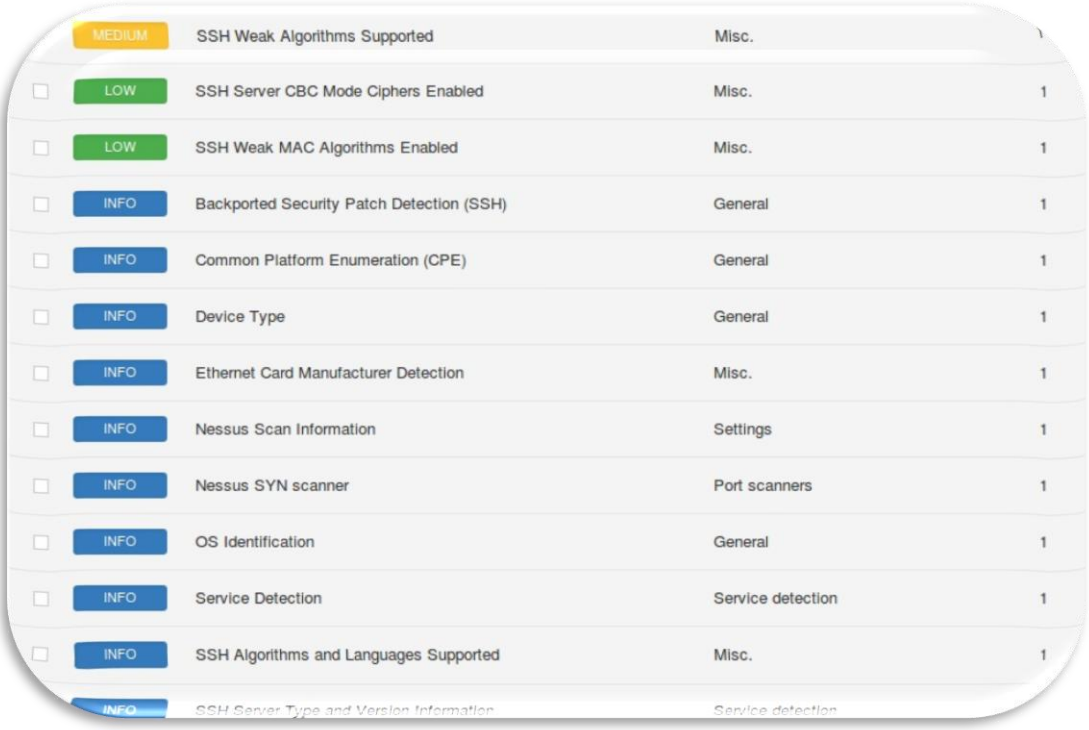
Εικόνα 19. Επίπεδα σοβαρότητας και επικινδυνότητας των ευπαθειών στο σύστημα.

Πιο συγκεκριμένα, όπως παρουσιάζεται στην Εικόνα 20, η ευπάθεια μεσαίου μεγέθους σοβαρότητας αποτελεί η SSH Weak Algorithms Supported και οι δύο με χαμηλού επιπέδου σοβαρότητας οι SSH Server CBC Mode Ciphers Enabled και SSH Weak MAC Algorithms Supported. Οι παραπάνω αδυναμίες αναφέρονται σε ζητήματα ασφάλειας στο Υπολογιστικό Σύννεφο που αφορούν τον Έλεγχο πρόσβασης, την Ασφάλεια καθώς και την Τοποθεσία των δεδομένων.

Όλα τα ευαίσθητα δεδομένα και πληροφορίες που επεξεργάζονται εκτός του οργανισμού ή του χώρου του ιδιώτη παρουσιάζουν μεγάλη επικινδυνότητα, καθώς εξωτερικοί χρήστες μπορούν να παρακάμψουν όλους τους φυσικούς και λογικούς ελέγχους ώστε να παραβιάσουν το σύστημα. Αποτελεί ευθύνη κάθε παρόχου αλλά και κάθε χρήστη ξεχωριστά, να εξασφαλίσει την προστασία των αποθηκευμένων δεδομένων από παραβιάσεις ασφάλειας, λόγω ευπαθειών σε υπηρεσίες ή εφαρμογές ή ακόμα και από επιθέσεις κακόβουλων χρηστών.

Στην συνέχεια, παρουσιάζονται πληροφορίες του συστήματος οι οποίες αφορούν το λειτουργικό σύστημα το οποίο χρησιμοποιείται, εφαρμογές και υπηρεσίες που λειτουργούν καθώς και άλλες γενικές πληροφορίες που αφορούν το συγκεκριμένο μηχάνημα. Οι πληροφορίες αυτές αναφέρονται στα ζητήματα ασφάλειας που αφορούν τα Ανασφαλή Interfaces και Application

Programming Interfaces καθώς και τα Ζητήματα Κοινόχρηστων Τεχνολογιών. Οποιοδήποτε πρόβλημα στα Software Interfaces που χρησιμοποιούνται για την διάθεση των υπηρεσιών στους χρήστες του Cloud καθώς και τις κοινόχρηστες τεχνολογίες μεταξύ των χρηστών, δημιουργεί σημαντικά ζητήματα ασφάλειας. Είναι απαραίτητη λοιπόν η γνώση και ανάλυση όλων των διαθέσιμων πληροφοριών που μπορεί κάποιος επιτιθέμενος να εκμεταλλευθεί κακόβουλα.



Εικόνα 20. Αναλυτικά αποτελέσματα Nessus Scan.

Το Nessus δίνει αναλυτική επεξήγηση αλλά και τρόπους επίλυσης και διαχείρισης όλων των πιθανών ευπαθειών, κάτι το οποίο διευκολύνει την διαδικασία οργάνωσης στρατηγικών και βημάτων για βελτίωση της λειτουργίας και ασφάλειας των συστημάτων.

Πιο συγκεκριμένα, όσο αφορά την ευπάθεια SSH Weak Algorithms Supported, προτείνεται η αφαίρεση των αδύναμων αλγορίθμων κρυπτογράφησης καθώς θεωρούνται επικίνδυνοι για την ασφάλεια του συστήματος. Για την ευπάθεια SSH Weak MAC Algorithms Supported, προτείνεται η απενεργοποίηση του MD5 και 96-bit MAC καθώς θεωρούνται αδύναμοι αλγόριθμοι για την ασφάλεια του SSH Server. Τέλος, όσο αφορά την ευπάθεια SSH Server CBC Mode Ciphers Enabled, καλή τακτική θεωρείται η απενεργοποίηση του CBC τρόπου κρυπτογράφησης, καθώς κάποιος πιθανός επιτιθέμενος μπορεί να εκμεταλλευθεί τον συγκεκριμένο τρόπο ώστε να αποκρυπτογραφήσει σημαντικές πληροφορίες για τον χρήστη.

4.2 OpenVas

Ένα δεύτερο εργαλείο ανίχνευσης, ανάλυσης και διαχείρισης πιθανών ευπαθειών και πληροφοριών του συστήματος αποτελεί το OpenVas Vunerability Scanner (http://www.openvas.org/). Μετά την εγκατάσταση του προγράμματος αυτού, υλοποιήθηκε σάρωση του συστήματος κάθε ενός από τους απομακρυσμένους χρήστες που αποτελούν το υλοποιημένο περιβάλλον Cloud. Για τις ανάγκες της συγκεκριμένης εργασίας, υλοποιήθηκε ένα αρκετά λεπτομερές σύστημα σάρωσης του συστήματος κάθε χρήστη (Full and Deep Ultimate Scan για κάθε απομακρυσμένο χρήστη). Τα αποτελέσματα της υλοποίησης της σάρωσης αυτής παρουσιάζονται στην Εικόνα 21.

Vulnerability	Severity	QoD	Host	Location	Created
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.168.1.109	general/tcp	Thu Mar 2 15:19:08 2017
Check open ports	0.0 (Log)	95%	192.168.1.109	22/tcp	Thu Mar 2 15:33:54 2017
Record route	0.0 (Log)	99%	192.168.1.109	general/icmp	Thu Mar 2 15:26:24 2017
Traceroute	0.0 (Log)	80%	192.168.1.109	general/tcp	Thu Mar 2 15:20:05 2017
TCP timestamps	2.6 (Low)	80%	192.168.1.109	general/tcp	Thu Mar 2 15:22:34 2017
CPE Inventory	0.0 (Log)	80%	192.168.1.109	general/CPE-T	Thu Mar 2 15:33:53 2017

Εικόνα 21. Υλοποίηση του OpenVas Scan.

Όπως παρατηρείται, αναλύονται πληροφορίες για το σύστημα όπως για παράδειγμα το είδος λειτουργικού συστήματος, πιθανές ανοικτές πόρτες και υπηρεσίες και εφαρμογές σε λειτουργία και κάθε αποτέλεσμα της σάρωσης αυτής διαθέτει επίπεδο σοβαρότητας και επικινδυνότητας. Ανάλυση της ευπάθειας που παρουσιάζεται με χαμηλό επίπεδο σοβαρότητας (Severity 2.6 Low) αναλύεται στην Εικόνα 22.

...erability	Severity	QoD	Host	Location	Actio...
TCP timestamps	2.6 (Low)	80%	192.168.1.109	general/tcp	

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 4350776
Paket 2: 4351058

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

...e also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Εικόνα 22. Ανάλυση και επίλυση ευπάθειας TCP timestamps.

Οι αδυναμίες που εμφανίζονται στο σύστημα αφορούν τα ζητήματα ασφάλειας που εμφανίζονται σε Ανασφαλή Software Interfaces, Κοινόχρηστες Τεχνολογίες, Έλεγχο Πρόσβασης καθώς και την Ασφάλεια και Τοποθεσία των αποθηκευμένων δεδομένων και πληροφοριών, όπως έχει αναλυθεί και παραπάνω.

Κεφάλαιο 5
Επίλογος

Το Cloud Computing, αποτελεί μοντέλο το οποίο δίνει την δυνατότητα δημιουργίας πρακτικής, ελαστικής και κατ'απαίτηση διαδικτυακής πρόσβασης σε μία κοινόχρηστη ομάδα υπολογιστικών πόρων. Οι πόροι αυτοί μπορεί να είναι δίκτυα, διακομιστές, αποθηκευτικός χώρος, εφαρμογές καθώς και υπηρεσίες, οι οποίες παραδίδονται διαμέσου του διαδικτύου και αφορούν το hardware, λογισμικό, δεδομένα και μεγάλο αριθμό εφαρμογών που βρίσκονται αποθηκευμένα στα data centers.

Το Υπολογιστικό σύννεφο αποτελεί μία νέα αναδυόμενη τεχνολογία, η οποία συνδέεται με την έννοια του Grid Computing καθώς και με άλλες συναφή τεχνολογίες όπως το Utility και Distributed Computing.

Κάποια από τα βασικά χαρακτηριστικά του Υπολογιστικού σύννεφου είναι η κατ'απαίτηση εξυπηρέτηση που παρέχει, η ευρεία σύνδεση στο διαδίκτυο, η εύκολη πρόσβαση σε ομάδες υπολογιστικών πόρων, η ραγδαία ελαστικότητα και τέλος οι οριοθετημένες διαθέσιμες υπηρεσίες που παρέχονται. Οι υπηρεσίες που παρέχονται στους χρήστες μπορούν να διαχωριστούν στα μοντέλα Software-as-a-Service (SaaS), Platform-as-a-Service (Paas) και Infrastructure-as-a-Service (IaaS) για μεγαλύτερη ευελιξία καθώς και για περισσότερα οικονομικά οφέλη. Επίσης, το Υπολογιστικό σύννεφο μπορεί να διαχωριστεί σε συγκεκριμένα

μοντέλα ανάπτυξης όπως το Private Cloud, Public Cloud, Community και Hybrid Cloud για την βελτίωση των εφαρμογών, υπηρεσιών, υποδομής καθώς και οποιονδήποτε άλλων πόρων που παρέχονται μέσω Cloud.

Η δημοτικότητα των πλατφόρμων Υπολογιστικού σύννεφου κατά την διάρκεια των τελευταίων ετών, έχει αυξηθεί καθώς ο αριθμός των οργανισμών και εταιριών της Τεχνολογίας των Πληροφοριών που χρησιμοποιεί και παρέχει υπηρεσίες τέτοιου είδους στις συγκεκριμένες πλατφόρμες, ολοένα και αυξάνεται.

Η διαρκώς αυξανόμενη χρήση του Cloud απορρέει από την μεγάλη ποικιλία των υπηρεσιών που παρέχονται καθώς και από τα πολλά οφέλη της χρήσης του. Κάποια από τα σημαντικότερα πλεονεκτήματα της χρήσης των αρχιτεκτονικών Υπολογιστικού σύννεφου είναι το χαμηλό κόστος, το αυξημένο πλήθος αποθηκευμένων δεδομένων, η δυνατότητα ανάκτησης δεδομένων, η προσβασιμότητα καθώς και η βελτίωση των υπηρεσιών.

Παράλληλα από τα πολλά οφέλη της χρήσης του Υπολογιστικού σύννεφου, υπάρχουν και κάποια μειονεκτήματα που δημιουργούν περιορισμούς αλλά και σοβαρά προβλήματα. Ένα από αυτά αποτελεί το πρόβλημα της προσβασιμότητας, καθώς σε περιπτώσεις αδυναμίας σύνδεσης στο διαδίκτυο ή σε περιπτώσεις αργής σύνδεσης, η πρόσβαση καθιστάται δύσκολη ή ακόμα και αδύνατη.

Ένα μεγάλο θέμα στην χρήση του Υπολογιστικού σύννεφου είναι τα ζητήματα ασφάλειας που προκύπτουν. Καθώς δεν μπορεί να υπάρχει μέγιστη και απόλυτη ασφάλεια της εμπιστευτικότητας των δεδομένων, κάποιος κακόβουλος χρήστης έχοντας πρόσβαση σε τόσο μεγάλο πλήθος δεδομένων του δίνεται η δυνατότητα μίας επιτυχημένης επίθεσης σε κάποιο σύστημα, παραβιάζοντας έτσι κάποια από τα βασικά χαρακτηριστικά της ασφάλειας που αποτελούν η εμπιστευτικότητα, η ακεραιότητα καθώς και η διαθεσιμότητα των δεδομένων. Οι απειλές ασφάλειας αφορούν δεδομένα, ευαίσθητες και απόρρητες πληροφορίες, δίκτυα και πλήθος ευπαθειών. Οι ευπάθειες αυτές μπορούν εύκολα να εκμεταλλευθούν από κακόβουλους χρήστες και να αποτελέσουν σοβαρό ζήτημα σε οργανισμούς και καταναλωτές.

Κάποιες από τις πιο σημαντικές επιθέσεις σε πλατφόρμες Cloud αποτελούν οι εξής: Distributed Denial of Service Attack (DDos), VM Denial of Service Attacks (VM Dos), Keystroke Timing Attacks, Side-Channel Attacks, Hypervisor Attacks, Cloud Malware Injection Attacks, Fraudulent Resource Consumption Attacks, Phishing και Ransomware.

Τα κυριότερα ζητήματα ασφάλειας που απασχολούν τους χρήστες και πάροχους πλατφόρμων Υπολογιστικού σύννεφου είναι ο έλεγχος πρόσβασης, η ανάκτηση των δεδομένων, η ασφάλεια των δεδομένων, η συμμόρφωση χρηστών στις καθορισμένες ρυθμίσεις, η τοποθεσία των δεδομένων, τα ανασφαλή Interfaces και API (Application Programming Interfaces) και τα ζητήματα κοινόχρηστων τεχνολογιών. Εφόσον τα ζητήματα αυτά εμφανίζονταιι συχνά και πολλές φορές με σοβαρές επιπτώσεις στα συστήματα, παραβιάζοντας τα βασικά χαρακτηριστικά της ασφάλειας, οι χρήστες καθώς και οι πάροχοι είναι αναγκαίο να λάβουν δραστικά μέτρα.

Στην συγκεκριμένη εργασία παρουσιάστηκαν τρόποι εγγύησης της ασφάλειας ενός εικονικού υλοποιημένου περιβάλλοντος Υπολογιστικού σύννεφου, με την χρήση εργαλείων αυτοματοποίησης. Η χρήση της διαδικασίας της αυτοματοποίησης συμπεριλαμβάνει όλες τις τεχνικές με τις οποίες οι υπηρεσίες διαθέτονται αυτόματα από το υπολογιστικό σύστημα χωρίς την συμβολή του χρήστη ή οργανισμού.

Παρουσιάστηκαν και αναλύθηκαν τα πολλά οφέλη χρήσης εργαλείων αυτοματοποίησης όπως η λιγότερη κατανάλωση χρόνου από την μεριά του κάθε χρήστη αλλά και οργανισμού, η βελτίωση της συνεργασίας και της παραγωγικότητας μεταξύ των μελών που χρησιμοποιούν πλατφόρμες Υπολογιστικού σύννεφου, η εξάλειψη των πιθανών επαναλαμβανόμενων διαδικασιών, η μείωση των λαθών, η μείωση της πολυπλοκότητας των διαδικασιών, η αύξηση των καινοτόμων πόρων και η ευκολότερη επιβολή των διάφορων πολιτικών οργανισμών ή εταιριών.

Η μεθοδολογία που ακολουθήθηκε ήταν μέσω της χρήσης ενός εικονικού περιβάλλοντος δημιουργημένου με το εργαλείο αυτοματοποίησης Vagrant. Στην συνέχεια οι απομακρυσμένοι χρήστες διαμορφώθηκαν κατάλληλα, μέσα στο υλοποιημένο Υπολογιστικό σύννεφο, μέσω του εργαλείου αυτοματοποίησης Ansible.

Στην συνέχεια χρησιμοποιήθηκαν εργαλεία ανίχνευσης, ανάλυσης καθώς και διαχείρισης ευπαθειών στον κάθε χρήστη που αντιπροσωπεύει το υλοποιημένο εικονικό Cloud Computing σύστημα, για εύρεση πιθανών επικίνδυνων αδυναμιών που μπορεί να εκμεταλλευθούν κακόβουλοι χρήστες προς όφελός τους. Τα εργαλεία αυτά δίνουν την δυνατότητα λεπτομερούς σάρωσης των συστημάτων και κατάταξης των ευπαθειών με βαθμό επικινδυνότητας. Στα πλαίσια της διατριβής χρησιμοποιήθηκαν τα εργαλεία Nessus Vulnerability Scanner και OpenVas.

Στην εργασία αυτή, όπως αναφέρθηκε, παρουσιάστηκαν τρόποι ασφάλισης των χρηστών ενός εικονικού Υπολογιστικού σύννεφου σύμφωνα με τα ζητήματα ασφάλειας που παρουσιάζονται, εκμεταλλευόμενοι τα πολλαπλά οφέλη χρήσης εργαλείων αυτοματοποίησης.

1. Έλεγχος πρόσβασης-Ασφάλεια των δεδομένων-Τοποθεσία των δεδομένων.

Όσο αφορά τα ζητήματα ασφάλειας που αφορούν τον έλεγχο πρόσβασης και την ασφάλεια των δεδομένων, στις πλατφόρμες Υπολογιστικού σύννεφου είναι απαραίτητη η λήψη δραστικών βημάτων. Όλα τα ευαίσθητα δεδομένα και πληροφορίες που επεξεργάζονται εκτός του οργανισμού ή του χώρου του ιδιώτη παρουσιάζουν μεγάλη επικινδυνότητα, καθώς εξωτερικοί χρήστες μπορούν να παρακάμψουν όλους τους φυσικούς και λογικούς ελέγχους ώστε να παραβιάσουν το σύστημα. Αποτελεί ευθύνη κάθε παρόχου αλλά και κάθε χρήστη ξεχωριστά, να εξασφαλίσει την προστασία των αποθηκευμένων δεδομένων από παραβιάσεις ασφάλειας, λόγω ευπαθειών σε υπηρεσίες ή εφαρμογές ή ακόμα και από επιθέσεις κακόβουλων χρηστών. Τα μέτρα που θα πρέπει να ληφθούν, αφορούν κυρίως στην κρυπτογράφηση και στην προστασία της ακεραιότητας των αποθηκευμένων δεδομένων.

Είναι απαραίτητη η χρήση και η δημιουργία λογαριασμών με κρυπτογραφημένους κωδικούς πρόσβασης για προστασία της ακεραιότητας και αυθεντικότητας των δεδομένων καθώς και η χρήση SSH κλειδιών για κάθε ένα δημιουργημένο λογαριασμό. Με την χρήση και δημιουργία κλειδιών, εγγυάται η ασφάλεια του συστήματος και κάθε πιθανή επίθεση Brute-force καθιστάται δυσκολότερη.

Σωστή τακτική ασφάλισης των συστημάτων, επίσης, αποτελεί η εγκατάσταση SSL πιστοποιητικών για κρυπτογράφηση της κίνησης επιπέδου εφαρμογών, καθώς με την χρήση των ψηφιακών πιστοποιητικών εξασφαλίζεται η ακεραιότητα και αυθεντικότητα των ευαίσθητων δεδομένων που μεταφέρονται και αποστέλλονται μέσω του διαδικτύου.

Η χρήση κάποιου εργαλείου firewall είναι απαραίτητη για την προστασία των συστημάτων από ανεπιθύμητη εισχώρηση σε αυτά καθώς και από επιθέσεις Denial of Service (Dos). Υπάρχει μεγάλο πλήθος εργαλείων firewall όπως τα Ip Tables, Ufw, IPCop Firewall, ShoreWall και IpFire. Για τις ανάγκες της συγκεκριμένης εργασίας χρησιμοποιήθηκε το Ufw εργαλείο firewall.

Τέλος, συνιστάται απενεργοποίηση του IPv6 πρωτοκόλλου ή η ρύθμισή του μέσω ενός firewall εργαλείου καθώς και η αποφυγή IP Spoofing ώστε να αποφυγεί η συγκάλυψη των διευθύνσεων IP σε περίπτωση μη εξουσιοδοτημένης εισόδου στο σύστημα.

2. Ανάκτηση των δεδομένων-Τοποθεσία των δεδομένων.

Καθώς τα δεδομένα δεν βρίσκονται αποθηκευμένα στις εγκαταστάσεις του οργανισμού ή του χρήστη, η ύπαρξη τους αλλά και η διαθεσιμότητα τους σε περίπτωση καταστροφής αμφισβητείται. Οι πάροχοι υπηρεσιών Υπολογιστικού σύννεφου πρέπει να διατηρούν την ασφάλεια των δεδομένων, καθώς οι ίδιοι οι πελάτες δεν μπορούν να γνωρίζουν την ακριβή φυσική τοποθεσία τους. Οι οργανισμοί από την μεριά τους, θα πρέπει να είναι ενημερωμένοι για τους κανονισμούς και νόμους που ισχύουν καθώς και να λαμβάνουν δικά τους μέτρα και στρατηγικές αντιμετώπισης.

Η χρήση μέτρων για την διασφάλιση του ελέγχου πρόσβασης καθώς και της ασφάλειας των δεδομένων, είναι αναγκαία για πρόληψη και αντιμετώπιση πιθανών επιθέσεων που αφορούν την αυθεντικότητα και διαθεσιμότητα των αποθηκευμένων δεδομένων, όπως αναφέρθηκε παραπάνω. Καλή πρακτική αποτελεί η απενεργοποίηση του Irqbalance για πιθανές ανεπιθύμητες διακοπές στο hardware καθώς και η εγκατάσταση και ρύθμιση εργαλείου παρακολούθησης του συστήματος (monitoring tool).

Οι εφαρμογές και υπηρεσίες κατά την χρήση τους, δημιουργούν διάφορα αρχεία (Log files) για την παρακολούθηση της κινητικότητας και των δραστηριοτήτων που λαμβάνουν μέρος οποιαδήποτε στιγμή. Τα αρχεία αυτά παίζουν ιδιαίτερα σημαντικό ρόλο στην κατανόηση και ανάλυση γεγονότων, αφορούν την απόδοση, την ανάκτηση μέρους ή και ολόκληρου πλήθους δεδομένων και συμβάλουν ενεργά στην αντιμετώπιση μελλοντικών γεγονότων. Υπάρχει μεγάλη ποικιλία εργαλείων παρακολούθησης και ανάλυσης των log αρχείων, όπως το Logwatch, Graylog2, Logstash και Logcheck, όμως για τις ανάγκες της διατριβής αυτής χρησιμοποιήθηκε το Logwatch.

3. Ανασφαλή Interfaces και APIs (Application Programming Interfaces).

Η λειτουργία, διαχείριση, ο έλεγχος και η ρύθμιση των υπηρεσιών παρέχονται στον καταναλωτή με την μορφή Software Interfaces και Application Programming Interfaces,

οπότε οποιοδήποτε ζήτημα ασφάλειας παρουσιαστεί μπορεί να αποφέρει καταστροφικές συνέπειες στους χρήστες του Υπολογιστικού σύννεφου.

Απαραίτητη θεωρείται η χρήση πιστοποιητικών SSL καθώς όπως ήδη αναφέρθηκε, με την χρήση των ψηφιακών πιστοποιητικών εξασφαλίζεται η ακεραιότητα και αυθεντικότητα των ευαίσθητων δεδομένων που μεταφέρονται και αποστέλλονται μέσω του διαδικτύου. Σημαντικό βήμα για θέματα ασφάλειας που προκύπτουν από τα ανασφαλή Interfaces και APIs, είναι η εγκατάσταση και ρύθμιση σειράς εργαλείων για παρακολούθηση και ανίχνευση πιθανών ευάλωτων στοιχείων του συστήματος.

Για τον καθορισμό ανοιχτών και σε λειτουργία υπηρεσιών και συνδέσεων χρησιμοποιείται πλήθος εργαλείων όπως το tcpdump, top και vmstat, για τις ανάγκες της διατριβής όμως, χρησιμοποιήθηκε το εργαλείο netstat που αποτελεί μέλος του Net-tools. Για τον καθορισμό ανοιχτών πορτών χρησιμοποιήθηκε το εργαλείο nmap, υπάρχουν όμως αρκετές εναλλακτικές λύσεις όπως το εργαλείο Fing και Angry IP Scanner. Η ανεύρεση υπηρεσιών σε λειτουργία καθώς και ανοιχτών και προσβάσιμων πορτών, αποτελεί αναγκαίο μέτρο ασφάλειας καθώς δυσκολεύει την διαδικασία ανεύρεσης ευπαθειών και τρόπων εκμετάλλευσης τους από την μεριά του επιτιθέμενου.

Η εγκατάσταση εργαλείων αναζήτησης Rootkits, όπως το Rkhunter και Chkorootkit αποτελεί ένα από τα βήματα που πρέπει να ληφθούν για την παρακολούθηση του συστήματος από συλλογές κακόβουλων εφαρμογών για μη εξουσιοδοτημενη είσοδο σε αυτό και ασφάλιση των αδύναμων Interfaces, καθώς και η εγκατάσταση Intrusion Detection Systems (IDs) για παρακολούθηση παραβιάσεων ασφαλείας, όπως τα Snort, AIDE, Suricata, Bro, Psad και Kismet. Για την συγκεκριμένη διατριβή χρησιμοποιήθηκε το Chkrootkit για αναζήτηση Rootkits και το Psad όσο αφορά τα Intrusion Detection εργαλεία. Τέλος, όπως ήδη αναφέρθηκε χρησιμοποιήθηκε το εργαλείο Logwatch για την παρακολούθηση της κινητικότητας και των δραστηριοτήτων που συμβαίνουν οποιαδήποτε στιγμή στο σύστημα.

4. Ζητήματα κοινόχρηστων τεχνολογιών.

Οι υπηρεσίες που διαμοιράζονται μεταξύ χρηστών, αποτελούν από τα κυριότερα ζητήματα ασφάλειας των πληροφοριών, οπότε θεωρείται αναγκαία η λήψη συγκεκριμένων βημάτων και στρατηγικών. Πέρα από τα μέτρα λήψης διασφάλισης του ελέγχου πρόσβασης και ασφάλειας των δεδομένων καθώς και τα εργαλεία παρακολούθησης και ανίχνευσης

αδυναμιών στο σύστημα που χρησιμοποιήθηκαν, απαιτείται η λήψη επιπλέον μέτρων για τα ζητήματα που αφορούν τις κοινόχρηστες τεχνολογίες που παρέχει το Υπολογιστικό σύννεφο.

Ένα από αυτά αποτελεί η ασφάλιση της κοινόχρηστης μνήμης καθώς με αυτό διασφαλίζεται η σωστή λειτουργία μεταξύ όλων των χρηστών του Cloud και αποτρέπονται πιθανές επιθέσεις, καθώς η shared memory μπορεί να χρησιμοποιηθεί σε επιθέσεις που αφορούν ανοιχτές και σε λειτουργία υπηρεσίες.

Σημαντικό μέτρο επίσης, αποτελεί η χρήση εργαλείων ανίχνευσης, ανάλυσης και διαχείρισης ευπαθειών και αδυναμιών στο σύστημα όπως τα Nessus Vulnerability Scanner, OpenVas, Metasploit και Intruder. Για τις ανάγκες της συγκεκριμένης εργασίας, χρησιμοποιήθηκαν τα Nessus και OpenVas προγράμματα ανίχνευσης.

5. Συμμόρφωση χρηστών στις καθορισμένες ρυθμίσεις.

Αποτελεί υποχρέωση των πελατών να ασφαλίζουν και να κρυπτογραφούν τα δικά τους δεδομένα και πληροφορίες, ακόμα και αν είναι αποθηκευμένα σε κάποιο data center που βρίσκεται στην δικαιοδοσία του παρόχου υπηρεσιών Cloud καθώς και να ακολουθούν συγκεκριμένους κανόνες και στρατηγικές για την χρήση του Υπολογιστικού σύννεφου. Εμφανίζεται λοιπόν, η ανάγκη για ύπαρξη συγκεκριμένων προτύπων για την αύξηση της ασφάλειας και της διαλειτουργικότητας των πλατφόρμων Cloud.

Κάποιοι παγκόσμιοι οργανισμοί, ήδη έχουν αναπτύξει πρότυπα, οδηγίες και διαδικασίες ασφάλειας και λειτουργικότητας του Υπολογιστικού σύννεφου με κάποιους από αυτούς να αποτελούν οι National Institute of Standards and Technology (NIST), Cloud Standards Customer Council (CSCC), The European Telecommunications Standards Institute (ETSI), Distributed Management Task Force (DMTF) και πολλοί άλλοι.

Τελευταίο βήμα και εξαιρετικά σημαντικό για την εγγύηση της ασφάλειας στα περιβάλλοντα Cloud, αποτελεί η διαρκής αναβάθμιση και βελτίωση των συστημάτων λόγω της διαρκούς εξέλιξης των τεχνολογιών. Οι αναβαθμίσεις software μπορούν να αποτελούν είτε λογισμικά ενημέρωσης για μεγάλες ευπάθειες ασφάλειας που μπορεί να ανακαλυφθούν είτε επιδιορθώσεις για μικρά σφάλματα που μπορεί να παρουσιαστούν. Καθώς διαρκώς εμφανίζονται νέες εκδόσεις λειτουργικών συστημάτων και εφαρμογών, οι υπολογιστές δεν λαμβάνουν όλες τις απαραίτητες

ενημερώσεις και επιδιορθώσεις ασφάλειας, οπότε είναι ιδιαίτερα σημαντικές οι συνεχείς ενημερώσεις και αναβαθμίσεις.

Με την χρήση και τον σχεδιασμό ενός περιβάλλοντος Υπολογιστικού σύννεφου, είναι απαραίτητα μέτρα και στρατηγικές για αποφυγή και αποτροπή επιθέσεων σχεδιασμένων για Cloud Computing πλατφόρμες. Με την διαρκή αναβάθμιση και ανανέωση των βασικών στρατηγικών, διασφαλίζεται η καλή λειτουργία των περιβαλλόντων αυτών καθώς και η εξασφάλιση της ακεραιότητας, αυθεντικότητας και διαθεσιμότητας των αποθηκευμένων δεδομένων και πληροφοριών. Οι πάροχοι Cloud πλατφόρμων, όπως η Microsoft Corporation με την πλατφόρμα Azure Services Platform, η Google με τις υπηρεσίες που παρέχονται μέσω του Google App Engine και η Amazon με τις υπηρεσίες που παρέχονται μέσω του Amazon Web Services, πρέπει να υπακούουν στα πρότυπα και στρατηγικές που διαρκώς αναβαθμίζονται καθώς και στα Standards που έχουν αναπτυχθεί.

Η χρήση του Υπολογιστικού σύννεφου, που παρέχει πλήθος υπηρεσιών, εφαρμογών, ευκαιρίες ανάπτυξης, αύξηση παραγωγικότητας και ανταγωνιστικότητας, ελαστικότητα και διευκόλυνση, με την διαρκή υπακοή στους νόμους, στρατηγικές και πρότυπα καθώς και με την συνεχή αναβάθμιση και βελτίωση των συστημάτων, χρηστών, οργανισμών και παρόχων, αναμένεται να γίνει ευρεία και παγκόσμια προσφέροντας περισσότερες και καινοτόμες υπηρεσίες και εφαρμογές στους χρήστες [31-32].

Δημοσίευση

Τα ερευνητικά αποτελέσματα της Μεταπτυχιακής Διατριβής “Μυστικότητα και Εμπιστευτικότητα σε Αρχιτεκτονικές Υπολογιστικού Σύννεφου (Cloud Computing)” έχουν δημοσιευτεί:

- P. Spanaki, N. Sklavos, "Cloud Computing: Security Issues and Establishing Virtual Cloud Environment via Vagrant to Secure Cloud Hosts", Chapter in the Book: *Computer and Network Security Essentials*, editors Kevin Daimi, Levent Ertaul, Guillermo Francia, Eman El-Sheikh, Luis Hernandez Encinas, Springer, 2017

Βιβλιογραφία

[01] Chauhan M.A, Babar M.A, Benetallah B (2016). Architecting Cloud Enabled Systems a Systematic Survey of Challenges and Solutions, Doi: 10.1002/spe.2409, p. 1

[02] Binu S. and Misbahuddin M. (2013). A Survey of Traditional and Cloud Specific Security Issue, p. 110, 116, 118

[03] Mell P, Grance T (2011), The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145, p. 2-3

[04] I Foster, Yong Zhao, I Raicu, and S Lu (2011), Cloud Computing and Grid Computing 360-degree compared In Grid Computing Environments Workshop 2008. GCE '08, p. 1-10

[05] Arutyunov V.V. (2012), Cloud Computing: It's History of Development, Modern State and Future Considerations 2012. ISSN 0147-6882, Scientific and Technical Information Processing 2012, Vol. 39, No 3, Doi: 10.3103/S0147688212030082, pp. 173-178

[06] Bulusu S, Sudia K (2012), A Study on Cloud Computing Security Challenges, Dissertation School of Computing Blekinge Institute of Technology, Sweden, p. 7-9

[07] M. Missbach et al. (2013), A Short History of Cloud Computing, SAP on the Cloud, Management for Professional, Doi: 10.1007/978-3-642-31211-3_1, Springer 2013, p.1

[08] Popovic K, Hocenski Z (June 2010), Cloud Computing security issues and challenges, MIPRO, 2010 Proceedings of the 33rd International Convention, p. 1-6

[09] Rastogi N, Gloria M.J.K, Hendler J (2015), Security and Privacy of Performing Data Analytics in the Cloud: A Three-way Handshake of Technology, Policy, and Management Journal of Information Policy, Volume 5, p.133, 134, 142

[10] Shrivastava N, Yadav R (2013). A Review of Cloud Computing Security Issues, International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, p. 551

[11] D.M. Ajay (2016), E. Umamaheswari, An Initiation for Testing the Security of a Cloud Service Provider, Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC – 16'), p. 34, 37-38

[12] Albeshri, Aiiad Ahmad and Caelli William (2010), Mutual protection in a cloud computing environment, In: IEEE 12thInternational Conference on High Performance Computing and Communications (HPCC 2010), 1-3 September 2010, Melbourne. p 641

[13] Yan X. et al. (2011), The Research and Design of Cloud Computing Security Framework (2011), Advances in Computer, Communication, Control & Automation, LNEE 121, p. 758

[14] Grobauer B, Walloschek T, Stocker E (2011). Understanding Cloud Computing Vulnerabilities, IEEE Security and Privacy Magazine 9(2):50 – 57, Doi: 10.1109/MSP.2010.115, p. 3-6

[15] Mahmood Z (ed) (2014), Cloud Computing Challenges, Limitations and R&D Solutions, Springer 2014, Heidelberg, p. 5, 8-18

[16] Antonopoulos N, Gillam L (eds) (2010), Cloud Computing Principles, Systems and Applications, Springer 2010, Heidelberg, p. 31

[17] N. Sklavos, P. Souras, "Economic Models and Approaches in Information Security for Computer Networks", International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January 2006, pp. 14-20

[18] H. Li et al. (2012), A Deep Understanding of Cloud Computing Security, NCIS 2012, CCIS 345, Springer, p. 99

[19] Song D.X, Wanger D, Tian X (2001), Timing Analysis of Keystrokes and Timing Attacks on SSH, Proceedings of the10th USENIX Security Symposium Washington, D.C., USA, August 13–17 2001, p. 5

[20] Kumar S. (2005), Impact of Distributed Denial of Service (DDos) Attack Due to ARP Storm, ICN 2005, LNCS 3421, Springer-Verlag Berlin Hedelberg, p. 997-998

[21] Lonea A. et al. (2013), Evaluation of Experiments on Detecting Distributed Denial of Service (Ddos) Attacks in Eucalyptus Private Cloud, Soft Computing Applications, AISC 195, Springer 2013, p. 367-368

[22] A. Bechtsoudis, N. Sklavos, "Side Channel Attacks Cryptanalysis Against Block Ciphers Based on FPGA Devices", proceedings of IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'10), Kefalonia, Greece, July 5-7, 2010, p. 1

[23] Jensen M, Schwenk J, Gruschka N, Iacono LL, On Technical Security Issues in Cloud Computing. Proceedings of the 2009 IEEE international conference on cloud computing (CLOUD '09), Bangalore, 21–25 Sept 2009, p. 109–116

[24]S. Shafieian et al. (2014), Attacks in Public Clouds: Can They Hinder the Rise of the Cloud? , Cloud Computing, Computer Communications and Networks, DOI 10.1007/978-3-319-10530-7_1, Springer 2014, p. 9-16

[25] T. Galibus et al. (2016), Common Cloud Attacks and Vulnerabilities, Elements of Cloud Storage Security, Springer Briefs in Computer Science, DOI: 10.1007/978-3-319-44962-3_2, Springer 2016, p. 23-24

[26] (2017), Πρόσβαση στις 20/4/2017 στο: https://www.vagrantup.com/intro/index.html

[27] (2017), Πρόσβαση στις 20/4/2017 στο: https://www.ansible.com/it-automation

[28] (2017),Πρόσβαση στις 21/4/2017 στο: http://docs.ansible.com/ansible/playbooks_intro.html

[29] (2017), Πρόσβαση στις 21/4/2017 στο:
http://docs.ansible.com/ansible/intro_inventory.html

[30] A. Bechtsoudis, N. Sklavos, "Aiming at Higher Network Security Through Extensive Penetration Trees", IEEE Latin America Transactions, Volume 10, Issue 3, 2012, p. 1

[31] N. Sklavos, M. Hubner, D. Goehringer, P. Kitsos, System-Level Design Methodologies for Telecommunication, Springer, ISBN: 3319006622, 2013

[32] T. Dagiuklas, N. Sklavos, Mobile Multimedia Communications, Third International Conference on Mobile Multimedia Communications, Nafpaktos, Greece, August 27-29, ACM International Conference Proceeding Series 329, ICST Brussels, Belgium, ISBN: 9789630626705, 2007