Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Ζητήματα ευπαθειών και ασφάλειας σε περιβάλλοντα νέφους και τρόποι αντιμετώπισης

Νικολαΐδης Γεώργιος Αύγουστος

Επιβλέπων Καθηγητής
Αναστάσιος Νταγιούκλας

Ιανουάριος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ζητήματα ευπαθειών και ασφάλειας σε περιβάλλοντα νέφους και τρόποι αντιμετώπισης

Νικολαΐδης Γεώργιος Αύγουστος

Επιβλέπων Καθηγητής
Αναστάσιος Νταγιούκλας

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

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Ιανουάριος 2015

Περίληψη

Το υπολογιστικό νέφος είναι μια γρήγορα αναπτυσσόμενη τεχνολογία και ένα ευρέως αποδεκτό υπολογιστικό μοντέλο σε όλο τον κόσμο εξαιτίας των πλεονεκτημάτων του για την γρήγορη ανάπτυξη, τη σχέση αποδοτικότητας-κόστους, το μεγάλο αποθηκευτικό χώρο και την εύκολη πρόσβαση στο σύστημα ανά πάσα στιγμή και από οπουδήποτε. Ωστόσο, πέρα από τα πλεονεκτήματα υπάρχουν και μειονεκτήματα, σχετικά με την ασφάλεια και την προστασία της ιδιωτικής ζωής, τα οποία και θεωρούνται ως κύρια εμπόδια για την ευρύτερη υιοθέτησή του. Την ίδια στιγμή, λόγω της κατανεμημένης φύσης του συστήματος, υπάρχει ο κίνδυνος επιθέσεων ασφαλείας σχετικά με τις υπηρεσίες και τους πόρους στο υπολογιστικό νέφος. Οι επιθέσεις αυτές μπορεί να είναι τόσο εκτός όσο και εντός του δικτύου του παρόχου του νέφους.

Η συγκεκριμένη διπλωματική εργασία, έχει σαν σκοπό να παρουσιάσει το υπολογιστικό νέφος και τη λειτουργία του, όπως επίσης και θέματα τα οποία αφορούν τους κινδύνους και την ασφάλεια σε αυτό.

Ξεκινώντας λοιπόν, στο πρώτο κεφάλαιο της εργασίας, γίνεται μια παρουσίαση του υπολογιστικού νέφους μέσα από ορισμούς, γίνεται αναφορά στα κύρια χαρακτηριστικά του όπως επίσης και στα μοντέλα που διαθέτει. Ακόμα, αναφέρονται τα διάφορα πλεονεκτήματα και μειονεκτήματα όσον αφορά τη λειτουργία του.

Εν συνεχεία, στα κεφάλαια 2 και 3 αναλύονται τα θέματα της ασφάλειας, των κινδύνων, των πιθανών επιθέσεων και των αδυναμιών που συνδέονται με το υπολογιστικό νέφος. Όπως θα αντιληφθεί ο αναγνώστης, υπάρχουν διάφοροι τύποι επιθέσεων και απειλών που μπορεί να συναντήσει κανείς στο υπολογιστικό νέφος και γι΄αυτό το λόγο αποκτούν ακόμα μεγαλύτερη σημασία τα κεφάλαια αυτά. Είναι καίριας σημασίας το να μπορεί να διασφαλίζεται η ακεραιότητα και η σημαντικότητα των πληροφοριών που υπάρχουν μέσα στο νέφος από κακόβουλες παρεμβάσεις. Η εμπιστοσύνη άλλωστε είναι ένας από τους σημαντικότερους παράγοντες επιλογής του υπολογιστικού νέφους από τους χρήστες.

Στο επόμενο, τέταρτο κεφάλαιο, γίνεται ακριβώς αναφορά σε ένα από τα σημαντικότερα στοιχεία, όπως αναφέρθηκε παραπάνω, που πρέπει να διαθέτει το νέφος, την εμπιστοσύνη. Στο πέμπτο κεφάλαιο, γίνεται παρουσίαση των εφαρμογών στο υπολογιστικό νέφος, των προϋποθέσεων που πρέπει να πληρούνται για την ανάπτυξή τους, της λειτουργικότητά τους και άλλων στοιχείων γύρω από τις εφαρμογές στο νέφος. Επίσης, γίνεται αναφορά στην εικονοποίηση των εφαρμογών στο νέφος και την έκρηξη νέφους. Τέλος, στο έκτο και τελευταίο κεφάλαιο, η πτυχιακή εργασία κλείνει με τα συμπεράσματα.

Summary

Cloud computing is a rapidly growing technology and a widely accepted model of computation around the world because of its advantages for rapid development, the relation cost-effectiveness, the large storage space and easy access to the system at any time and from anywhere. However, beyond the advantages there are also disadvantages about security and privacy, which are considered as major obstacles to wider adoption. At the same time, due to the distributed nature of the system, there is the risk of security attacks on services and resources in the cloud. These attacks can be both outside and within the network service provider cloud.

This thesis aims to provide cloud computing its operation, as well as issues relating to risks and safety in it.

In the first chapter we present the cloud through definitions, its main features as well as the models available. Still, presents the various advantages and disadvantages of its operation.

In Chapters 2 and 3 are analyzed the security issues, risks, potential attacks and vulnerabilities associated with cloud computing. There are various types of attacks and threats that one can encounter in the cloud and therefore are even more important. It is crucial to be able to ensure the integrity and significance of the information found within the cloud from malicious interference. Trust is also one of the most important factors for the users to choose cloud.

The fourth chapter refers to one of the most important issues as mentioned above, that must have a cloud, confidence. In the fifth chapter we present applications in the cloud, the conditions which must be met for their development, their functionality and other information about the applications in the cloud. Reference is also made to the visualization of applications in the cloud. Finally in the sixth and final chapter, thesis ends with conclusions.

Περιεχόμενα

Κεφάλαιο 1
Ορισμός – Τύποι Μοντέλων Υπολογιστικών Νεφών

1.1 Εισαγωγή

Στα δίκτυα υπολογιστών, το υπολογιστικό νέφος (Cloud Computing) περιλαμβάνει ένα μεγάλο αριθμό υπολογιστών που συνδέονται μέσω ενός δικτύου επικοινωνίας, όπως το διαδίκτυο, παρόμοιο με το βοηθητικό πρόγραμμα υπολογιστών [46]. Στην επιστήμη, το υπολογιστικό νέφος είναι ένα συνώνυμο για κατανεμημένα συστήματα πληροφορικής μέσω δικτύου και σημαίνει την ικανότητα να τρέχει ένα πρόγραμμα ή εφαρμογή σε πολλούς συνδεδεμένους υπολογιστές ταυτόχρονα.

Δικτυακές υπηρεσίες, που φαίνεται να παρέχονται από πραγματικό υλικό διακομιστή και στην πραγματικότητα εξυπηρετούνται από την εικονική

προσομοίωση υλικού, από λογισμικό που εκτελείται σε μία ή περισσότερες πραγματικές μηχανές, συχνά αποκαλείται υπολογιστικό νέφος. Τέτοιοι εικονικοί servers, δεν μπορούν να υπάρξουν στο φυσικό περιβάλλον και συνεπώς μπορούν να μετακινηθούν και να κλιμακωθούν πάνω ή κάτω χωρίς να επηρεάζουν τον τελικό χρήστη, κάτι σαν ένα σύννεφο που γίνεται μεγαλύτερο ή μικρότερο, χωρίς να είναι ένα φυσικό αντικείμενο.

Παρά το γεγονός ότι δεν υπάρχει μοναδικός ορισμός για το υπολογιστικό νέφος, ένας ορισμός που είναι κοινά αποδεκτός παρέχεται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών [52]:

«Το υπολογιστικό νέφος είναι ένα μοντέλο για να βρίσκεται παντού, βολικό, με on-demand πρόσβαση στο δίκτυο σε μια κοινόχρηστη πισίνα ρύθμισης υπολογιστικών πόρων (π.χ., δίκτυα, servers, αποθήκευση, εφαρμογές και υπηρεσίες) που μπορεί να τροφοδοτηθεί γρήγορα και να κυκλοφορήσει με την ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης παροχής υπηρεσιών» [49].

Αυτή η κοινόχρηστη πηγή πόρων είναι ενωμένη μέσω εικονικοποίησης (virtualization) ή τεχνικών προγραμματισμού των εργασιών. Εικονικοποίηση είναι η δημιουργία ενός συνόλου λογικών πόρων (είτε πρόκειται για μια πλατφόρμα hardware, λειτουργικό σύστημα, των πόρων του δικτύου ή άλλων πόρων) που εφαρμόζονται συνήθως από στοιχεία λογισμικού που λειτουργούν σαν φυσικοί πόροι. Ειδικότερα, το λογισμικό που ονομάζεται «hypervisor» (επόπτης) μιμείται το φυσικό υλικό του υπολογιστή και ως εκ τούτου επιτρέπει το λογισμικό του λειτουργικού συστήματος να εκτελείται στην εικονική πλατφόρμα – μια εικονική μηχανή (VM-Virtual Machine) – να διαχωρίζεται από τους υποκείμενους πόρους του υλικού.

Οι πόροι που διατίθενται μέσω του υπολογιστικού νέφους, περιλαμβάνουν το υλικό (hardware) και το λογισμικό (software) των συστημάτων σε απομακρυσμένα κέντρα δεδομένων, καθώς και υπηρεσίες που βασίζονται σε αυτές που είναι προσβάσιμες μέσω του διαδικτύου. Οι πόροι αυτοί μπορούν να διαχειριστούν δυναμικά και κλιμακωτά για να ταιριάζουν με το φορτίο, χρησιμοποιώντας ένα επιχειρηματικό μοντέλο με χρέωση ανά πόρο. Βασικά χαρακτηριστικά του νέφους είναι η ελαστικότητα (elasticity), η πολυμίσθωση

(multiple lease), η μέγιστη αξιοποίηση των πόρων και η χρέωση με τη χρήση. Αυτά τα νέα χαρακτηριστικά παρέχουν τα μέσα για να αξιοποιηθούν μεγάλες υποδομές, όπως τα κέντρα δεδομένων μέσω εικονοποίησης ή της διαχείριση της εργασίας και της διαχείρισης των πόρων.

Το υπολογιστικό νέφος (ή, πιο απλά «νέφος») παρέχει ευκαιρίες αγοράς με τεράστιες δυνατότητες τόσο για την αποτελεσματικότητα, όσο και τις νέες επιχειρηματικές ευκαιρίες (ιδίως ως προς τη σύνθεση των υπηρεσιών), και είναι σχεδόν βέβαιη η βαθιά μεταμόρφωση των υποδομών της τεχνολογίας των πληροφοριών, των μοντέλων και των υπηρεσιών. Όχι μόνο υπάρχει εξοικονόμηση κόστους λόγω της οικονομικής κλίμακας από την πλευρά του φορέα παροχής υπηρεσιών και των pay-as-you-go[1] μοντέλων, αλλά ο επιχειρηματικός κίνδυνος μειώνεται επειδή υπάρχει λιγότερη ανάγκη να δανειστούν χρήματα για την αρχική επένδυση σε υποδομές.

Η υιοθέτηση του υπολογιστικού νέφους, μπορεί να κινηθεί αρκετά γρήγορα ανάλογα με τις τοπικές ανάγκες, το πλαίσιο των επιχειρήσεων και τις ιδιαιτερότητες της αγοράς. Είναι ακόμα στα πρώτα στάδια, αλλά οι τεχνολογίες νέφους υιοθετούνται ευρέως σε όλα τα μέρη του κόσμου. Οι οικονομικές δυνατότητες του υπολογιστικού νέφους και η ικανότητά του να επιταχύνει την καινοτομία, βάζει τις επιχειρήσεις και τις κυβερνήσεις υπό αυξημένη πίεση, ώστε να υιοθετήσουν λύσεις που βασίζονται στο υπολογιστικό νέφος.

Αν και η αίσθηση που υπάρχει γύρω από το νέφος τείνει να ενθαρρύνει τους ανθρώπους να πιστεύουν ότι είναι πανάκεια, αρκετά συχνά αγνοείται η εγγενής πολυπλοκότητα που προστίθεται από το νέφος. Υπάρχει μια σειρά από προκλήσεις για την παροχή υπηρεσιών του υπολογιστικού νέφους:

- η ανάγκη για συμμόρφωση με τις τοπικές και περιφερειακές ρυθμίσεις,
- η λήψη των απαραίτητων εγκρίσεων όταν τα δεδομένα έχουν πρόσβαση από άλλη δικαιοδοσία,

[1] Pay-as-you-go: Με την υπηρεσία των pay-as-you-go μοντέλων ο χρήστης χρεώνεται μόνο όσους πόρους χρησιμοποιεί κάθε φορά. Έτσι, το μοντέλο αυτό προσφέρει την μεγίστη δυνατή εκμετάλλευση των πόρων σε σχέση με την ζήτηση, γιατί ο πελάτης πληρώνει μόνο για τους πόρους που πραγματικά αξιοποιεί.

- η πρόσθετη πολυπλοκότητα όσον αφορά τη διαχείριση, τη συντήρηση και την ευθύνη, που ενυπάρχουν στο νέφος και μια αντιληπτή έλλειψη εμπιστοσύνης στον τομέα των υπηρεσιών νέφους.

Πολλοί Προϊστάμενοι Πληροφοριακών Συστημάτων (CIOs-Chief Information Officers) σε μεγάλες επιχειρήσεις, προσδιορίζουν την ασφάλεια ως τον κορυφαίο λόγο για να μην αγκαλιάζουν το δημόσιο νέφος πιο επιθετικά και να μην επωφελούνται από τις σχετιζόμενες βελτιστοποιήσεις του κόστους [31]. Επιπρόσθετα, μια μάλλον κοινή ανησυχία από κοινό με τεχνικές γνώσεις είναι η προστασία των δεδομένων, με τους καταναλωτές να τάσσονται υπέρ των ρυθμιστικών αρχών σχετικά με τις δυνητικά σημαντικές επιπτώσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και την απαιτούμενη συμμόρφωση με τους τοπικούς κανονισμούς [9].

Το νέφος επίσης, και με την σημερινή μορφή παγκοσμιοποίησης που υπάρχει, δεν είναι και ό,τι καλύτερο για την προστασία της ιδιωτικής ζωής [69]. Για παράδειγμα, το σημείο στο οποίο βρίσκεται κάποιος, ενώ από νομικής άποψης μπορεί να είναι σημαντικό, στο νέφος όμως η πληροφορία αυτή μπορεί να είναι σε πολλά σημεία, δηλαδή μπορεί να διαχειρίζεται από διαφορετικές οντότητες και μπορεί να είναι δύσκολο να γνωρίζει κάποιος την ακριβή γεωγραφική θέση κάποιου αλλά, και ποιος συγκεκριμένος διακομιστής ή αποθηκευτική συσκευή χρησιμοποιείται. Επί του παρόντος είναι δύσκολο να εξακριβωθούν οι απαιτήσεις που πληρούνται, καθώς η υφιστάμενη παγκόσμια νομοθεσία είναι πολύπλοκη και περιλαμβάνει περιορισμούς εξαγωγών, περιορισμούς της διατήρησης των δεδομένων, περιορισμούς τομέων και νομοθεσίας σε κρατικό ή / και εθνικό επίπεδο. Η νομική συμβουλή είναι απαραίτητη, ο διασυνοριακός περιορισμός της ροής των δεδομένων πρέπει να λαμβάνεται υπόψη και πρέπει να ληφθεί μέριμνα ώστε κατά περίπτωση να διαγράφονται δεδομένα και εικονικές συσκευές αποθήκευσης. Παρά το γεγονός ότι συχνά υπάρχει μια έμφαση στην ασφάλεια, στην πραγματικότητα, το πιο σύνθετο ζήτημα για την αντιμετώπιση, είναι η μυστικότητα.

Το γενικό πλαίσιο, είναι μια ενδιαφέρουσα πτυχή, καθώς διαφορετικές πληροφορίες μπορούν να έχουν διαφορετική μυστικότητα, ασφάλεια και

εμπιστευτικότητα. Η προστασία της ιδιωτικής ζωής πρέπει να ληφθεί υπόψη μόνο εάν η υπηρεσία του νέφους χειρίζεται προσωπικά στοιχεία (υπό την έννοια της συλλογής, μεταφοράς, επεξεργασίας, διανομής, πρόσβασης ή αποθήκευσης). Επιπλέον, οι απειλές της ιδιωτικότητας διαφέρουν ανάλογα με τον τύπο του νέφους. Προφανώς υπάρχει μικρή απειλή της ιδιωτικής ζωής, εφόσον οι υπηρεσίες νέφους είναι να επεξεργαστούν πληροφορίες που είναι (ή πολύ σύντομα θα είναι) δημόσιες. Από την άλλη πλευρά, υπάρχει μεγάλη απειλή της ιδιωτικής ζωής για υπηρεσίες νέφους που είναι δυναμικά εξατομικευμένες, με βάση τη θέση των ανθρώπων, τις προτιμήσεις, το ημερολόγιο και τα κοινωνικά δίκτυα, κλπ. Σε γενικές γραμμές το θέμα της ασφάλειας είναι ένα πολύπλοκο θέμα με ρυθμιστικές και οργανωτικές διαστάσεις [11][30].

1.2. Τύποι μοντέλων υπολογιστικών νεφών

1.2.1 Αναπτυξιακά ή μοντέλα διάθεσης

Στα αναπτυξιακά ή μοντέλα διάθεσης, η δικτύωση, η πλατφόρμα, η αποθήκευση και η υποδομή του λογισμικού παρέχονται ως υπηρεσίες που κλιμακώνονται πάνω ή κάτω ανάλογα με τη ζήτηση. Το υπολογιστικό νέφος έχει τέσσερα βασικά αναπτυξιακά μοντέλα, τα οποία είναι:

Ιδιωτικό νέφος (Private Cloud)

Το ιδιωτικό νέφος είναι ένας νέος όρος που ορισμένοι έχουν χρησιμοποιήσει πρόσφατα για να περιγράψουν τις προσφορές που μιμείται το υπολογιστικό νέφος σε ιδιωτικά δίκτυα. Είναι στημένο για να βρίσκεται στα πλαίσια ενός εσωτερικού επιχειρηματικού κέντρου δεδομένων. Στο ιδιωτικό νέφος, κλιμακούμενοι πόροι και εικονικές εφαρμογές παρέχονται από τον προμηθευτή του νέφους και είναι διαθέσιμα στους χρήστες του νέφους για να τα μοιραστούν και να τα χρησιμοποιήσουν. Διαφέρει από το δημόσιο νέφος στο ότι όλοι οι πόροι και οι εφαρμογές διαχειρίζονται από την ίδια την «επιχείρηση», παρόμοιο με την λειτουργικότητα του Intranet. Η χρησιμοποίηση του ιδιωτικού νέφους μπορεί να είναι πολύ πιο ασφαλής από εκείνη του δημοσίου, λόγω των ειδικών εσωτερικών μηχανισμών που διαθέτει. Μόνο η «οργάνωση-επιχείρηση» και ορισμένα

συγκεκριμένα ενδιαφερόμενα μέρη μπορούν να έχουν πρόσβαση για να λειτουργήσουν ένα συγκεκριμένο ιδιωτικό νέφος [59].

Δημόσιο νέφος (Public Cloud)

Το δημόσιο νέφος, περιγράφει το υπολογιστικό νέφος στην παραδοσιακή κύρια έννοιά του, όπου οι πόροι τροφοδοτούνται δυναμικά πάνω σε μια self-service βάση στο internet, μέσω web εφαρμογών, υπηρεσιών internet, από έναν τρίτο πάροχο που μοιράζεται πόρους και λογαριασμούς πάνω σε μια υψηλής χρησιμότητας υπολογιστική βάση. Συνήθως βασίζεται σε ένα μοντέλο χρέωσης ανά χρήστη, παρόμοιο με ένα σύστημα προπληρωμένης μέτρησης ηλεκτρικής ενέργειας, το οποίο είναι αρκετά ευέλικτο για να καλύψει την αιχμή της ζήτησης για τη βελτιστοποίηση του νέφους [2]. Τα δημόσια νέφη είναι λιγότερο ασφαλή από άλλα μοντέλα διότι τοποθετούν μια πρόσθετη επιβάρυνση, της διασφάλισης ότι οι εφαρμογές και τα δεδομένα δεν θα υπόκεινται σε κακόβουλες επιθέσεις.

Υβριδικό νέφος (Hybrid Cloud)

Το υβριδικό νέφος, είναι ένα ιδιωτικό νέφος που συνδέεται με μία ή περισσότερες εξωτερικές υπηρεσίες νέφους, με κεντρική διαχείριση, τροφοδοτούμενο ως μια ενιαία μονάδα και περιβάλλεται από ένα ασφαλές δίκτυο [26]. Παρέχει εικονικές λύσεις πληροφορικής μέσω ενός συνδυασμού τόσο των δημόσιων όσο και των ιδιωτικών νεφών. Το υβριδικό νέφος παρέχει πιο ασφαλή έλεγχο των δεδομένων και των εφαρμογών του και επιτρέπει διάφορα μέρη να έχουν πρόσβαση σε πληροφορίες μέσω του διαδικτύου. Έχει επίσης μια ανοικτή αρχιτεκτονική που επιτρέπει τις διασυνδέσεις με άλλα συστήματα διαχείρισης, π.χ. το υβριδικό νέφος μπορεί να περιγράψει τη διαμόρφωση συνδυάζοντας μια τοπική συσκευή, όπως ένας συνδεδεμένος υπολογιστής με τις υπηρεσίες νέφους. Μπορεί επίσης να περιγράφει διαμορφώσεις εικονικές συνδυασμένες με φυσικές, για παράδειγμα, ως επί το πλείστον εικονικό περιβάλλον που απαιτεί φυσικούς servers, routers, ή άλλο υλικό όπως μια συσκευή δικτύου που λειτουργεί ως ένα τείχος προστασίας ή φίλτρο spam.

Νέφος κοινότητας (Community Cloud)

Αυτό το είδος νέφους είναι για την αποκλειστική χρήση από μια συγκεκριμένη κοινότητα καταναλωτών από οργανώσεις που έχουν κοινές απόψεις. Αυτή η ρύθμιση ενδέχεται να υπάρχει μέσα ή έξω από τις εγκαταστάσεις CSP (Content Service Provider). Αυτό το νέφος θα μπορούσε να ελέγχεται, να συντηρείται και να διευθύνεται από ένα τρίτο μέρος ή συνδυασμό της ίδιας της οργάνωσης.

1.2.2 Μοντέλα υπηρεσιών

Μετά τα αναπτυξιακά μοντέλα νέφους, η επόμενη εξέταση της ασφάλειας σχετίζεται με τα διάφορα μοντέλα υπηρεσιών. Τα τρία βασικά μοντέλα υπηρεσιών είναι: Infrastructure-as-a-Service (IaaS) – (Υποδομή ως υπηρεσία), Platform-as-a-Service (PaaS) – (Πλατφόρμα ως υπηρεσία), Software-as-a-Service (SaaS) – (Λογισμικό ως υπηρεσία) Network-as-a-Service (NaaS) – (Δίκτυο ως υπηρεσία).

Infrastructure-as-a-Service (IaaS) – (Υποδομή ως υπηρεσία)

Η υποδομή ως υπηρεσία, είναι ένα ενιαίο στρώμα ενοικίασης νέφους, όπου οι πόροι του υπολογιστικού νέφους του παρόχου, διαμοιράζονται μόνο με σύμβαση σε πελάτες με χρέωση ανά χρήση. Αυτό ελαχιστοποιεί σε μεγάλο βαθμό την ανάγκη για τεράστιες αρχικές επενδύσεις σε hardware για υπολογιστές, όπως servers, συσκευές δικτύωσης και επεξεργαστική ισχύ. Επιτρέπουν επίσης διάφορους βαθμούς της οικονομικής και λειτουργικής ευελιξίας να μην βρίσκονται στα εσωτερικά κέντρα δεδομένων ή με υπηρεσίες συνεγκατάστασης, επειδή υπολογιστικοί πόροι μπορούν να προστεθούν ή να κυκλοφορήσουν πολύ πιο γρήγορα και αποτελεσματικά από άποψη κόστους από ό, τι σε ένα εσωτερικό κέντρο δεδομένων ή μια υπηρεσία συνεγκατάστασης [31]. Η υποδομή ως υπηρεσία και άλλες συναφείς υπηρεσίες επιτρέπουν ξεκινήματα και άλλες επιχειρήσεις να επικεντρώνονται στις βασικές ικανότητές τους χωρίς να ανησυχούν πολύ για την πρόβλεψη και τη διαχείριση της υποδομής. Η υποδομή ως υπηρεσία, απομονώνει εντελώς το υλικό κάτω από αυτήν και επιτρέπει στους χρήστες να καταναλώνουν υποδομές ως υπηρεσία, χωρίς να τους ανησυχεί

τίποτα για τις υποκείμενες πολυπλοκότητες. Το νέφος έχει μια συγκλονιστική πρόταση αξίας από άποψη κόστους, αλλά «έξω από το κουτί» η IaaS παρέχει μόνο ένα βασικό επίπεδο ασφάλειας (περιμετρικό firewall, εξισορρόπηση φορτίου, κλπ.) και εφαρμογές που διακινούνται στο σύννεφο θα χρειάζονται υψηλότερα επίπεδα ασφάλειας να παρέχονται στον ξενιστή.

Platform-as-a-Service (PaaS) – (Πλατφόρμα ως υπηρεσία)

Η πλατφόρμα ως υπηρεσία είναι ένα σύνολο λογισμικού και εργαλείων ανάπτυξης που φιλοξενούνται σε διακομιστές του παρόχου. Είναι ένα στρώμα πάνω από την IaaS στη στοίβα και αφαιρεί τα πάντα μέχρι το Λειτουργικό Σύστημα (OS-Operating System) κλπ. Αυτό προσφέρει μια ολοκληρωμένη σειρά προγραμματιστικού περιβάλλοντος, όπου ένας προγραμματιστής μπορεί να αξιοποιήσει για τη δημιουργία των εφαρμογών τους, χωρίς καμία ιδέα για το τι συμβαίνει κάτω από την υπηρεσία. Προσφέρει στους προγραμματιστές μια υπηρεσία που παρέχει την διαχείριση ενός πλήρους κύκλου ζωής της ανάπτυξης λογισμικού, από το σχεδιασμό μέχρι την οικοδόμηση εφαρμογών, την ανάπτυξη των δοκιμών και τη συντήρηση. Ο,τιδήποτε άλλο, αποσπάται μακριά από το "οπτικό πεδίο" των προγραμματιστών. Η πλατφόρμα ως υπηρεσία νέφους, λειτουργεί όπως την IaaS, αλλά παρέχει ένα πρόσθετο επίπεδο «ενοικιαζόμενης» λειτουργικότητας. Οι πελάτες που χρησιμοποιούν PaaS υπηρεσίες, μεταφέρουν ακόμα περισσότερα έξοδα από κεφαλαιουχικές επενδύσεις στις λειτουργικές δαπάνες αλλά πρέπει να αναγνωριστούν κάποιοι πρόσθετοι περιορισμοί και, ενδεχομένως σε κάποιο βαθμό ο εγκλωβισμός που τίθεται από τα πρόσθετα στρώματα λειτουργικότητας [61]. Η χρήση των εικονικών μηχανών δρά ως καταλύτης στο στρώμα PaaS στο υπολογιστικό νέφος. Οι εικονικές μηχανές πρέπει να προστατεύονται από κακόβουλες επιθέσεις. Ως εκ τούτου, η διατήρηση της ακεραιότητας των αιτήσεων και η σωστή επιβολή ελέγχων ακριβείας ταυτότητας κατά τη διάρκεια της μεταφοράς των δεδομένων μεταξύ ολόκληρων καναλιών δικτύωσης, είναι θεμελιώδους σημασίας.

Software-as-a-Service (SaaS) – (Λογισμικό ως υπηρεσία)

Το λογισμικό ως υπηρεσία, είναι ένα μοντέλο διανομής λογισμικού κατά το οποίο οι εφαρμογές που φιλοξενούνται από τον πωλητή ή τον πάροχο υπηρεσιών,

διατίθεται σε πελάτες μέσω ενός δικτύου, συνήθως το Internet. Το λογισμικό ως υπηρεσία, γίνεται ένα όλο και πιο διαδεδομένο μοντέλο διάθεσης, ως βασική τεχνολογία που υποστηρίζει διαδικτυακές υπηρεσίες και υπηρεσίες προσανατολισμένες στην αρχιτεκτονική (SOA - Service Oriented Architectures), ώριμες και νέες αναπτυξιακές προσεγγίσεις γίνονται δημοφιλής. Το SaaS επίσης, συχνά συνδέεται με ένα μοντέλο χορήγησης αδειών με pay-as-you-go συνδρομή. Εν τω μεταξύ, η ευρυζωνική υπηρεσία γίνεται όλο και περισσότερο διαθέσιμη για την υποστήριξη της πρόσβασης των χρηστών από τις περισσότερες περιοχές σε όλο τον κόσμο. Το SaaS πιο συχνά χρησιμοποιείται για την παροχή λειτουργικότητας επιχειρηματικού λογισμικού σε εταιρικούς πελάτες με χαμηλό κόστος, επιτρέποντας ταυτόχρονα οι πελάτες αυτοί να αποκτήσουν τα ίδια οφέλη από την εμπορική άδεια, λειτουργώντας στο εσωτερικό του λογισμικού χωρίς τη σχετική πολυπλοκότητα της εγκατάστασης, τη διαχείριση, την υποστήριξη, τη χορήγηση αδειών και το υψηλό αρχικό κόστος. Η αρχιτεκτονική των SaaS εφαρμογών έχει σχεδιαστεί ειδικά για να υποστηρίξει πολλούς ταυτόχρονους χρήστες (multitenancy) την ίδια στιγμή. Οι εφαρμογές του λογισμικού ως υπηρεσία, είναι προσβάσιμες μέσω web browsers από το διαδίκτυο, ως εκ τούτου η ασφάλεια του web browser είναι ζωτικής σημασίας. Οι ειδικοί ασφάλειας των πληροφοριών θα πρέπει να εξετάσουν διάφορες μεθόδους εξασφάλισης των SaaS εφαρμογών. Ασφάλεια διαδικτυακών υπηρεσιών - Web Services security (WS), Extendable Markup Language (XML), Secure Socket Layer (SSL) και διαθέσιμες επιλογές που χρησιμοποιούνται για την ενίσχυση της προστασίας των δεδομένων, μεταδίδονται μέσω του διαδικτύου [26].

Συνδυάζοντας τα τρία είδη των νεφών με τα μοντέλα υπηρεσιών, υπάρχει μια ολιστική εικόνα του νέφους, που περιβάλλεται από συσκευές σύνδεσης σε συνδυασμό με τις πληροφορίες σε θέματα ασφαλείας. Εικονικοί φυσικοί πόροι, εικονικές υποδομές, καθώς και εικονικές πλατφόρμες και επιχειρηματικές εφαρμογές, παρέχονται και καταναλώνονται ως υπηρεσίες στο νέφος [44]. Οι προμηθευτές νέφους αλλά και οι πελάτες, έχουν την ανάγκη να διατηρούν την ασφάλεια του υπολογιστικού νέφους σε όλες τις διασυνδέσεις.

Network-as-a-Service (NaaS) – (Το δίκτυο ως υπηρεσία)

Το δίκτυο ως υπηρεσία, περιγράφει υπηρεσίες για τη συνδεσιμότητα του δικτύου. Περιλαμβάνει τη βελτιστοποίηση της κατανομής των πόρων με την εξέταση δικτυακών και υπολογιστικών πόρων ως ένα ενιαίο σύνολο.

Ο όρος «Δίκτυο ως υπηρεσία» (NaaS) χρησιμοποιείται συχνά σε συνδυασμό με άλλους όρους μάρκετινγκ όπως το υπολογιστικό νέφος (cloud computing), μαζί με ακρωνύμια όπως «η υποδομή ως υπηρεσία» (IaaS), «η πλατφόρμα ως υπηρεσία» (PaaS), και «το λογισμικό ως υπηρεσία» (SaaS) [3].

Το δίκτυο ως υπηρεσία, μερικές φορές περιλαμβάνει την παροχή μιας εικονικής υπηρεσίας δικτύου από τους ιδιοκτήτες της υποδομής του δικτύου σε τρίτους. Επίσης, συχνά περιλαμβάνει και την εικονοποίηση του δικτύου, χρησιμοποιώντας ένα πρωτόκολλο όπως το OpenFlow[2] (ανοιχτής ροής) (SDN)[3].

Μερικά μοντέλα υπηρεσιών είναι:

Το Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network (VPN)): Επεκτείνει ένα ιδιωτικό δίκτυο και τους πόρους που περιέχονται σε αυτό σε όλα τα δίκτυα, όπως το δημόσιο Internet. Επιτρέπει σε έναν υπολογιστή να στέλνει και να λαμβάνει δεδομένα μέσω κοινόχρηστων ή δημόσιων δικτύων σαν να ήταν ένα ιδιωτικό δίκτυο με τη λειτουργικότητα και τις πολιτικές του ιδιωτικού δικτύου [12].

Το εύρος ζώνης-φάσμα σε πρώτη ζήτηση (Bandwidth on demand (BoD)): Τεχνική με την οποία η χωρητικότητα του δικτύου αποδίδεται με βάση τις απαιτήσεις μεταξύ των διαφόρων κόμβων ή χρηστών. Σύμφωνα με αυτό το μοντέλο τα

[2] Το OpenFlow είναι ένα ανοιχτό πρότυπο που επιτρέπει στους ερευνητές να τρέξουν πειραματικά πρωτόκολλα στα πανεπιστημιακά δίκτυα. Προστίθεται ως χαρακτηριστικό σε εμπορικά ethernet switches, σε δρομολογητές και σημεία ασύρματης πρόσβασης και παρέχει ένα τυποποιημένο περιβάλλον για να επιτρέπει στους ερευνητές να διεξάγουν πειράματα, χωρίς να απαιτείται από τους πωλητές να εκθέτουν την εσωτερική λειτουργία των συσκευών δικτύου τους.

[3] Το λογισμικό ορισμένης δικτύωσης (SDN), είναι μια προσέγγιση για τη δικτύωση των υπολογιστών, που επιτρέπει στους διαχειριστές του δικτύου να διαχειρίζονται τις υπηρεσίες του δικτύου μέσω της αφαίρεσης της λειτουργικότητας χαμηλότερου επίπεδου. Αυτό γίνεται με την αποσύνδεση του συστήματος το οποίο λαμβάνει αποφάσεις σχετικά με το πού αποστέλλεται η κυκλοφορία (το επίπεδο ελέγχου) από τα υποκείμενα συστήματα που διαβιβάζουν τη κίνηση προς τον επιλεγμένο προορισμό (το επίπεδο των δεδομένων). Οι εφευρέτες και οι προμηθευτές αυτών των συστημάτων ισχυρίζονται ότι αυτό απλοποιεί τη δικτύωση. Το SDN απαιτεί κάποια μέθοδο για το επίπεδο ελέγχου ώστε να επικοινωνεί με το επίπεδο δεδομένων. Ένας τέτοιος μηχανισμός, OpenFlow, συχνά παρερμηνεύεται να είναι ισοδύναμος με SDN, αλλά άλλοι μηχανισμοί θα μπορούσαν επίσης να ενταχθούν στην έννοια.

ποσοστά σύνδεσης μπορεί να προσαρμοστούν δυναμικά στις απαιτήσεις κίνησης των κόμβων που συνδέονται με το σύνδεσμο.

Η εικονοποίηση του δικτύου κινητής τηλεφωνίας: Μοντέλο στο οποίο ένας κατασκευαστής τηλεπικοινωνιών ή ανεξάρτητος διαχειριστής του δικτύου κατασκευάζει και λειτουργεί ένα δίκτυο (ασύρματο ή συνδεσιμότητα μεταφοράς) και πουλάει τις δυνατότητες πρόσβασης της επικοινωνίας του σε τρίτους (συνήθως εταιρείες κινητής τηλεφωνίας) χρεώνοντας με βάση την χρησιμοποίηση της χωρητικότητας. Ένας φορέας εικονικού δικτύου κινητής (MVNO), είναι ένας πάροχος υπηρεσιών επικοινωνίας κινητής, που δεν κατέχει το ραδιοφάσμα ή την ασύρματη υποδομή δικτύου μέσω της οποίας παρέχει τις υπηρεσίες του. Συνήθως ένας φορέας εικονικού δικτύου κινητής προσφέρει τις υπηρεσίες επικοινωνίας, χρησιμοποιώντας την υποδομή του δικτύου ενός εγκατεστημένου φορέα δικτύου κινητής τηλεφωνίας [42].

Οι λειτουργίες εικονοποίησης δικτύου (NFV-Network Functions Virtualization): Οι λειτουργίες εικονοποίησης δικτύου (NFV) είναι μια αρχιτεκτονική έννοια του δικτύου, που προτείνει τη χρήση της πληροφορικής και συναφών τεχνολογιών εικονοποίησης, για την εικονικοποίηση λειτουργιών ολόκληρων τάξεων κόμβου του δικτύου, σε δομικά στοιχεία που μπορούν να συνδεθούν μαζί για να δημιουργήσουν υπηρεσίες επικοινωνίας.

Η εικονοποίηση δικτύου προσφέρει ένα νέο τρόπο για το σχεδιασμό, την ανάπτυξη και την διαχείριση των υπηρεσιών δικτύωσης. Το NFV διαχωρίζει τις λειτουργίες του δικτύου, όπως η μετάφραση διευθύνσεων δικτύου (NAT), το firewalling, η ανίχνευση εισβολής, το όνομα του τομέα των υπηρεσιών (DNS), την προσωρινή αποθήκευση, κ.λπ., από ιδιόκτητες συσκευές υλικού, έτσι ώστε να μπορεί να τρέξει το λογισμικό. Έχει σχεδιαστεί για να εδραιώσει και να παραδώσει τα στοιχεία δικτύου που απαιτούνται, για να υποστηρίξουν μια πλήρως εικονοποιημένη υποδομή - συμπεριλαμβανομένων των εικονικών servers, την αποθήκευση και ακόμη και άλλα δίκτυα. Μπορεί να εφαρμοστεί σε οποιαδήποτε επεξεργασία δεδομένων ή έλεγχο λειτουργιών, τόσο σε ενσύρματες όσο και ασύρματες δικτυακές υποδομές [30].

Τα πλεονεκτήματα του NFV είναι :

- η μείωση του CapEx: μειώνοντας την ανάγκη για την αγορά του σκοπού κατασκευής υλικού και την υποστήριξη pay-as-you μοντέλων, για την εξάλειψη της σπατάλης άνω των προβλέψεων.
- Η μείωση του OpEX: μειώνοντας χώρους, δύναμη και απαιτήσεις ψύξης του εξοπλισμού και απλουστεύοντας την εξάπλωση και τη διαχείριση των υπηρεσιών δικτύου.
- Η επιτάχυνση του χρόνου αγοράς: μειώνοντας το χρόνο για την ανάπτυξη νέων υπηρεσιών δικτύωσης, για την υποστήριξη των μεταβαλλόμενων απαιτήσεων των επιχειρήσεων, αξιοποιώντας νέες ευκαιρίες αγοράς και βελτιώνοντας την απόδοση των επενδύσεων των νέων υπηρεσιών. Επίσης, μειώνει τους κινδύνους που συνδέονται με την εξάπλωση νέων υπηρεσιών, επιτρέποντας στους παρόχους την εύκολη δοκιμή και εξέλιξη των υπηρεσιών, ώστε να καθορίσουν τι ανταποκρίνεται καλύτερα στις ανάγκες των πελατών.
- Ευελιξία: αναβαθμίζοντας γρήγορα προς τα πάνω ή προς τα κάτω τις υπηρεσίες για την αντιμετώπιση των μεταβαλλόμενων απαιτήσεων, στηρίζοντας την καινοτομία, επιτρέποντας υπηρεσίες που θα παρέχονται μέσω του λογισμικού σε κάθε πελάτη.

1.3 Κύρια Χαρακτηριστικά των Υπολογιστικών Νεφών

Ένας άλλος τρόπος ορισμού του υπολογιστικού νέφους, είναι να εξεταστούν τα χαρακτηριστικά του, ειδικά αυτά που έχουν συμφωνηθεί και είναι γενικά αποδεκτά από διαφορετικές ομάδες:

- Κοινόχρηστοι πόροι: ή ό,τι καλείται συγκέντρωση πόρων, όπου δεν υπάρχουν πόροι που διατίθενται για ένα χρήστη, αλλά αντ 'αυτού συγκεντρώνονται μαζί για να εξυπηρετήσουν πολλαπλούς καταναλωτές. Πόροι είτε για την εφαρμογή, υποδοχής ή επίπεδου δικτύου, έχουν ανατεθεί και εκ νέου ανατεθεί, ανάλογα με τις ανάγκες των καταναλωτών. Αυτό δημιουργεί μια αίσθηση ανεξαρτησίας της

τοποθεσίας, όπου οι χρήστες δεν μπορούν να εντοπίσουν πού ακριβώς εκτελούνται οι υπολογισμοί [52].

- On-demand αυτοεξυπηρέτηση: οι χρήστες μπορούν να αντιστοιχίσουν στους εαυτούς τους πρόσθετους πόρους, όπως αποθήκευση ή επεξεργαστική ισχύ αυτόματα, χωρίς ανθρώπινη παρέμβαση. Αυτό είναι συγκρίσιμο με την αυτόνομη υπολογιστική, όπου το σύστημα υπολογιστών είναι ικανό αυτοδιαχείρισης.
- Ελαστικότητα: μαζί με την αυτοτροφοδότηση των πόρων, το υπολογιστικό νέφος χαρακτηρίζεται από την ικανότητα να εντοπίζει και να απελευθερώσει πόρους γρήγορα. Αυτό θα επιτρέπει στους καταναλωτές να αναβαθμίσουν τους πόρους που χρειάζονται, ανά πάσα στιγμή να αντιμετωπίζουν βαριά φορτία και αιχμές χρήσης και στη συνέχεια, κλιμάκωση προς τα κάτω με την επιστροφή των πόρων στην πισίνα όταν τελειώσει.
- Pay as you go: ή αυτό που είναι γνωστό όπως μετρήσιμη υπηρεσία. Η υπολογιστική στο νέφος προσφέρεται ως ένα βοηθητικό πρόγραμμα το οποίο οι χρήστες πληρώνουν για την βάση της κατανάλωσης, σε αντίθεση δε, με οποιαδήποτε άλλη επιχείρηση κοινής ωφέλειας όπως, η ηλεκτρική ενέργεια, το φυσικό αέριο και το νερό.

Θα μπορούσε να υποστηριχθεί ότι το κύριο χαρακτηριστικό του υπολογιστικού νέφους είναι ότι ο υπολογισμός γίνεται με το "σύννεφο" και τα υπόλοιπα χαρακτηριστικά προέρχονται από, ή συμπληρώνουν αυτό το απλό γεγονός. Πρόσθετα χαρακτηριστικά έχουν επίσης αναφερθεί στη βιβλιογραφία, αλλά τα περισσότερα από αυτά είναι συμπληρωματικά προς τα κύρια χαρακτηριστικά που αναφέρθησαν παραπάνω [67].

1.4 Πλεονεκτήματα

Το υπολογιστικό νέφος βασίζεται στην κατανομή των πόρων για την επίτευξη της συνοχής και της οικονομίας κλίμακας, παρόμοια με ένα βοηθητικό πρόγραμμα (όπως το δίκτυο ηλεκτρικής ενέργειας) σε ένα δίκτυο [66]. Στη βάση του

υπολογιστικού νέφους είναι η ευρύτερη έννοια της σύγκλισης των υποδομών και των κοινών υπηρεσιών.

Το νέφος, επικεντρώνεται επίσης στη μεγιστοποίηση της αποτελεσματικότητας των κοινών πόρων. Οι πόροι του νέφους, δεν μοιράζονται συνήθως μόνο από πολλαπλούς χρήστες, αλλά επίσης ανακατανέμονται δυναμικά ανάλογα με την ζήτηση. Αυτό μπορεί να λειτουργήσει για την κατανομή των πόρων στους χρήστες. Για παράδειγμα, μια εγκατάσταση ηλεκτρονικών υπολογιστών νέφους που διατίθεται για ευρωπαίους χρήστες κατά τη διάρκεια των Ευρωπαϊκών εργάσιμων ωρών με μια συγκεκριμένη εφαρμογή (π.χ., e-mail), μπορεί να διαθέσει τους ίδιους πόρους για να εξυπηρετήσει χρήστες στη Βόρεια Αμερική κατά τις εργάσιμες ώρες της Βόρειας Αμερικής με μια άλλη εφαρμογή (π.χ., έναν web server). Η προσέγγιση αυτή θα πρέπει να μεγιστοποιήσει τη χρήση της υπολογιστικής ισχύος, μειώνοντας έτσι τις περιβαλλοντικές ζημίες, καθώς θα χρειάζεται λιγότερη ενέργεια, για κλιματισμό, κ.λπ. για μια ποικιλία λειτουργιών. Με το υπολογιστικό νέφος, πολλοί χρήστες μπορούν να έχουν πρόσβαση σε έναν διακομιστή για να ανακτούν και ενημερώνουν τα δεδομένα τους χωρίς να αγοράζουν άδειες για διαφορετικές εφαρμογές. Ο όρος «κινείται σε σύννεφο» αναφέρεται επίσης σε μια οργάνωση που κινείται μακριά από το παραδοσιακό μοντέλο CAPEX (Capital Expenditure) (αγόρασε το ειδικό υλικό και υποτίμησέ το πάνω από ένα χρονικό διάστημα) στο μοντέλο OPEX[4] (Operational Expenditure) (χρησιμοποίησε μια κοινή υποδομή cloud και πλήρωσέ το όσο το χρησιμοποιεις).

Οι υποστηρικτές ισχυρίζονται ότι το υπολογιστικό νέφος επιτρέπει στις εταιρείες να αποφύγουν εκ των προτέρων το κόστος της υποδομής, με έμφαση σε έργα που διαφοροποιούν τις επιχειρήσεις τους αντί των υποδομών [1]. Οι υποστηρικτές ισχυρίζονται επίσης ότι το υπολογιστικό νέφος επιτρέπει στις επιχειρήσεις να πάρουν τις εφαρμογές τους και να λειτουργήσουν πιο γρήγορα, με βελτιωμένη διαχειρισιμότητα και λιγότερη συντήρηση, και δίνει τη δυνατότητα για ταχύτερη προσαρμογή των πόρων για την κάλυψη διακυμάνσεων και απρόβλεπτη ζήτηση των επιχειρήσεων [6][53]. Οι πάροχοι νέφους, συνήθως χρησιμοποιούν ένα «pay

[4] Το μοντέλο OPEX αναφέρεται σε ένα συνεχές κόστος για τη λειτουργία ενός προϊόντος, μιας επιχείρησης, ή συστήματος.

as you go» μοντέλο. Αυτό μπορεί να οδηγήσει σε απροσδόκητα υψηλές χρεώσεις, εάν οι διαχειριστές δεν προσαρμοστούν στο μοντέλο τιμολόγησης του νέφους [15].

1.5 Μειονεκτήματα

Αν και τα πλεονεκτήματα του υπολογιστικού νέφους που αναφέρθησαν παραπάνω είναι σημαντικά, εντούτοις υπάρχουν και σημαντικά μειονεκτήματα που περιγράφονται παρακάτω.

- Ένα από τα σημαντικότερα μειονεκτήματα χωρίς καμία αμφιβολία είναι η ιδιωτικότητα και η ασφάλεια των δεδομένων. Αυτό συμβαίνει διότι τα δεδομένα του οργανισμού μεταφέρονται σε συστήματα που δεν είναι πλέον υπό τον έλεγχό του. Αυτό έχει ως αποτέλεσμα να υπάρχει κίνδυνος να τελεστεί αδίκημα από τρίτους. Για τον λόγο αυτό, δεν μπορεί κάποιος να εμπιστευτεί απόλυτα έναν πάροχο νέφους να διατηρήσει την ιδιωτικότητα των δεδομένων ενός οργανισμού, αν και το νομοθετικό και κανονιστικό πλαίσιο είναι αυστηρό [7].
- Όπως είναι γενικώς αποδεκτό, τα πλεονεκτήματα του υπολογιστικού νέφους έχουν να κάνουν με τους μικρότερους οργανισμούς παρά με τους μεγάλους. Οι μεγάλοι οργανισμοί έχουν τη δυνατότητα να υποστηρίξουν προσωπικό πληροφορικής και ενέργειες σχεδίασης κατάλληλου λογισμικού για τις ιδιαίτερες ανάγκες τους.
- Όταν χρησιμοποιείται μια εφαρμογή ή μια υπηρεσία στο νέφος, χρησιμοποιείται κάτι που δεν είναι απαραιτήτως τόσο εξατομικευμένο (τουλάχιστον στο βαθμό που ενδεχομένως κάποιος επιθυμεί). Επιπλέον, αν και πολλές εφαρμογές υπολογιστικού νέφους είναι πολύ εξελιγμένες, οι «παραδοσιακές» εφαρμογές που αναπτύσσονται από διάφορες εταιρείες έχουν πολλές λειτουργίες που δεν περιλαμβάνονται σε εκείνες που είναι διαθέσιμες εντός του υπολογιστικού νέφους.
- Το υπολογιστικό νέφος είναι ένα άναρχο σύστημα, όπως είναι το Διαδίκτυο σε γενικές γραμμές. Όλα τα αιτήματα που υποστηρίζονται

από το πρωτόκολλο HTTP (PUT, GET, κ.ά.) είναι αιτήματα σε έναν πάροχο υπηρεσιών, ο οποίος τα επεξεργάζεται και στη συνέχεια στέλνει μια απάντηση. Κατόπιν ο εξυπηρετούμενος μπορεί να αποστείλει νέο αίτημα και να λάβει νέα απάντηση κ.ο.κ. Αν και μπορεί να μοιάζει ότι συνεχίζεται μια συνομιλία μεταξύ του πελάτη και του παρόχου, στην ουσία υπάρχει μια αρχιτεκτονική αποσύνδεση μεταξύ διαφορετικών αιτημάτων, η οποία εισάγει μία έλλειψη κατάστασης, που έχει με τη σειρά της ως αποτέλεσμα τα μηνύματα να ταξιδεύουν σε διαφορετικές διαδρομές και τα δεδομένα να φθάνουν χωρίς αλληλουχία. Επομένως, για να επιβληθεί η συνοχή των δοσοληψιών στο σύστημα, χρειάζεται να προστεθούν ορισμένες τεχνικές, κυρίως με τη μορφή μεσιτών υπηρεσιών, διαχειριστών δοσοληψιών κ.λπ. Αυτό στη συνέχεια μπορεί να επηρεάσει κατά πολύ την απόδοση ορισμένων εφαρμογών.

- Σήμερα, οι περισσότεροι οργανισμοί βρίσκονται αντιμέτωποι με νομοθετικά και κανονιστικά ζητήματα που αφορούν τη λειτουργία τους. Στην Ευρώπη, η Ευρωπαϊκή Ένωση (Ε.Ε) έχει μια σειρά από δικές της νομοθεσίες σχετικά με τις επιχειρήσεις. Η επέκταση ενός υπολογιστικού νέφους μεταξύ διαφόρων χωρών μπορεί να έχει το μειονέκτημα της συμμόρφωσης με μια σειρά διαφορετικών νόμων (ανάλογα με το τι ισχύει στη κάθε χώρα) και κατά συνέπεια τα ένδικα μέσα (π.χ. η προσφυγή κατά του παρόχου νέφους για ένα θέμα παραβίασης ιδιωτικότητας) δεν είναι απόλυτα σαφές με ποιά νομοθεσία θα κριθούν. Οι νόμοι και οι ρυθμιστικές διατάξεις των περισσότερων χωρών τοποθετούν ολόκληρο το φορτίο ευθύνης επάνω στον πελάτη [24].

Κεφάλαιο 2
Η Ασφάλεια στο Υπολογιστικό Νέφος

2.1 Θέματα ασφάλειας που συνδέονται με το υπολογιστικό νέφος

Υπάρχει μια σειρά από θέματα ασφάλειας που σχετίζονται με το υπολογιστικό νέφος. Τα θέματα αυτά κατατάσσονται σε κατηγορίες όπως: τα θέματα ασφάλειας που αντιμετωπίζουν οι πάροχοι του υπολογιστικού νέφους και τα θέματα ασφάλειας που αντιμετωπίζουν οι πελάτες τους. Στις περισσότερες περιπτώσεις, ο πάροχος πρέπει να εξασφαλίσει ότι οι υποδομές του είναι ασφαλείς και ότι τα δεδομένα και οι εφαρμογές του πελάτη του προστατεύονται, ενώ ο πελάτης πρέπει να εξασφαλίσει ότι ο πάροχος έχει λάβει τα κατάλληλα μέτρα ασφαλείας για την προστασία των πληροφοριών του.

Η παρακάτω λίστα περιέχει διάφορα ζητήματα ασφάλειας, όπως παρουσιάζονται από τον Gartner [8]:

- Προνομιακή πρόσβαση: Ποιος έχει ειδικευτεί / έχει προνομιακή πρόσβαση στα δεδομένα; Ποιος αποφασίζει σχετικά με την πρόσληψη και τη διαχείριση των εν λόγω διαχειριστών;
- Τοποθεσία δεδομένων: Επιτρέπει ο προμηθευτής του νέφους κάθε έλεγχο πάνω από τη θέση των δεδομένων;

- Διαχωρισμός των δεδομένων: Είναι η κρυπτογράφηση διαθέσιμη σε όλα τα στάδια και όλα αυτά τα συστήματα κρυπτογράφησης σχεδιάστηκαν και δοκιμάστηκαν από έμπειρους επαγγελματίες;
- Διαθεσιμότητα των δεδομένων: Εφόσον ο πάροχος του νέφους μετακινήσει όλα τα δεδομένα του πελάτη σε διαφορετικό περιβάλλον, θα έπρεπε το υπάρχον περιβάλλον να γίνει επικίνδυνο ή μη διαθέσιμο;
- Κανονιστική συμμόρφωση: Είναι ο προμηθευτής του νέφους πρόθυμος να υποβληθεί σε εξωτερικούς ελέγχους ή / και πιστοποιήσεις ασφάλειας (όπως την επικύρωση αξιολόγησης νέφους: Cloud Validation Assessment);
- Ανάκτηση: Τι συμβαίνει με τα δεδομένα στην περίπτωση μιας καταστροφής; Και ο προμηθευτής προσφέρει πλήρη αποκατάσταση, και αν ναι, πόσο καιρό παίρνει αυτή η διαδικασία;
- Έλεγχος Παράνομης Δραστηριότητας: Έχει ο προμηθευτής τη δυνατότητα να διερευνήσει οποιαδήποτε ανάρμοστη ή παράνομη δραστηριότητα συμβαίνει στο νέφος;
- Μακροπρόθεσμη βιωσιμότητα: Τι συμβαίνει με τα δεδομένα αν ο πάροχος του νέφους βγει από την επιχείρηση, επιστρέφονται τα στοιχεία του πελάτη και σε ποια μορφή;

2.1.1 Θέματα ασφάλειας βασιζόμενα στα μοντέλα υπηρεσιών και διάθεσης

Στην SaaS, οι πάροχοι είναι πιο υπεύθυνοι για την ασφάλεια. Οι πελάτες πρέπει να εξαρτώνται από τους παρόχους για τα μέτρα ασφαλείας. Δεδομένου ότι το δημόσιο νέφος είναι λιγότερο ασφαλές από το ιδιωτικό νέφος, τα ισχυρότερα μέτρα ασφαλείας απαιτούνται στα δημόσια νέφη. Επίσης, στην SaaS, καθίσταται δύσκολο για τον χρήστη να διασφαλίσει ότι διατηρείται η σωστή ασφάλεια ή όχι. Τα ιδιωτικά νέφη θα μπορούσαν επίσης να απαιτήσουν περισσότερη επεκτασιμότητα για να φιλοξενήσουν προσαρμοσμένες απαιτήσεις. Τα παρακάτω βασικά στοιχεία ασφαλείας [63] θα πρέπει να εξεταστούν προσεκτικά ως αναπόσπαστο μέρος της διαδικασίας ανάπτυξης εφαρμογών και ανάπτυξης SaaS:

i. Η ασφάλεια των δεδομένων (Data security)
ii. Η τοποθεσία των δεδομένων (Data locality)
iii. Η ακεραιότητα των δεδομένων (Data integrity)
iv. Ο διαχωρισμός των δεδομένων (Data segregation)
v. Η πρόσβαση στα δεδομένα (Data access)
vi. Η εμπιστευτικότητα των δεδομένων (Data confidentiality)
vii. Η ασφάλεια των δικτύων (Network security)
viii. Επαλήθευση ταυτότητας και αδειοδότηση (Authentication and authorization)
ix. Διαθεσιμότητα (Availability)
x. Η διαχείριση ταυτότητας και η διαδικασία εγγραφής (Identity management and sign-on process)

Στην PaaS, οι πελάτες έχουν τη δυνατότητα να δημιουργήσουν τις δικές τους εφαρμογές πάνω από τις πλατφόρμες που παρέχονται. Έτσι, είναι ευθύνη των πελατών να προστατεύσουν τις εφαρμογές τους, ενώ οι πάροχοι είναι υπεύθυνοι μόνο για την απομόνωση των εφαρμογών και των χώρων εργασίας των πελατών του ενός από τον άλλο. Έτσι, η διατήρηση της ακεραιότητας των εφαρμογών και η επιβολή των ελέγχων ταυτότητας, είναι οι βασικές απαιτήσεις ασφάλειας στην PaaS.

Το IaaS χρησιμοποιείται κυρίως ως ένα μοντέλο παράδοσης. Το κύριο μέλημα της ασφάλειας στο IaaS, είναι να διατηρεί τον έλεγχο επί των στοιχείων του πελάτη που αποθηκεύονται στο σκληρό δίσκο του παρόχου. Οι καταναλωτές είναι υπεύθυνοι για την ασφάλεια των λειτουργικών συστημάτων, των εφαρμογών και του περιεχομένου. Ο πάροχος του νέφους πρέπει να παρέχει χαμηλού επιπέδου δυνατότητες προστασίας των δεδομένων [64].

Ανάλυση των κυριότερων απειλών στο υπολογιστικό νέφος και αντιμετώπισή τους

Κυριότερες απειλές στο υπολογιστικό νέφος	Ανάλυση	Αντιμετώπιση	Service models
1) Κακόβουλη χρήση του υπολογιστικού νέφους	Οι πάροχοι του Infrastructure as a Service (IaaS) προσφέρουν στους πελάτες τους την ψευδαίσθηση της απεριόριστης υπολογιστικής, δικτυακής και αποθηκευτικής χωρητικότητας, σε συνδυασμό με την προβολή μιας πολύ εύκολης διαδικασίας εγγραφής κατά την οποία κάθε απλός κάτοχος μιας πιστωτικής κάρτας δύναται άμεσα να εγγραφεί και να ξεκινήσει να χρησιμοποιεί της υπηρεσίες του υπολογιστικού νέφους. Επιπλέον, κάποιοι πάροχοι προσφέρουν ακόμη και δωρεάν δοκιμαστικές περιόδους περιορισμένης πρόσβασης στις υπηρεσίες. Εκμεταλλευόμενοι λοιπόν τη σχετική ανωνυμία αυτών των διαδικασιών εγγραφής και των μοντέλων χρήσης των υπηρεσιών, οι spammers, οι προγραμματιστές κακόβουλων προγραμμάτων καθώς και πολλοί άλλοι ηλεκτρονικοί εγκληματίες, έχουν τη δυνατότητα να διεξάγουν τις δραστηριότητές τους με ασυδοσία. Οι πάροχοι που υπέφεραν παραδοσιακά από τέτοιου είδους επιθέσεις είναι αυτοί των Platform as a Service (PaaS). Ωστόσο, πρόσφατες έρευνες δείχνουν ότι πλέον οι hackers έχουν αρχίσει να στοχεύουν και σε IaaS.	1) Αυστηρότερες διαδικασίες που αφορούν στην αρχική εγγραφή και την επικύρωση της ταυτότητας των χρηστών των υποδομών Υπολογιστικού Νέφους. 2) Ενισχυμένες διαδικασίες και καλύτερος συντονισμός αναφορικά με λειτουργίες ελέγχου απάτης. 3) Αυξημένες διαδικασίες παρακολούθησης και ελέγχου με σκοπό την αποκάλυψη περιπτώσεων μη εξουσιοδοτημένης χρήσης των υποδομών του Υπολογιστικού Νέφους αναφορικά με τα δεδομένα του φορέα και της επιχείρησης. 4) Παρακολούθηση των «μαύρων λιστών» που αφορούν στα κακόβουλα δίκτυα	**IaaS, PaaS**

		και έχουν δοθεί δημοσίως.	
2) Επισφαλείς διεπαφές προγραμματισμού εφαρμογών (APIs)	Οι πάροχοι υπηρεσιών για το υπολογιστικό νέφος, προσφέρουν μια σειρά από διεπαφές περιβάλλοντος στο χρήστη, μέσω των οποίων οι πελάτες διαχειρίζονται και αλληλεπιδρούν με τις υπηρεσίες του νέφους. Η τροφοδότηση, η διαχείριση, η ενορχήστρωση καθώς και η παρακολούθηση εκτελούνται χρησιμοποιώντας αυτές τις διασυνδέσεις. Επομένως, η ασφάλεια και η διαθεσιμότητα γενικώς των υπηρεσιών νέφους, είναι άμεσα εξαρτώμενες από την ασφάλεια σε αυτές τις βασικές διεπαφές. Καθώς στην όλη υπόθεση εμπλέκονται σοβαρά ζητήματα αυθεντικοποίησης, ελέγχου πρόσβασης, κρυπτογράφησης και παρακολούθησης των διεργασιών, οι διεπαφές πρέπει να σχεδιάζονται έτσι ώστε να προστατεύουν το σύστημα τόσο από τυχαίες όσο και από κακόβουλες προσπάθειες καταστρατήγησης.	1) Ανάλυση του μοντέλου ασφάλειας της διασύνδεσης χρήστη του παρόχου. 2) Αυστηρή αυθεντικοποίηση και έλεγχος πρόσβασης σε συνδυασμό με κρυπτογραφημένη μετάδοση δεδομένων μέσω των APIs. 3) Πλήρης κατανόηση της λειτουργίας αλλά και των αλληλεξαρτήσεων που αφορούν στη χρήση των APIs.	**IaaS, PaaS, SaaS**
3) Κακόβουλοι χρήστες από την πλευρά του παρόχου	Η απειλή «εκ των έσω» είναι ένα πολύ γνωστό πρόβλημα για τους οργανισμούς. Η απειλή του «ανθρώπινου παράγοντα» ενισχύεται για τους πελάτες υπηρεσιών υπολογιστικού νέφους λόγω του ότι υπόκεινται σε ένα κοινό σύστημα διαχείρισης σε συνδυασμό με μια γενικότερη έλλειψη διαφάνειας στις διαδικασίες και τις διεργασίες του παρόχου. Το πρόβλημα ενισχύεται όταν συχνά υπάρχει πολύ μικρή έως και καθόλου διαφάνεια στα κριτήρια πρόσληψης των εργαζομένων του οργανισμού. Αυτού του είδους η κατάσταση, προφανώς δημιουργεί μια ελκυστική ευκαιρία για κακόβουλη επίθεση ξεκινώντας από έναν απλό hacker μέχρι και οργανωμένους κυβερνο-εγκληματίες διεθνώς.	1) Καθορισμός απαιτήσεων για το ανθρώπινο δυναμικό όπου αποτελούν μέρος νόμιμων συμβολαίων. 2) Διαφάνεια και πληροφόρηση για την ασφάλεια και τις πρακτικές διαχείρισης. 3) Προσδιορισμός διαδικασιών ενημέρωσης των πελατών από τον πάροχο σε περίπτωση παραβίασης της	**IaaS, PaaS, SaaS**

		ασφάλειας της υποδομής Υπολογιστικού Νέφους.	
4) Ζητήματα τεχνολογίας κοινής χρήσης	Οι πάροχοι του IaaS προσφέρουν τις υπηρεσίες τους με ένα κλιμακούμενο τρόπο μέσω της κοινής χρήσης της υποδομής. Συχνά όμως τα στοιχεία που συνθέτουν αυτή την υποδομή, όπως είναι η CPU και η GPU, δεν έχουν εξαρχής σχεδιαστεί ώστε να προσφέρουν ισχυρή ανεξαρτησία στις ιδιότητές τους. Προκειμένου να καλυφθεί αυτό το κενό, χρησιμοποιείται ένας εικονικός τρόπος πρόσβασης μεταξύ των δευτερευόντων λειτουργικών συστημάτων και των διαθέσιμων φυσικών πόρων. Ωστόσο, ακόμη και αυτή η δίοδος έχει τα μειονεκτήματά της διότι είναι δυνατό τα δευτερεύοντα λειτουργικά συστήματα να αποκτούν έλεγχο ή επιρροή σε μη επιτρεπτά επίπεδα του συστήματος.	1) Εφαρμογή ισχυρών πρακτικών εγκατάστασης και παραμετροποίησης της τεχνολογικής υποδομής. 2) Επίβλεψη του περιβάλλοντος για μη εξουσιοδοτημένες αλλαγές ή δραστηριότητες. 3) Επιβολή ισχυρής αυθεντικοποίησης και ελέγχου πρόσβασης για τον έλεγχο και τις εφαρμογές των διαχειριστών. 4) Επαρκείς διαδικασίες ανάλογα με το επίπεδο της υπηρεσίας για την αντιμετώπιση της ευπάθειας και των κενών ασφαλείας. 5) Εφαρμογή σαρώσεων ευπάθειας και ελέγχου ρυθμίσεων των υποδομών Υπολογιστικού Νέφους.	**IaaS**
5) Απώλεια ή διαρροή δεδομένων	Υπάρχουν πολλοί τρόποι για την απώλεια των δεδομένων. Η διαγραφή και η αλλαγή των εγγραφών χωρίς να υπάρχει εφεδρικό αντίγραφο είναι δύο προφανή παραδείγματα. Επίσης, η απώλεια ενός κλειδιού κωδικοποίησης μπορεί να	1) Υιοθέτηση αυστηρού ελέγχου πρόσβασης στα APIs. 2) Κρυπτογράφηση και προστασία της ακεραιότητας των	**IaaS, PaaS, SaaS**

	προκαλέσει την καταστροφή, ενώ θα πρέπει να προλαμβάνεται η πρόσβαση μη εξουσιοδοτημένων οντοτήτων σε ευαίσθητα δεδομένα. Η απώλεια ή η διαρροή δεδομένων ενδέχεται να έχει καταστροφικό αντίκτυπο σε μια επιχείρηση. Επιπροσθέτως, η απώλεια ζωτικής σημασίας δεδομένων, ενδέχεται να έχει ιδιαίτερα αρνητικές ανταγωνιστικές και οικονομικές συνέπειες. Στη χειρότερη περίπτωση, ανάλογα με τα στοιχεία που διαρρέουν, μπορεί να υπάρξουν ακόμη και νομικά προβλήματα.	μεταφερόμενων δεδομένων. 3) Προστασία δεδομένων τόσο στη διαδικασία του σχεδιασμού όσο και της εκτέλεσης. 4) Εφαρμογή αυστηρής πολιτικής δημιουργίας κλειδιών κρυπτογράφησης, αποθήκευσης, διαχείρισης και καταστροφής. 5) Καθορισμός της στρατηγικής δημιουργίας αντιγράφων ασφαλείας και της συντήρησης των δεδομένων από τον πάροχο.	
6) Πειρατεία Λογαριασμού ή Υπηρεσίας	Η πειρατεία λογαριασμού ή υπηρεσίας δεν είναι κάτι νέο στο χώρο της τεχνολογίας. Επιθέσεις όπως είναι το phising, η απάτη και η εξερεύνηση των ευπαθειών του λογισμικού ακόμη είναι επιτυχείς. Το πρόβλημα τέτοιων επιθέσεων ενισχύεται με τη συχνή επαναχρησιμοποίηση κωδικών και κλειδιών. Τα υπολογιστικά νέφη και οι λύσεις που προτείνουν φέρνουν νέες απειλές στο προσκήνιο. Έχοντας ως βάση για τις επιθέσεις του το λογαριασμό ενός πελάτη και τις υπηρεσίες που χρησιμοποιεί, ο επιτιθέμενος μπορεί να εκμεταλλευτεί τη δύναμη της φήμης του πελάτη για να εξαπολύσει διαδοχικές επιθέσεις σε ανυποψίαστους χρήστες.	1) Απαγόρευση διαμοιρασμού των στοιχείων λογαριασμών μεταξύ χρηστών και υπηρεσιών. 2) Υιοθέτηση ισχυρών τεχνικών διπλής αυθεντικοποίησης όπου είναι δυνατό. 3) Εγκατάσταση επίβλεψης για την εξεύρεση μη εξουσιοδοτημένων δραστηριοτήτων. 4) Κατανόηση της πολιτικής ασφάλειας κάθε παρόχου	**IaaS, PaaS, SaaS**

		υπηρεσιών υπολογιστικού Νέφους.	
7) Άγνωστο προφίλ κινδύνου	Όταν μια εταιρεία εγγράφεται σε μια υπηρεσία του υπολογιστικού νέφους, τα χαρακτηριστικά και οι λειτουργίες της υπηρεσίας είναι σίγουρα καλά διαφημισμένες αλλά τι συμβαίνει με τις λεπτομέρειες των εσωτερικών διαδικασιών ασφάλειας; Τι συμβαίνει με την παραμετροποίηση, τα κενά ασφαλείας και την αντιμετώπισή τους; Πώς αποθηκεύονται τα δεδομένα και οι σχετικές εγγραφές της εταιρείας και ποιος έχει πρόσβαση σε αυτά; Τι πληροφορίες θα διαρρεύσουν σε περίπτωση προβλήματος ασφάλειας; Πολύ συχνά τέτοιες ερωτήσεις δεν απαντώνται ξεκάθαρα από τους παρόχους ή παραβλέπονται με αποτέλεσμα οι πελάτες να αφήνονται με ένα άγνωστο προφίλ κινδύνου το οποίο φυσικά μπορεί να περιέχει σοβαρές απειλές.	1) Μερική ή πλήρης κοινοποίηση λεπτομερειών της υποδομής (π.χ. τείχη προστασίας, τρόποι αντιμετώπισης κενών ασφαλείας κτλ.) 2) Επίβλεψη και ειδοποίηση για απαραίτητα ζητήματα ασφαλείας	**IaaS, PaaS, SaaS**

Βασιζόμενα στα μοντέλα ανάπτυξης, τα δημόσια νέφη είναι λιγότερο ασφαλή από τα άλλα μοντέλα νεφών, καθώς επιτρέπουν στους χρήστες να έχουν πρόσβαση στα δεδομένα σε δίκτυα ευρείας περιοχής. Στο δημόσιο νέφος, τα πρόσθετα μέτρα ασφάλειας, όπως είναι η εμπιστοσύνη, απαιτούνται για να διασφαλιστεί ότι όλες οι εφαρμογές και τα δεδομένα σχετικά με την πρόσβαση σε δημόσια νέφη δεν υπόκεινται σε κακόβουλες επιθέσεις. Η χρησιμοποίηση του ιδιωτικού νέφους μπορεί να είναι πολύ πιο ασφαλής σε σχέση με το δημόσιο νέφος, όταν καθορίζεται για κάποια συγκεκριμένη οργάνωση. Ένα υβριδικό νέφος είναι ένα ιδιωτικό νέφος που συνδέεται με ένα ή περισσότερα δημόσια νέφη. Τα υβριδικά νέφη παρέχουν πιο ασφαλή έλεγχο των δεδομένων και των εφαρμογών καθώς το καθένα και όλα μαζί είναι σε κεντρική διαχείριση [57].

Α. Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση αποτελεί σημαντική προϋπόθεση για την ασφάλεια των πληροφοριών στο υπολογιστικό νέφος, για να εξασφαλιστεί ότι η ακεραιότητα των αναφορών διατηρείται. Στην περίπτωση των δημόσιων νεφών, πολλοί πελάτες μοιράζονται τους υπολογιστικούς πόρους που παρέχονται από έναν μόνο πάροχο υπηρεσιών. Έτσι, η κατάλληλη εξουσιοδότηση απαιτείται ανεξάρτητα από το μοντέλο παράδοσης που χρησιμοποιείται. Στο ιδιωτικό νέφος, η εξουσιοδότηση διατηρείται από το διαχειριστή του συστήματος.

Β. Αναγνώριση και επαλήθευση ταυτότητας (Identification & authentication)

Επειδή οι μεγάλες ανησυχίες σε δημόσια και ιδιωτικά νέφη περιλαμβάνουν εσωτερικές και εξωτερικές απειλές, (π.χ. συλλογή δεδομένων, ιδιωτικότητας και συμμόρφωσης) έτσι, είναι η ικανότητα του παρόχου υπηρεσιών νέφους να υπάρχει μια ασφαλής υποδομή για την προστασία των δεδομένων των πελατών και την προστασία από μη εξουσιοδοτημένη πρόσβαση. Χρειάζεται να υπάρχουν κάποιες διαδικασίες αναγνώρισης και ταυτοποίησης για την επαλήθευση και την επικύρωση των μεμονωμένων χρηστών του νέφους με βάση τα διαπιστευτήριά τους πριν από την πρόσβαση όλων των δεδομένων πάνω στο νέφος. Αυτός είναι ο λόγος που η αναγνώριση και η ταυτοποίηση είναι υποχρεωτική απαίτηση της ασφάλειας σε δημόσια και ιδιωτικά νέφη.

Γ. Ακεραιότητα (Integrity)

Η απαίτηση της ακεραιότητας έγκειται στην εφαρμογή της δέουσας επιμέλειας μέσα στην περιοχή του νέφους, κυρίως κατά την προσπέλαση των δεδομένων. Ως εκ τούτου (ACID – ατομικότητα (atomicity), συνέπεια (consistency), απομόνωση (isolation), αντοχή (resistance)) οι ιδιότητες των στοιχείων του νέφους θα πρέπει χωρίς αμφιβολία να επιβάλλονται σθεναρά, σε όλα τα μοντέλα υπηρεσιών του υπολογιστικού νέφους.

Δ. Εμπιστευτικότητα (Confidentiality)

Στο υπολογιστικό νέφος, η εμπιστευτικότητα παίζει σημαντικό ρόλο κυρίως στη διατήρηση του ελέγχου πάνω από τα δεδομένα των οργανισμών που βρίσκονται σε πολλαπλές κατανεμημένες βάσεις δεδομένων. Δηλώνοντας την εμπιστευτικότητα των προφίλ των χρηστών και την προστασία των δεδομένων τους, που είναι ουσιαστικά η πρόσβαση, επιτρέπει για πληροφορίες πρωτόκολλα ασφαλείας που πρέπει να εφαρμόζονται σε διάφορα στρώματα των εφαρμογών νέφους.

Η εμπιστευτικότητα των δεδομένων είναι ένα από τα πιο δύσκολα πράγματα για να εγγυηθεί κανείς, σε ένα υπολογιστικό περιβάλλον δημόσιου νέφους. Υπάρχουν πολλοί λόγοι γι' αυτό: Καταρχάς, καθώς το δημόσιο νέφος μεγαλώνει, ο αριθμός των ατόμων που εργάζονται για τον πάροχο του νέφους που έχουν πράγματι πρόσβαση στα στοιχεία του πελάτη (αν έχουν το δικαίωμα σε αυτά ή όχι) επίσης μεγαλώνει, πολλαπλασιάζοντας έτσι τον αριθμό των πιθανών πηγών για την παραβίαση του απορρήτου. Δεύτερον, οι ανάγκες για ελαστικότητα, απόδοση και ανοχή σε σφάλματα οδηγούν σε μαζική επικάλυψη δεδομένων και απαιτεί επιθετική δέσμευση των δεδομένων, η οποία με τη σειρά της πολλαπλασιάζει τον αριθμό των στόχων του «κλέφτη» δεδομένων, που μπορεί να πάει μετά. Τρίτον, η κρυπτογράφηση δεδομένων από άκρο σε άκρο δεν είναι ακόμη διαθέσιμη. Έτσι, η εμπιστευτικότητα των δεδομένων θα πρέπει να μεγιστοποιηθεί με τη χρήση ενός μεγάλου αριθμού ιδιωτικών νεφών να διαχειρίζονται τα μεγαλύτερα κομμάτια.

Ε. Διαθεσιμότητα (Availability)

Η διαθεσιμότητα είναι μια από τις πιο κρίσιμες απαιτήσεις ασφάλειας των πληροφοριών στο υπολογιστικό νέφος, επειδή είναι ένας βασικός παράγοντας

απόφασης όταν αποφασίζεται μεταξύ ιδιωτικού, δημόσιου ή υβριδικού παρόχου νέφους, καθώς και στα μοντέλα υπηρεσιών. Η συμφωνία σε επίπεδο υπηρεσιών είναι το πιο σημαντικό τεκμήριο, το οποίο αναδεικνύει την ταραχή της διαθεσιμότητας υπηρεσιών νέφους και των πόρων μεταξύ του παρόχου του νέφους και του πελάτη.

Ο στόχος της διαθεσιμότητας των συστημάτων υπολογιστικού νέφους (συμπεριλαμβανομένων των εφαρμογών και υποδομών του) είναι να διασφαλίσει ότι οι χρήστες του, μπορούν να τα χρησιμοποιήσουν ανά πάσα στιγμή, σε οποιοδήποτε μέρος. Πολλοί πάροχοι συστημάτων υπολογιστικού νέφους, παρέχουν υποδομές και πλατφόρμες νέφους που βασίζονται σε εικονικές μηχανές (Virtual Machines). Έτσι, η διαθεσιμότητα είναι μια υποχρεωτική απαίτηση ασφαλείας για τα IaaS και PaaS, ανεξάρτητα από το αν χρησιμοποιείται δημόσιο ή ιδιωτικό νέφος. Καθώς στο ιδιωτικό νέφος όλες οι υπηρεσίες είναι εσωτερικές στην επιχείρηση, έτσι η διαθεσιμότητα επίσης απαιτείται όταν είναι να χρησιμοποιηθεί το SaaS.

ΣΤ. Μη-αποκήρυξη (Non-repudiation)

Μη αποκήρυξη στο υπολογιστικό νέφος μπορεί να επιτευχθεί με την εφαρμογή των παραδοσιακών πρωτοκόλλων ασφαλείας ηλεκτρονικού εμπορίου και συμβολικών προβλέψεων για την μετάδοση δεδομένων σε εφαρμογές νέφους (cloud), όπως οι ψηφιακές υπογραφές, χρονοσφραγίδες και η επιβεβαίωση είσπραξης υπηρεσιών (ψηφιακή απόδειξη των μηνυμάτων, που επιβεβαιώνουν τα δεδομένα που αποστέλλονται / παραλαμβάνονται).

2.2 Προκλήσεις ασφάλειας

Τα περιβάλλοντα υπολογιστικού νέφους είναι περιβάλλοντα στα οποία κάθε τομέας μπορεί να χρησιμοποιήσει διαφορετική ασφάλεια, προστασία της ιδιωτικής ζωής, καθώς και απαιτήσεις εμπιστοσύνης, και ενδεχομένως, χρησιμοποιούν διάφορους μηχανισμούς, διασυνδέσεις και σημασιολογία [64]. Οι

κύριες προκλήσεις για την ασφάλεια στο υπολογιστικό νέφος και οι λύσεις τους αναφέρονται παρακάτω.

2.2.1 Συμφωνία σε επίπεδο υπηρεσιών

Μια συμφωνία σε επίπεδο υπηρεσιών (SLA - Service-Level Agreement) [72] είναι ένα μέρος της σύμβασης παροχής υπηρεσιών μεταξύ του καταναλωτή και του παρόχου που ορίζει επισήμως το επίπεδο των υπηρεσιών. Χρησιμοποιείται για να προσδιορίσει και να καθορίσει τις ανάγκες του πελάτη και να μειώσει τους τομείς των συγκρούσεων όπως: οι υπηρεσίες που πρέπει να παραδοθούν, η απόδοση, η παρακολούθηση και η υποβολή εκθέσεων διαχείρισης των προβλημάτων, η νομική συμμόρφωση και η επίλυση των διαφορών, τα καθήκοντα και οι αρμοδιότητες των πελατών, η ασφάλεια και εμπιστευτικές πληροφορίες τερματισμού.

2.2.2 Πιστοποίηση και διαχείριση ταυτότητας

Με τη χρήση των υπηρεσιών νέφους (cloud), ο χρήστης μπορεί να έχει πρόσβαση στις πληροφορίες από διάφορα μέρη μέσω του διαδικτύου. Έτσι, χρειάζεται κάποιος μηχανισμός διαχείρισης ταυτότητας (Identity Management - IDM) [64], για τον έλεγχο ταυτότητας των χρηστών και την παροχή υπηρεσιών προς αυτούς με βάση τα διαπιστευτήρια και τα χαρακτηριστικά. Ένα σύστημα IDM θα πρέπει να είναι σε θέση να προστατεύει ιδιωτικές και ευαίσθητες πληροφορίες σχετικά με τους χρήστες και τις διαδικασίες. Κάθε επιχείρηση θα έχει το δικό της σύστημα διαχείρισης ταυτότητας, για τον έλεγχο της πρόσβασης σε πληροφορίες και υπολογιστικούς πόρους.

2.2.3 Στοιχεία – Κεντρική ασφάλεια και προστασία

Στο υπολογιστικό νέφος, οι χρήστες μπορούν να μοιραστούν, να αποθηκεύσουν και να έχουν πρόσβαση στα δεδομένα μέσω του νέφους. Έτσι, τα δεδομένα από

έναν πελάτη πρέπει να είναι κατάλληλα διαχωρισμένα από εκείνα του άλλου και πρέπει να είναι σε θέση να μετακινούνται με ασφάλεια από το ένα σημείο στο άλλο [40]. Οι πάροχοι υπηρεσιών νέφους (cloud) πρέπει να εφαρμόσουν τα κατάλληλα μέτρα ασφαλείας για την αποτροπή διαρροών δεδομένων ή την πρόσβαση από τρίτα μη εξουσιοδοτημένα πρόσωπα. Ο πάροχος του νέφους θα πρέπει να εκχωρήσει προσεκτικά τα προνόμια στους πελάτες και επίσης να διασφαλίσει ότι τα εκχωρούμενα καθήκοντα δεν μπορούν να καταστρατηγηθούν ακόμη και από προνομιούχους χρήστες του νέφους. Οι πολιτικές ελέγχου πρόσβασης θα πρέπει να εφαρμόζονται σωστά. Όταν κάποιος θέλει να έχει πρόσβαση στα δεδομένα, το σύστημα θα πρέπει να ελέγχει τους κανόνες πολιτικής και να τα αποκαλύπτει μόνο αν οι πολιτικές είναι ικανοποιημένες. Υφιστάμενες κρυπτογραφικές τεχνικές μπορούν επίσης να χρησιμοποιηθούν για την ασφάλεια των δεδομένων.

2.2.4 Διαχείριση εμπιστοσύνης

Σε περιβάλλοντα υπολογιστικού νέφους (cloud computing), ο πελάτης εξαρτάται από τον παροχέα για διάφορες υπηρεσίες. Σε πολλές υπηρεσίες, ο πελάτης πρέπει να αποθηκεύσει τα εμπιστευτικά δεδομένα του στην πλευρά του παρόχου. Έτσι, θα πρέπει να αναπτυχθεί ένα πλαίσιο εμπιστοσύνης, για να καταστεί δυνατή η αποτελεσματική λήψη ενός γενικού συνόλου απαιτούμενων παραμέτρων για τη δημιουργία εμπιστοσύνης και τη διαχείρισή της, όπως επίσης και λοιπών αλληλεπιδράσεων και απαιτήσεων [58].

2.2.5 Έλεγχος πρόσβασης και λογιστικής

Λόγω της ετερογένειας και της ποικιλομορφίας που υπάρχει στον τομέα των υπηρεσιών υπολογιστικού νέφους (cloud computing), θα πρέπει να επιβάλλονται πολύ λεπτές πολιτικές ελέγχου πρόσβασης. Οι υπηρεσίες ελέγχου πρόσβασης θα πρέπει να είναι αρκετά ευέλικτες ώστε να συλλάβουν δυναμικά χαρακτηριστικά ή προσβάσεις βάση πιστοποιητικών. Τα μοντέλα ελέγχου πρόσβασης θα πρέπει επίσης να είναι σε θέση να συλλάβουν σχετικές πτυχές της συμφωνίας σε επίπεδο

υπηρεσιών (SLA's). Εφόσον το μοντέλο του υπολογιστικού νέφους είναι μοντέλο πληρωμή με τη χρήση (pay-per-usage model), απαιτούνται οι κατάλληλες λογιστικές εγγραφές για σκοπούς χρέωσης. Στα νέφη (clouds), οι πάροχοι υπηρεσιών συνήθως δεν γνωρίζουν τους χρήστες εκ των προτέρων, έτσι είναι δύσκολο να ανατεθούν ρόλοι σε χρήστες άμεσα. Ως εκ τούτου, χαρακτηριστικά ή προσβάσεις βάση πιστοποιητικών μπορεί να χρησιμοποιηθούν για να ενισχύσουν αυτή την ικανότητα. Γλώσσα ασφαλείας (Security Assertion Markup Language - SAML), γλώσσα επεκτάσιμου ελέγχου πρόσβασης (Extensible Access Control Markup Language - XACML) και πρότυπα υπηρεσιών δικτύου μπορούν να χρησιμοποιηθούν για να καθορίσουν τις ασφαλείς πολιτικές ελέγχου πρόσβασης. Ανάμεσα στις πολλές μεθόδους που προτείνονται μέχρι στιγμής, ο ελέγχος πρόσβασης βάσει ρόλου (Role-Based Access Control - RBAC) [64], έχει γίνει ευρέως αποδεκτός λόγω της απλότητάς του, της ευελιξίας στη λήψη δυναμικών απαιτήσεων, καθώς και στην υποστήριξη της αρχής των λιγότερων προνομίων και την αποδοτική διαχείριση των προνομίων.

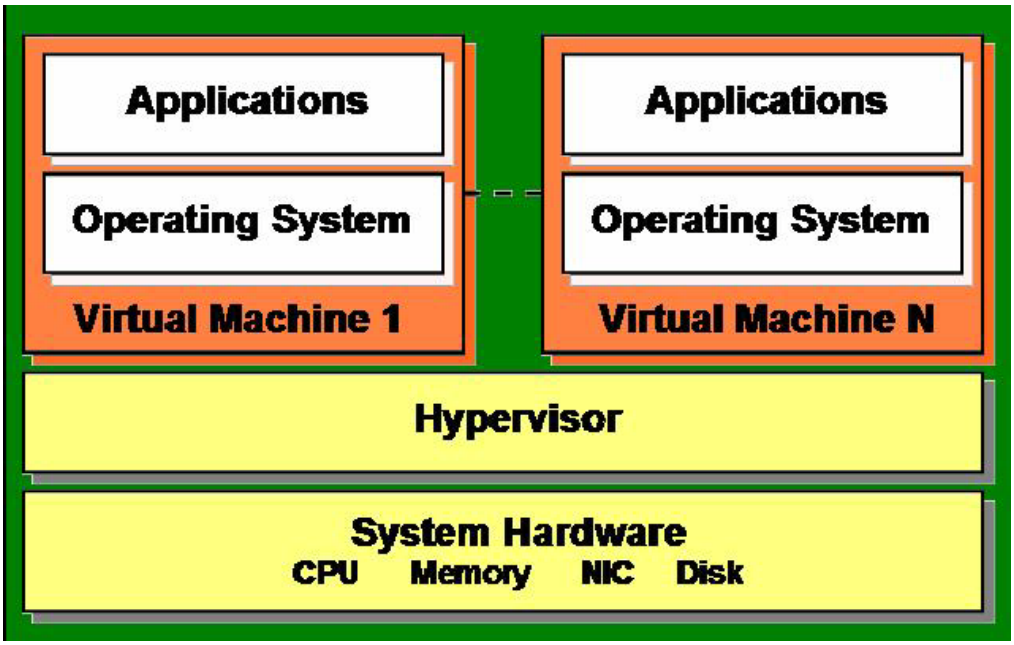
2.3 Εικονοποίηση (Virtualization)

Η εικονοποίηση επιτρέπει στους χρήστες να δημιουργούν, να αντιγράφουν, να μοιράζονται και να επαναφέρουν εικονικές μηχανές, οι οποίες μπορεί να τους επιτρέψουν να εκτελέσουν μια ποικιλία εφαρμογών [51]. Ωστόσο, εισάγονται νέες ευκαιρίες επίθεσης, λόγω του επιπλέον στρώματος που πρέπει να διασφαλιστεί. Η ασφάλεια της εικονικής μηχανής γίνεται εξίσου σημαντική με τη φυσική ασφάλεια του μηχανήματος, καθώς και κάθε ελάττωμα σε κάθε ένα από αυτά, μπορεί να επηρεάσει το άλλο [36]. Τα εικονοποιημένα περιβάλλοντα είναι ευάλωτα σε όλους τους τύπους των επιθέσεων για κανονικές υποδομές, ωστόσο η ασφάλεια είναι η μεγαλύτερη πρόκληση, καθώς η εικονοποίηση προσθέτει περισσότερα σημεία εισόδου και μεγαλύτερη πολυπλοκότητα διασύνδεσης. Σε αντίθεση με τους φυσικούς servers, οι εικονικές μηχανές (VM's) έχουν δύο όρια: φυσικά και εικονικά [22].

2.4 Επόπτης εικονικής μηχανής (Virtual Machine Monitor - Hypervisor)

Ο επόπτης εικονικής μηχανής (Virtual Machine Monitor - VMM) ή επόπτης (hypervisor) είναι υπεύθυνος για την απομόνωση της εικονικής μηχανής. Ως εκ τούτου, εάν ο επόπτης βρίσκεται σε κίνδυνο, οι εικονικές μηχανές του μπορεί επίσης να τεθούν σε κίνδυνο [35]. Το VMM είναι ένα λογισμικό χαμηλού επιπέδου που ελέγχει και παρακολουθεί τις εικονικές μηχανές του, όπως κάθε παραδοσιακό λογισμικό ελέγχει τα κενά ασφαλείας. Κρατώντας το VMM, όσο το δυνατόν απλό και μικρό, μειώνεται ο κίνδυνος να βρεθούν τρωτά σημεία στην ασφάλεια, δεδομένου ότι θα είναι πιο εύκολο να βρεθούν και να διορθωθούν τυχόν ευπάθειες [58].

Επιπλέον, η εικονοποίηση εισάγει τη δυνατότητα μεταφοράς εικονικών μηχανών μεταξύ των φυσικών servers για την ανοχή σφαλμάτων, την εξισορρόπηση φορτίου ή τη συντήρηση. Αυτό το χρήσιμο χαρακτηριστικό μπορεί επίσης να δημιουργήσει προβλήματα ασφαλείας. Ένας εισβολέας μπορεί να θέσει σε κίνδυνο την ενότητα της μεταφοράς στον VMM και να μεταφέρει ένα «θύμα» εικονική μηχανή σε έναν κακόβουλο διακομιστή. Επίσης, είναι σαφές ότι η μεταφορά εικονικής μηχανής (VM) εκθέτει το περιεχόμενο της εικονικής μηχανής στο δίκτυο, κάτι το οποίο μπορεί να θέσει σε κίνδυνο την ακεραιότητα των δεδομένων και την εμπιστευτικότητα. Μια κακόβουλη εικονική μηχανή μπορεί να μεταφερθεί σε άλλο υποδοχέα (με άλλο VMM) και να τον θέτει σε κίνδυνο [28].



Εικόνα 2.4. Η σχέση μεταξύ hyrervisor και virtual machine.

Πηγή: www.google.gr/εικόνες

Κεφάλαιο 3
Τύποι Επιθέσεων στο Υπολογιστικό Νέφος

3.1 Απειλή για την ασφάλεια, κίνδυνοι και αδυναμίες

Με την αυξανόμενη δημοτικότητα των εταιρειών υπολογιστικού νέφους και τη δημόσια συνδεσιμότητα του μέσω του διαδικτύου, το υπολογιστικό νέφος γίνεται το επόμενο σύνορο για ιούς, χάκερς και κυβερνοτρομοκράτες, ώστε να ξεκινήσουν τις επιθέσεις. Πολλές επιχειρήσεις βλέπουν σοβαρά το υπολογιστικό νέφος για να μειώσουν το κόστος και στο όχι πολύ μακρινό μέλλον, ο ρυθμός υιοθέτησης του υπολογιστικού νέφους θα εκτοξευθεί στα ύψη, όπως επίσης θα αυξηθεί συγχρόνως και η ευπάθεια σε ιούς, σε χάκερς και επιθέσεις στον κυβερνοχώρο. Αυτό θα γίνει διότι το οργανωμένο έγκλημα και οι τρομοκράτες, θα δουν το υπολογιστικό νέφος ως ένα νέο σύνορο για να προσπαθήσουν να κλέψουν προσωπικές πληροφορίες, να διακόψουν υπηρεσίες και να προκαλέσουν βλάβες στο δίκτυο υπολογιστικού νέφους των επιχειρήσεων. Ένα περιστατικό για τον κίνδυνο της ασφάλειας του υπολογιστικού νέφους συνέβη όταν η Google, η οποία είναι ένας σημαντικός πάροχος υπολογιστικού νέφους και λογισμικού ως υπηρεσία (SaaS), δέχτηκε επίθεση στα συστήματά της. Οι εγκληματολόγοι του κυβερνοχώρου, υποστήριξαν ότι οι επιθέσεις προήλθαν από την Κίνα [47]. Με το υπολογιστικό νέφος, η φυσική θέση των δεδομένων είναι διασκορπισμένη σε όλη την γεωγραφική περιοχή που θα μπορούσε να εκταθεί πάνω από ηπείρους, χώρες ή περιοχές. Μία από τις κορυφαίες ανησυχίες για την ασφάλεια των επιχειρήσεων

είναι η φυσική θέση των δεδομένων που αποθηκεύονται στο νέφος, ιδίως αν βρίσκονται σε άλλη χώρα, διότι οι νόμοι της χώρας υποδοχής και του εξοπλισμού ισχύουν για τα δεδομένα σχετικά με τις μηχανές [62] και αυτό θα μπορούσε να είναι ένα μεγάλο πρόβλημα, αν η χώρα υποδοχής δεν έχει επαρκείς νόμους για την προστασία των ευαίσθητων δεδομένων ή αν το έθνος υποδοχής γίνεται αφιλόξενο ή όταν η κυβέρνηση του έθνους υποδοχής αλλάζει και γίνεται μη φιλική.

Υπήρξαν περιπτώσεις όπου υπήρξε πλήρης συσκότιση ολόκληρων υπηρεσιών νέφους για ώρες ή ακόμη και ημέρες λόγω σφαλμάτων. Το Gmail της Google ήταν πεσμένο για δύο ώρες, τα GoToMeeting και GoToWebinar της Ctrix ήταν προσωρινά μη διαθέσιμα, οι υπηρεσίες αποθήκευσης του Amazon.com ήταν εκτός λειτουργίας για 8 βασανιστικές ώρες [29]. Ας φανταστεί κάποιος μια εταιρεία που εξαρτάται πλήρως από έναν πάροχο υπηρεσιών υπολογιστικού νέφους του οποίου το σύστημα είχε διακοπεί για ώρες ή ημέρες, η απώλεια των επιχειρήσεων θα μπορούσε να είναι καταστροφική.

3.1.1 Απειλές – Οι 7 θανάσιμες απειλές του υπολογιστικού νέφους

Το υπολογιστικό νέφος αντιμετωπίζει εξίσου, απειλές για την ασφάλεια που βρίσκονται σήμερα στις υπάρχουσες πλατφόρμες υπολογιστών, δικτύων, intranets, ίντερνετ σε επιχειρήσεις. Αυτές οι απειλές και οι αδυναμίες, έρχονται σε διάφορες μορφές. Η Συμμαχία Ασφάλειας Νέφους [11] έκανε μια έρευνα σχετικά με τις απειλές που αντιμετωπίζει το υπολογιστικό νέφος και προσδιόρισε τις επτά πιο σημαντικές απειλές:

- Κακοποίηση και φαύλη χρήση του νέφους.
- Ανασφαλείς διασυνδέσεις και διεπαφή προγραμματισμού εφαρμογών (API's).
- Κακόβουλοι εισβολείς (εκ των έσω).
- Εικονική τεχνολογία.
- Απώλεια δεδομένων ή διαρροή.
- Υποκλοπή - παραβίαση υπηρεσιών

- Άγνωστο προφίλ κινδύνου.

Κακοποίηση και φαύλη χρήση του νέφους

Οι πάροχοι νέφους διευκολύνουν τους χρήστες με διάφορους τύπους υπηρεσιών, συμπεριλαμβανομένων το απεριόριστο εύρος ζώνης και την χωρητικότητα αποθήκευσης. Ορισμένοι πάροχοι υπηρεσιών νέφους, προσφέρουν δωρεάν περιορισμένες περιόδους δοκιμής που δίνει την ευκαιρία στους χάκερς να έχουν πρόσβαση στο νέφος ανήθικα. Ο αντίκτυπός του περιλαμβάνει αποκωδικοποίηση και ράγισμα των κωδικών πρόσβασης, δρομολόγηση πιθανών σημείων επιθέσεων και εκτέλεση κακόβουλων εντολών. Οι spammers, οι κακόβουλοι συγγραφείς κώδικα και άλλοι εγκληματίες του κυβερνοχώρου, μπορούν να ασκούν τις δραστηριότητές τους με σχετική ατιμωρησία, καθώς οι πάροχοι υπηρεσιών νέφους γίνονται στόχος για τα αδύναμα συστήματα καταγραφής τους και τις περιορισμένες δυνατότητες ανίχνευσης της απάτης που διαθέτουν. Για παράδειγμα, μερικοί εγκληματίες του κυβερνοχώρου χρησιμοποιούν πλούσιες εφαρμογές περιεχομένου, όπως τα αρχεία flash, που τους επιτρέπουν να κρύψουν τον κακόβουλο κώδικά τους και να χρησιμοποιούν τα προγράμματα περιήγησης των χρηστών για να εγκαταστήσουν το κακόβουλο λογισμικό [13].

Ανασφαλείς διασυνδέσεις και διεπαφές προγραμματισμού εφαρμογών (Application programming interface - API's).

Οι χρήστες του νέφους, χρησιμοποιούν διεπαφές λογισμικού και API's για την πρόσβαση και τη διαχείριση των υπηρεσιών νέφους. Αυτά τα API's πρέπει να ασφαλίζονται, διότι αποτελούν αναπόσπαστο κομμάτι κατά τη διάρκεια της παροχής, της διαχείρισης, της ενορχήστρωσης και της παρακολούθησης των διεργασιών που τρέχουν σε περιβάλλον νέφους. Η ασφάλεια και η διαθεσιμότητα των υπηρεσιών νέφους, εξαρτάται από την ασφάλεια αυτών των API's έτσι θα πρέπει να περιλαμβάνουν χαρακτηριστικά της ταυτότητας, του ελέγχου πρόσβασης, κρυπτογράφησης και παρακολούθησης της δραστηριότητας. Τα API's πρέπει να είναι σχεδιασμένα για να προστατεύουν τόσο τυχαίες όσο και

κακόβουλες προσπάθειες για την αποφυγή των απειλών. Αν ο πάροχος υπηρεσιών νέφους βασίζεται σε ένα σύνολο αδύναμων API's, η ποικιλία των θεμάτων ασφαλείας θα πρέπει να αυξηθεί και να σχετίζεται με την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα, όπως κακόβουλη ή αγνώστων στοιχείων πρόσβαση, εξαρτήσεις API's, περιορισμένη παρακολούθηση / καταγραφή των δυνατοτήτων, άκαμπτη πρόσβαση, ανώνυμη πρόσβαση, επαναχρησιμοποιήσιμοι κωδικοί πρόσβασης και ακατάλληλες άδειες [14].

Κακόβουλοι εισβολείς (εκ των έσω)

Οι επιθέσεις σε εμπιστευτικές πληροφορίες μπορεί να πραγματοποιηθούν από κακόβουλους εργαζόμενους απ' τη μεριά του παρόχου ή του χρήστη. Οι κακόβουλοι εισβολείς μπορούν να κλέψουν τα εμπιστευτικά δεδομένα των χρηστών του νέφους. Αυτή η απειλή μπορεί να σπάσει την εμπιστοσύνη των χρηστών του νέφους προς τον πάροχο. Ένας κακόβουλος εισβολέας μπορεί εύκολα να αποκτήσει κωδικούς πρόσβασης, κλειδιά κρυπτογράφησης και αρχεία. Οι επιθέσεις αυτές μπορεί να περιλαμβάνουν διάφορα είδη απάτης, ζημιές ή κλοπή πληροφοριών και κατάχρηση πόρων IT (IT – Information Technology - τεχνολογία πληροφοριών). Η απειλή των κακόβουλων επιθέσεων έχει αυξηθεί λόγω της έλλειψης διαφάνειας στις διαδικασίες των παρόχων του νέφους [16]. Αυτό σημαίνει ότι ένας πάροχος δεν μπορεί να αποκαλύψει το πώς οι εργαζόμενοι έχουν πρόσβαση και πώς η πρόσβαση αυτή παρακολουθείται ή πώς οι εκθέσεις καθώς και η συμμόρφωση της πολιτικής αναλύονται. Επιπλέον, οι χρήστες έχουν ελάχιστη πληροφόρηση σχετικά με τις πρακτικές ενοικίασης του φορέα τους, κάτι το οποίο θα μπορούσε να ανοίξει την πόρτα για έναν αντίπαλο, για χάκερς ή άλλους εισβολείς στο νέφος, οι οποίοι θα μπορούσαν να κλέψουν εμπιστευτικές πληροφορίες ή να αναλάβουν τον έλεγχο πάνω στο νέφος. Το επίπεδο πρόσβασης που χορηγείται θα μπορούσε να επιτρέψει σε χάκερς να συλλέξουν προσωπικά δεδομένα ή να αποκτήσουν τον πλήρη έλεγχο των υπηρεσιών νέφους με μικρό ή μηδαμινό κίνδυνο εντοπισμού. Οι κακόβουλες επιθέσεις εμπιστευτικών πληροφοριών μπορεί να βλάψουν την οικονομική αξία, καθώς και τη φήμη ενός οργανισμού.

Εικονική τεχνολογία

Λόγω της εικονοποίησης του νέφους, οι πάροχοι εγκαθιστούν τις εφαρμογές του χρήστη σε εικονικές μηχανές (VM's – Virtual Machines) μέσα σε μια κοινή υποδομή. Οι εικονικές μηχανές βασίζουν την εικονοποίηση σύμφωνα με το φυσικό υλικό του παρόχου του νέφους. Προκειμένου να διατηρηθεί η ασφάλεια των χρηστών, οι πάροχοι απομονώνουν τις εικονικές μηχανές τη μια από την άλλη, έτσι ώστε αν κάποια από αυτές είναι κακόβουλη, αυτό δεν θα επηρεάσει την άλλη εικονική μηχανή κάτω από τον ίδιο πάροχο. Η εικονική μηχανή διαχειρίζεται από έναν επόπτη εικονικής μηχανής, προκειμένου να παρέχει εικονική μνήμη όπως επίσης και CPU (Central Processing Unit) πολιτικές προγραμματισμού, στις εικονικές μηχανές. Δεδομένου ότι ο επόπτης είναι η κύρια πηγή της διαχείρισης μιας εικονικής πλατφόρμας νέφους, οι χάκερς στοχεύουν να έχουν πρόσβαση στην εικονική μηχανή και το φυσικό υλικό, επειδή ο επόπτης κατοικεί μεταξύ εικονικής μηχανής και υλικού [71], έτσι ώστε η επίθεση στον επόπτη να μπορέσει να βλάψει την εικονική μηχανή και το υλικό. Ισχυρή μόνωση θα πρέπει να χρησιμοποιηθεί για να διασφαλιστεί ότι η εικονική μηχανή δεν θα είναι σε θέση να επηρεάσει ή να αποκτήσει πρόσβαση στις λειτουργίες άλλων χρηστών που τρέχουν κάτω από τον ίδιο πάροχο υπηρεσιών νέφους. Αρκετοί προμηθευτές όπως οι Xen και KVM παρέχουν ισχυρούς μηχανισμούς ασφάλειας για την προστασία των εποπτών του νέφους, ωστόσο εξακολουθεί να αναγνωρίζεται ότι μερικές φορές η ασφάλεια των εικονικών μηχανών είναι σε κίνδυνο.

Απώλεια δεδομένων ή διαρροή

Η απώλεια δεδομένων μπορεί να προκύψει λόγω λειτουργικών βλαβών, αναξιόπιστης αποθήκευσης δεδομένων και ασυνεπειών στη χρήση των κλειδιών κρυπτογράφησης. Επιχειρησιακές αποτυχίες αναφέρονται σε διαγραφή ή τροποποίηση των αρχείων χωρίς ένα αντίγραφο ασφαλείας του αρχικού περιεχομένου που μπορεί να γίνει εκούσια ή ακούσια. Αναξιόπιστη αποθήκευση των δεδομένων αναφέρεται στην αποθήκευση δεδομένων σε αναξιόπιστα μέσα που θα είναι ανεπανόρθωτη, αν τα δεδομένα χαθούν [60]. Η ασυνεπής χρήση των

κλειδιών κρυπτογράφησης θα οδηγήσει σε απώλεια και μη εξουσιοδοτημένη άδεια χρήσης των δεδομένων από παράνομους χρήστες που θα οδηγήσει στην καταστροφή των ευαίσθητων και εμπιστευτικών πληροφοριών. Παράδειγμα απώλειας δεδομένων είναι η επίθεση χάκερς στο Twitter. Οι online λογαριασμοί του Twitter προσπελάστηκαν από χάκερς και πολλά ευαίσθητα εταιρικά έγγραφα εκλάπησαν. Τα έγγραφα αυτά «στεγάζονται» σε online υπηρεσίες της Google το Google Docs. Η Google δεν ήταν αυτή που έπρεπε να κατηγορηθεί για την διάρρηξη της ασφάλειας, καθώς η ασφάλεια των εγγράφων από το twitter δεν ήταν αρκετά αποτελεσματική. Αντ 'αυτού, το σύνολο των δεδομένων της εταιρείας ήταν μόνο ένας κωδικός πρόσβασης μακριά από την ανακάλυψη [56]. Είναι σαφές από αυτό το παράδειγμα ότι η απώλεια δεδομένων ή η διαρροή μπορεί να προκαλέσει ζημιά στην φήμη μιας εταιρείας και να προκαλέσει μια απώλεια που μπορεί να επηρεάσει σημαντικά υπαλλήλους, συνεταίρους και το ηθικό των χρηστών, καθώς και την εμπιστοσύνη. Η απώλεια του πυρήνα της πνευματικής ιδιοκτησίας μπορεί να έχει ανταγωνιστικές και οικονομικές επιπτώσεις εκτός από τις παραβιάσεις της συμμόρφωσης και τις νομικές συνέπειες.

Υποκλοπή - παραβίαση υπηρεσιών

Η πειρατεία λογαριασμών και υπηρεσιών αναφέρεται σε μη εξουσιοδοτημένη πρόσβαση που έχει αποκτηθεί από επιτιθέμενους ώστε να ελέγξουν τους λογαριασμούς των χρηστών, να κάνουν απάτες και να εκμεταλλευτούν τα τρωτά σημεία του λογισμικού. Για παράδειγμα, αν ένας εισβολέας αποκτήσει πρόσβαση σε διαπιστευτήρια χρηστών, μπορεί να κατασκοπεύσει τις δραστηριότητες / συναλλαγές τους, να χειριστεί τα δεδομένα τους, να επιστρέψει παραποιημένες πληροφορίες και να τους αποπροσανατολίσει σε παράνομες ιστοσελίδες[39]. Λογαριασμοί χρηστών ή περιπτώσεις υπηρεσιών, μπορεί να γίνουν μια νέα βάση για τους εισβολείς που μπορούν να αξιοποιήσουν τη φήμη των παρόχων υπηρεσιών νέφους, με τη δρομολόγηση επόμενων επιθέσεων. Με κλεμμένα διαπιστευτήρια, οι επιτιθέμενοι μπορούν συχνά να έχουν πρόσβαση σε κρίσιμες περιοχές ανεπτυγμένων υπηρεσιών του υπολογιστικού νέφους, επιτρέποντάς

τους έτσι να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των εν λόγω υπηρεσιών. Έλεγχοι ταυτότητας και εξουσιοδότηση με τη χρήση ρόλων και προστασίας των κωδικών πρόσβασης, είναι ένας συνηθισμένος τρόπος για να διατηρηθεί ο έλεγχος της πρόσβασης, όταν χρησιμοποιούνται web-browsers για την πρόσβαση σε συστήματα υπολογιστικού νέφους. Ωστόσο, αυτή η μέθοδος δεν επαρκεί για την εξασφάλιση ευαίσθητων και κρίσιμων δεδομένων.

Άγνωστο προφίλ κινδύνου

Είναι σημαντικό για τους χρήστες να γνωρίζουν τις εκδόσεις λογισμικού, τις πρακτικές ασφαλείας, τις ενημερώσεις του κώδικα και απόπειρες εισβολής. Ενώ η υιοθέτηση υπηρεσιών υπολογιστικού νέφους, τα χαρακτηριστικά και η λειτουργικότητα μπορεί να διαφημιστούν καλά, τι γίνεται με τις λεπτομέρειες ή την τήρηση των εσωτερικών διαδικασιών ασφαλείας, τη διαμόρφωση, τον έλεγχο. Στους χρήστες πρέπει να διευκρινίζεται πώς και πού τα στοιχεία τους και άλλες πληροφορίες αποθηκεύονται. Ωστόσο, δεν υπάρχει σαφής απάντηση, κάτι που αφήνει τους χρήστες με ένα άγνωστο προφίλ κινδύνου που μπορεί να περιλαμβάνει σοβαρές απειλές [14].

3.1.2 Κίνδυνοι

Κίνδυνος σύμφωνα με το Ινστιτούτο SAN[5], «είναι η πιθανή βλάβη που μπορεί να προκύψει από κάποια τρέχουσα διαδικασία ή από κάποιο μελλοντικό γεγονός.» Στην ασφάλεια της πληροφορικής, η διαχείριση του κινδύνου είναι η διαδικασία

[5] Το Ινστιτούτο SAN ιδρύθηκε το 1989 ως ένας οργανισμός ερευνών και εκπαίδευσης. Τα προγράμματά του αυτή τη στιγμή, φθάνουν σε περισσότερους από 165.000 επαγγελματίες ασφαλείας σε όλο το κόσμο. Μια σειρά ατόμων, από ελεγκτές και διαχειριστές δικτύου μέχρι προϊσταμένους ασφάλειας πληροφοριών, μοιράζονται τις γνώσεις που λαμβάνουν και από κοινού βρίσκουν λύσεις στις προκλήσεις που αντιμετωπίζουν. Στην καρδιά του SAN, βρίσκονται πολλοί επαγγελματίες ασφαλείας σε διάφορους παγκόσμιους οργανισμούς, από πανεπιστήμια μέχρι επιχειρήσεις, δουλεύοντας μαζί και βοηθώντας ολόκληρη την κοινότητα ασφάλειας πληροφοριών. Το SAN είναι η πιο αξιόπιστη και με διαφορά η μεγαλύτερη πηγή για την εκπαίδευση σε θέματα ασφάλειας πληροφοριών και την πιστοποίηση της ασφάλειας, στον κόσμο. Επίσης, αναπτύσσει, διατηρεί και καθιστά διαθέσιμη χωρίς κόστος, τη μεγαλύτερη συλλογή ερευνητικών εγγράφων σχετικά με τις διάφορες πτυχές της ασφάλειας των πληροφοριών και λειτουργεί το σύστημα έγκαιρης προειδοποίησης του Διαδικτύου.

με την οποία μπορεί να αντιληφθεί κάποιος και να απαντήσει σε παράγοντες που μπορεί να οδηγήσουν σε αποτυχία την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός πληροφοριακού συστήματος (Ινστιτούτο SAN). Ο κίνδυνος της ασφάλειας της πληροφορίας είναι η βλάβη σε μία διαδικασία ή οι σχετικές πληροφορίες που προκύπτουν από κάποιο σκόπιμο ή τυχαίο γεγονός που επηρεάζει αρνητικά τη διαδικασία ή τις σχετικές πληροφορίες (Ινστιτούτο SAN).

Συνεχίζοντας με το νέφος, εμφανίζεται στην επιχείρηση με μια σειρά από κινδύνους και αυτοί περιλαμβάνουν την εξασφάλιση κρίσιμων πληροφοριών, όπως την προστασία της πνευματικής ιδιοκτησίας, εμπορικά μυστικά, αλλά και προσωπικές πληροφορίες που θα μπορούσαν να πέσουν σε λάθος χέρια. Κάνοντας τις ευαίσθητες πληροφορίες διαθέσιμες στο διαδίκτυο, απαιτούνται σημαντικές επενδύσεις σε ελέγχους ασφαλείας, αλλά και παρακολούθηση της πρόσβασης στο περιεχόμενο αυτών. Στο περιβάλλον του νέφους, η επιχείρηση μπορεί να έχει μικρή ή καμία ορατότητα προς την αποθήκευση και τη δημιουργία αντιγράφων ασφαλείας των διαδικασιών και λίγο ή καθόλου φυσική πρόσβαση σε συσκευές αποθήκευσης από τον πάροχο του υπολογιστικού νέφους. Και, επειδή τα δεδομένα από πολλαπλούς πελάτες μπορούν να αποθηκεύονται σε ένα ενιαίο μέρος, ο έλεγχος των μέσων αποθήκευσης και η σωστή κατανόηση της πρόσβασης σε αρχεία, αλλά και η διαγραφή, θα είναι σημαντικές προκλήσεις [14].

3.1.3 Ευπάθεια

Σύμφωνα με τον Pfleenger (2006) , ευπάθεια, «είναι μια αδυναμία στο σύστημα ασφαλείας» η οποία θα μπορούσε εφόσον αξιοποιηθεί, να προκαλέσει βλάβη. Το υπολογιστικό νέφος σε μια επιχείρηση, είναι τόσο ευάλωτο, όσο ευάλωτη είναι και οποιαδήποτε άλλη τεχνολογία χρησιμοποιεί το διαδίκτυο για συνδεσιμότητα. Η ευπάθεια περιλαμβάνει, υποκλοπές, hacking (χάκερς), «ρωγμές» στο σύστημα, κακόβουλες επιθέσεις και διακοπές. Η μετακίνηση των δεδομένων σε μια υπηρεσία νέφους είναι ακριβώς όπως το «να βάζετε όλα τα αυγά σας σε ένα καλάθι [54] και στις αρχές του 2009 η σελίδα κοινωνικής δικτύωσης «Ma.gnolia» γνώρισε τη συντριβή του διακομιστή της, ο οποίος έχασε τεράστιο όγκο δεδομένων από τους χρήστες της και έτσι η υπηρεσία έκλεισε οριστικά.

Η έρευνα έχει δείξει ότι είναι δυνατό για τους επιτιθέμενους να χαρτογραφήσουν με ακρίβεια την φυσική τοποθεσία των δεδομένων εντός του νέφους και στη συνέχεια, να χρησιμοποιούν διάφορα τεχνάσματα για τη συγκέντρωση πληροφοριών [65]. Άλλη μια ευπάθεια σε μια επίθεση, είναι η άρνηση υπηρεσιών σε επίθεση και έχει βρεθεί ότι εάν ο επιτιθέμενος ανήκει στον ίδιο διακομιστή νέφους με το θύμα, μια συμβατική άρνηση υπηρεσιών σε επίθεση μπορεί να ξεκινήσει με τη χρήση όλων των πόρων του με τη μία.

Ερευνητές στο Πανεπιστήμιο της Καλιφόρνια στο Σαν Ντιέγκο και στο MIT λένε ότι μπορούν να αγοράσουν υπηρεσίες νέφους από το Amazon και να τοποθετήσουν μια εικονική μηχανή στην ίδια φυσική μηχανή ως μια εφαρμογή-στόχο, και μπορούν να χρησιμοποιήσουν την πρόσβαση της εικονικής τους μηχανής στους κοινόχρηστους πόρους του φυσικού μηχανήματος για να κλέψει δεδομένα, όπως κωδικούς πρόσβασης. Αυτή η τεχνική, είπαν οι ερευνητές, είναι σε πειραματικό στάδιο και δεν λειτουργεί όλη την ώρα, αλλά υποδεικνύει ότι οι παροχές υπηρεσιών νέφους είναι επιρρεπείς σε νέους τύπους επιθέσεων που δεν έχουν εμφανιστεί ξανά πριν. Και ενώ η επίθεσή τους διεξαγόταν μέσα στο EC2 νέφος της Amazon, λένε ότι η μέθοδός τους θα μπορούσε να λειτουργήσει εξίσου καλά και με άλλους παρόχους νέφους [27].

Οι ερευνητές οδηγήθηκαν στο να πουν ότι ένας τρόπος γύρω από την αδυναμία να βρέθηκε στο EC2 της Amazon είναι, το να επιμένουν οι πελάτες, οι μηχανές νέφους τους να είναι τοποθετημένες σε φυσικές μηχανές που μόνο αυτοί μπορούν να έχουν πρόσβαση ή επίσης και έμπιστα τρίτα άτομα. Αυτή η λύση πιθανώς να είναι υπερτιμημένη, επειδή μέρος της οικονομίας των υπηρεσιών νέφους είναι η μεγιστοποίηση της χρήσης των φυσικών διακομιστών φορτώνοντάς τους αποτελεσματικά με μηχανήματα νέφους και εντοπίζοντας το κέντρο δεδομένων του νέφους, όπου η τιμή χρησιμότητας είναι η φθηνότερη.

Το έργο των ερευνητών επισημαίνει ότι τα νέφη και τα εικονικά περιβάλλοντα που απασχολούν είναι σχετικά νέα, ως εκ τούτου εξακολουθούν να τραβούν την προσοχή των επιτιθέμενων ώστε να βρουν και να αξιοποιήσουν ανεξερεύνητα τρωτά σημεία [27]. Αυτό δε σημαίνει ότι οι υπηρεσίες νέφους δεν παρέχουν ασφάλεια και δε θα πρέπει να χρησιμοποιούνται.

Στην υπεράσπιση της ασφάλειας του υπολογιστικού νέφους, ο Edwards (2010), δήλωσε ότι με τη χρήση του ως «τεχνολογία λεπτού πελάτη, οι επιχειρήσεις μπορούν να περιορίσουν την έκθεση των απειλών που τίθενται από τα στριμωγμένα δεδομένα των φορητών υπολογιστών και τη δημιουργία αντιγράφων ασφαλείας. Θα υπάρχει πιο αποτελεσματικό λογισμικό ασφαλείας, επειδή με τους προμηθευτές λογισμικού υπολογιστικού νέφους θα καθοριστούν αναποτελεσματικές προσεγγίσεις ασφάλειας που καίνε πόρους [18]. Το νέφος θα είναι ένας καλύτερος ανιχνευτής ιών και στο Πανεπιστήμιο του Michigan ερευνητές έχουν ανακαλύψει ότι αν τα εργαλεία λογισμικού ενός anti-virus μετακινηθούν από έναν ηλεκτρονικό υπολογιστή στο νέφος, αυτό θα μπορούσε να ανιχνεύσει 35 τοις εκατό πιο πρόσφατους ιούς από ένα πρόγραμμα anti-virus για προσωπικό υπολογιστή. Το σημείο μηδέν είναι, ότι οι επιχειρήσεις θα πρέπει να αντιμετωπίζουν το νέφος με ένα ορισμένο ποσοστό καχυποψίας, θα πρέπει να αξιολογούν τον κίνδυνο που η υπηρεσία του νέφους αντιπροσωπεύει και να δεσμεύουν εκεί δεδομένα για τις εν λόγω υπηρεσίες που μπορούν να ανεχθούν αυτόν τον κίνδυνο» [27].

3.2 Βήματα για την ασφάλεια του νέφους

Ο Edwards (2009) ανέφερε ότι, με τον κίνδυνο για την ασφάλεια και την ευπάθεια στο υπολογιστικό νέφος, επιχειρήσεις που θέλουν να προχωρήσουν με το υπολογιστικό νέφος, θα πρέπει να χρησιμοποιούν τα ακόλουθα βήματα για να ελέγχουν και να κατανοούν την παρεχόμενη ασφάλεια από τον πάροχο του νέφους.

- Κατανοήστε το νέφος συνειδητοποιώντας πόσο η μοναδικά χαλαρή δομή του νέφους επηρεάζει την ασφάλεια των δεδομένων που αποστέλλονται σε αυτό. Αυτό μπορεί να γίνει με μια σε βάθος κατανόηση του πώς το υπολογιστικό νέφος μεταφέρει και λαμβάνει δεδομένα.
- Το ζήτημα διαφάνειας, με τη διασφάλιση ότι ο πάροχος του νέφους μπορεί να παρέχει λεπτομερείς πληροφορίες για την αρχιτεκτονική ασφαλείας του και είναι πρόθυμος να δεχθεί τακτικό έλεγχο ασφαλείας.

Ο τακτικός έλεγχος της ασφάλειας θα πρέπει να είναι από έναν ανεξάρτητο φορέα ή ομοσπονδιακή υπηρεσία.

- Η ενίσχυση της εσωτερικής ασφάλειας, με τη διασφάλιση ότι οι εσωτερικές τεχνολογίες ασφάλειας του παρόχου του νέφους και πρακτικές, συμπεριλαμβανομένων των firewalls και ελέγχων της πρόσβασης των χρηστών, είναι πολύ ισχυρές και μπορούν να τα πάνε πολύ καλά με τα μέτρα ασφαλείας του νέφους.
- Εξετάστε τις νομικές συνέπειες, γνωρίζοντας πώς οι νόμοι και οι κανονισμοί θα επηρεάσουν το τι στέλνετε στο νέφος.
- Δώστε προσοχή, παρακολουθώντας συνεχώς όλες τις εξελίξεις ή τις αλλαγές στις τεχνολογίες νέφους και πρακτικές που μπορεί να επηρεάσουν την ασφάλεια των δεδομένων.

3.2.1 Θέματα προς αποσαφήνιση πριν την υιοθέτηση του υπολογιστικού νέφους

Η Gartner Inc, η κορυφαία στον κόσμο συμβουλευτική εταιρεία στις ICT, έχει εντοπίσει επτά ανησυχίες για την ασφάλεια που μια επιχείρηση που χρησιμοποιεί το υπολογιστικό νέφος θα πρέπει να αντιμετωπίσει με τους παρόχους υπολογιστικού νέφους [17] πριν το υιοθετήσει:

- **Πρόσβαση χρήστη**. Ζητήστε από τους παρόχους για συγκεκριμένες πληροφορίες σχετικά με την πρόσληψη και την εποπτεία των προνομιούχων διαχειριστών και των ελέγχων για την πρόσβασή τους σε πληροφορίες. Οι μεγάλες εταιρείες θα πρέπει να απαιτήσουν και να επιβάλουν τα δικά τους κριτήρια για προσλήψεις προσωπικού που θα λειτουργούν στα περιβάλλοντα υπολογιστικού νέφους τους.
- **Κανονιστική Συμμόρφωση.** Βεβαιωθείτε ότι ο πάροχός σας είναι πρόθυμος να υποβληθεί σε εξωτερικούς ελέγχους και πιστοποιήσεις ασφαλείας.
- **Τοποθεσία δεδομένων.** Οι επιχειρήσεις θα πρέπει να απαιτήσουν ότι ο πάροχος του υπολογιστικού νέφους και τα δεδομένα διεργασίας με

συγκεκριμένες δικαιοδοσίες θα πρέπει να υπακούουν στους κανόνες προστασίας της ιδιωτικής ζωής αυτών των δικαιοδοσιών.

- **Δεδομένα Διαχωρισμού.** Μάθετε τι γίνεται με τον διαχωρισμό των δεδομένων και ζητήστε απόδειξη ότι τα συστήματα κρυπτογράφησης αναπτύσσονται και είναι αποτελεσματικά.
- **Επαλήθευση ανάκαμψης καταστροφής.** Γνωρίστε τι θα συμβεί εάν η καταστροφή χτυπήσει, ζητώντας να δείτε από τον φορέας σας εάν θα είναι σε θέση να αποκαταστήσει πλήρως τα δεδομένα και τις υπηρεσίες, αλλά και πόσος καιρός θα χρειαστεί.
- **Αποκατάσταση μετά την καταστροφή.** Ζητήστε από τον πάροχο μια συμβατική δέσμευση για την υποστήριξη συγκεκριμένων τύπων ερευνών, όπως είναι η έρευνα που εμπλέκεται στη φάση της ανακάλυψης μιας δίκης και βεβαιωθείτε ότι ο πάροχος έχει υποστηρίξει με επιτυχία τέτοιες δραστηριότητες στο παρελθόν. Χωρίς απόδειξη, μην υποθέσετε ότι μπορεί να το κάνει.
- **Μακροπρόθεσμη βιωσιμότητα.** Ρωτήστε υποψήφιους παρόχους πώς θα πάρετε τα δεδομένα σας πίσω, αν αυτοί αποτύχουν και μάθετε εάν τα δεδομένα θα είναι σε τέτοια μορφή που θα μπορούσαν εύκολα να εισαχθούν σε μία αίτηση αντικατάστασης.

3.2.2 Ανάγκη για μια κυβερνητική στρατηγική και καλή τεχνολογία διακυβέρνησης

Προχωρώντας στο υπολογιστικό νέφος απαιτείται μια καλή στρατηγική διακυβέρνησης και μια καλή τεχνολογία διακυβέρνησης [41]. Το ενδιαφέρον για τη διακυβέρνηση έχει αναζωογονηθεί διότι η εμπιστοσύνη επεκτείνεται σε έναν πάροχο νέφους σε όλη την παραδοχή και σε εταιρικά όρια. Μια λειτουργία διακυβέρνησης υπολογιστικού νέφους απαιτεί την ενεργό συμμετοχή της διαχείρισης, το κατάλληλο φόρουμ για σχετικές αποφάσεις με την τεχνολογία πληροφοριών και την αποτελεσματική επικοινωνία μεταξύ του οργανισμού πληροφορικής και την ομάδα διαχείρισης της εταιρείας [45]. Maches (2010) πρότεινε τη διαχείριση του κινδύνου στο νέφος να συμπεριληφθεί στη λειτουργία

της διακυβέρνησης του υπολογιστικού νέφους, που απαιτεί επίγνωση των κινδύνων από υψηλόβαθμα εταιρικά στελέχη, μια σαφή κατανόηση της όρεξης της επιχείρησης για κίνδυνο, την κατανόηση των απαιτήσεων συμμόρφωσης, τη διαφάνεια σχετικά με τους σοβαρούς κινδύνους για την επιχείρηση και την ενσωμάτωση των αρμοδιοτήτων διαχείρισης του κινδύνου στον οργανισμό τεχνολογίας πληροφοριών.

Κεφάλαιο 4
Θέματα Εμπιστοσύνης στο Υπολογιστικό Νέφος

4.1 Η εμπιστοσύνη στο υπολογιστικό νέφος

Σε παραδοσιακά μοντέλα ασφάλειας, δημιουργείται μια περίμετρος ασφαλείας για να υπάρξει ένα όριο εμπιστοσύνης εντός του οποίου, θα υπάρχει αυτο-έλεγχος των υπολογιστικών πόρων και όπου ευαίσθητες πληροφορίες θα αποθηκεύονται και θα επεξεργάζονται. Για παράδειγμα, το όριο αυτό σηματοδοτείται συχνά από το εταιρικό τείχος προστασίας. Το δίκτυο παρέχει διέλευση προς άλλους αξιόπιστους κεντρικούς υπολογιστές, που λειτουργούν με παρόμοιο τρόπο. Αυτό το μοντέλο πραγματοποιήθηκε για το διαδίκτυο, αλλά δεν χρησιμοποιείται για το δημόσιο και το υβριδικό νέφος. Η περίμετρος ασφαλείας γίνεται θολή, με την έννοια ότι οι εμπιστευτικές πληροφορίες μπορεί να υποβάλλονται σε επεξεργασία εκτός των γνωστών περιοχών, καθώς αυτά τα υπολογιστικά περιβάλλοντα έχουν συχνά ασαφή όρια ως προς το ποια δεδομένα αποθηκεύονται ή/και υποβάλλονται σε επεξεργασία. Από την άλλη πλευρά, προκειμένου να λάβουν την υπηρεσία, οι καταναλωτές πρέπει να επεκτείνουν την εμπιστοσύνη τους προς τον πάροχο των υπηρεσιών νέφους και έτσι αυτό μπορεί να παρέχει ένα σημείο τριβής, όπως θα εξετασθεί περαιτέρω παρακάτω.

Στην αξιολόγηση της παροχής του υπολογιστικού νέφους, οι μηχανισμοί για την παροχή δυναμικής, τεχνολογικής βάσης εμπιστοσύνης, πρέπει να χρησιμοποιούνται σε συνδυασμό με κοινωνικούς και τεχνολογικούς μηχανισμούς για την παροχή διαρκούς εμπιστοσύνης: εάν οι διαδικασίες λογισμικού παρέχουν

πληροφορίες σχετικά με τον τρόπο με τον οποίο αποθηκεύονται οι πληροφορίες, αποκτούν πρόσβαση και διαμοιράζονται μέσα στο νέφος, όπου οι πληροφορίες μπορεί να είναι εμπιστευτικές μόνο αν οντότητες που εμπιστεύονται εγγυηθούν για τη μέθοδο της παροχής των πληροφοριών και την αξιολόγηση των πληροφοριών. Ανάλογα με το πλαίσιο, οι φορείς αυτοί θα μπορούσαν να είναι ομάδες καταναλωτών, ελεγκτές, ειδικοί ασφαλείας, ρυθμιστικές αρχές, εταιρείες με αποδεδειγμένη φήμη, κ.λπ. Επιπλέον, οι σχέσεις εμπιστοσύνης μπορεί να είναι κατά πολύ στο επίκεντρο ορισμένων λύσεων ασφαλείας και προστασίας προσωπικών δεδομένων: για παράδειγμα, για εγγυήσεις κλειδιών και άλλες μορφές διανομής κλειδιού και διαμοίρασης μυστικού, ελέγχου, ελέγχου συμμόρφωσης και ψευδωνύμου. Υπάρχει επίσης μια ισχυρή σχέση με την αναπτυξιακή πολιτική: εάν οι προσωπικές ή επιχειρηματικές κρίσιμες πληροφορίες πρέπει να αποθηκεύονται στο νέφος, η εμπιστοσύνη αποκτά νέα σημασία και το Κέντρο για την Πολιτική Ασφαλείας (CSP's – Center for Security Policy) πρέπει να αγκαλιάσει μια τέτοια προσέγγιση [34].

4.2 Η έλλειψη εμπιστοσύνης των καταναλωτών

Από τους ευρωπαίους πολίτες που συμμετείχαν στην έρευνα τον Ιούνιο του 2011, για τη στάση τους σχετικά με την προστασία των δεδομένων [19], διαπιστώθηκε ότι οι αρχές και οι φορείς - συμπεριλαμβανομένης της Ευρωπαϊκής Επιτροπής και του Ευρωπαϊκού Κοινοβουλίου (το 55% των ερωτηθέντων) - είναι πιο αξιόπιστοι από εμπορικές επιχειρήσεις. Στην πραγματικότητα, λιγότεροι από το 1/3 εμπιστεύονται τις εταιρείες τηλεφωνίας, τις εταιρείες κινητής τηλεφωνίας και τους παρόχους υπηρεσιών διαδικτύου (32%) και μόλις πάνω από το 1/5 εμπιστεύονται τις εταιρείες διαδικτύου, όπως μηχανές αναζήτησης, ιστοσελίδες κοινωνικής δικτύωσης και υπηρεσίες ηλεκτρονικού ταχυδρομείου (22%). Επιπλέον, το 70% των Ευρωπαίων, σύμφωνα με τη μελέτη αυτή, ανησυχούν ότι τα προσωπικά τους δεδομένα που κρατούνται από τις επιχειρήσεις, μπορεί να χρησιμοποιηθούν για άλλο σκοπό από αυτόν για τον οποίο συλλέχθηκαν. Σε μια πρόσφατη έρευνα (Cloud Industry Forum), τα αποτελέσματα του «πώς μπορώ να εμπιστευτώ έναν online πάροχο;» τα αποτελέσματα ήταν: η φήμη (29%), η

συστάσεις από αξιόπιστες πηγές (27%), η εμπειρία σε δίκη (20%), οι συμβάσεις (συμβόλαια κτλ.) (20%), άλλα (4%) [10].

Οργανισμοί χειρισμού προσωπικών πληροφοριών έχουν νομική και ηθική υποχρέωση για τη διασφάλιση της ιδιωτικής ζωής και ως εκ τούτου αποδεικνύουν έτσι την αξιόπιστη φύση της υπηρεσίας τους. Σημαντικές ερωτήσεις για τη διεύθυνση περιλαμβάνουν εάν τα δεδομένα είναι ασφαλή σε όλο το νέφος, εάν διαχειρίζονται με βάση τις προσδοκίες των χρηστών, εάν η διαχείριση δεδομένων είναι συμβατή με τους νόμους και τους κανονισμούς, τα δεδομένα είναι υπό έλεγχο σε όλο το κύκλο ζωής τους, εάν η κατάλληλη χρήση και οι υποχρεώσεις διασφαλίζονται καθ' όλη την αλυσίδα επεξεργασίας και αν υπάρχουν πρότυπα ή τις γενικές πρακτικές για τη λειτουργία του νέφους. Υπάρχει έλλειψη εμπιστοσύνης για το νέφος και οι απαντήσεις σε αυτά τα ερωτήματα προς το παρόν, όπως φαίνεται από τα αποτελέσματα μιας σειράς από πρόσφατες έρευνες, εξετάζονται παρακάτω.

Οι επιχειρηματικοί χρήστες αναγνωρίζουν τα πλεονεκτήματα του νέφους, στην επιτάχυνση της καινοτομίας, την επιτάχυνση των επιχειρηματικών διαδικασιών. Αντίστοιχα, οι επιχειρήσεις έχουν αρχίσει ήδη να κινούνται προς το νέφος: μια μελέτη της IDC (International Data Corporation – Διεθνούς Εταιρείας Δεδομένων) διαπίστωσε ότι το 70% των επιχειρήσεων, εξετάζουν ή ήδη χρησιμοποιούν ιδιωτικά νέφη [32]. Ωστόσο, CIO's (Chief Information Officers – Προϊστάμενοι Πληροφοριακών Συστημάτων) είναι πιο επιφυλακτικοί. Μια πρόσφατη μελέτη από τη Forrester διαπίστωσε ότι μια επιχείρηση, υιοθετεί το νέφος 2,5 φορές πιο γρήγορα από ό,τι επιχειρήσεις τεχνολογίας πληροφοριών. Στελέχη επιχειρήσεων τεχνολογίας πληροφοριών, αναφέρουν βάσιμες ανησυχίες σχετικά με τις προκλήσεις της διατήρησης της ασφάλειας, τα επίπεδα υπηρεσιών, και την απρόσκοπτη διακυβέρνηση σε ολόκληρη την αξιακή αλυσίδα. Θέλουν, επίσης, να είναι βέβαιοι ότι οι αποφάσεις που παίρνουν σήμερα για τους προμηθευτές τεχνολογίας νέφους, δεν θα τους εμποδίσει να καινοτομήσουν στο μέλλον. Ως εκ τούτου, μια σειρά από κρίσιμες προκλήσεις πρέπει να αντιμετωπιστούν, προκειμένου να ενθαρρύνουν την υιοθέτηση του νέφους σε επιχειρήσεις [20].

Τα βασικά εμπόδια για την υιοθέτηση του νέφους περιλαμβάνουν:

- Το 79% έχει να κάνει με τον προμηθευτή,
- το 75% ανησυχούν για την απόδοση του νέφους και τη διαθεσιμότητα,
- 70% των CIOs δήλωσαν ότι η ασφάλεια των δεδομένων είναι μια σημαντική ανησυχία,
- 63% είχαν την ανησυχία για την ενσωμάτωση των εσωτερικών και εξωτερικών υπηρεσιών.

Ομοίως, σε μια πρόσφατη έρευνα του 2010 από το Ινστιτούτο Ερευνών της Fujitsu [21] σχετικά με πιθανούς πελάτες νέφους, διαπιστώθηκε ότι το 88% των δυνητικών καταναλωτών νέφους ανησυχούν για το ποιος έχει πρόσβαση στα δεδομένα τους και απαίτησαν μεγαλύτερη συνειδητοποίηση του τι συμβαίνει στον φυσικό server. Σύμφωνα με μια μελέτη σχετικά με τις απόψεις των εμπειρογνωμόνων σε θέματα ασφάλειας και την εμπειρία του χρήστη για την εμπιστοσύνη στον τομέα των υπηρεσιών νέφους [70] ο πιο σημαντικός παράγοντας που επηρεάζει την αντίληψη της εμπιστοσύνης στον τομέα των υπηρεσιών νέφους είναι το εμπορικό σήμα (brand name), με την ασφάλεια και την προστασία της ιδιωτικής ζωής να είναι η δεύτερη πιο σημαντική πτυχή και η διαφάνεια και η αξιοπιστία να έρχονται τρίτες. Επίσης, σημαντικό ρόλο παίζουν ο καλός έλεγχος και οι πολιτικές συμφωνίας. Οι επιχειρήσεις είναι σκεπτικές σχετικά με τις υποσχέσεις που πολλοί προμηθευτές δίνουν: 62% των ερωτηθέντων θεωρούν ότι, όταν ψάχνουν για έναν προμηθευτή, ένας κώδικας ορθής πρακτικής θα είναι σημαντικός, ενώ ένα περαιτέρω 28% θεωρεί ότι είναι απαραίτητος για τη διαδικασία επιλογής τους [9].

Δεδομένου το ότι οι πελάτες δεν έχουν τον έλεγχο των πόρων του νέφους, δεν είναι σε θέση για να αξιοποιήσουν τεχνικούς μηχανισμούς, προκειμένου να προστατεύσουν τα δεδομένα τους από μη εξουσιοδοτημένη πρόσβαση ή από δευτερεύουσα χρήση ή άλλες μορφές κατάχρησης. Αντ' αυτού, θα πρέπει να βασίζονται σε συμβόλαια ή άλλους μηχανισμούς εμπιστοσύνης για να προσπαθήσουν να ενθαρρύνουν την κατάλληλη χρήση, σε συνδυασμό με μηχανισμούς που προβλέπουν αποζημίωση σε περίπτωση παραβίασης, όπως η

ασφάλιση, δικαστικές ενέργειες ή κυρώσεις για την παραβίαση συμφωνιών επιπέδου υπηρεσιών (SLA's – Service Level Agreement).

Όταν δεν είναι σαφές στους ιδιώτες γιατί τους ζητούνται προσωπικές πληροφορίες, ή το πώς και από ποιον θα υποβληθούν σε επεξεργασία, αυτή η έλλειψη ελέγχου και η έλλειψη διαφάνειας στην αλυσίδα εφοδιασμού του παρόχου, θα οδηγήσει σε καχυποψία και τελικά δυσπιστία. Υπάρχουν επίσης ανησυχίες σχετικά με την ασφάλεια για το εάν τα δεδομένα στο νέφος θα πρέπει να προστατεύονται επαρκώς, όπως εξετάστηκε ανωτέρω. Ως αποτέλεσμα, οι πελάτες μπορεί να συγκρατηθούν στο να χρησιμοποιήσουν υπηρεσίες νέφους, όπου εμπλέκονται προσωπικές πληροφορίες, χωρίς την κατανόηση των υποχρεώσεων που εμπλέκονται και τους κινδύνους συμμόρφωσης που αντιμετωπίζουν και τη διασφάλιση ότι οι πιθανοί προμηθευτές θα αντιμετωπίσουν τέτοιους κινδύνους. Αυτό ιδιαίτερα σε περιπτώσεις ευαίσθητων πληροφοριών, για παράδειγμα, οικονομικών και πληροφοριών που έχουν να κάνουν με την υγεία [68].

4.3 Ασθενείς σχέσεις εμπιστοσύνης

Οι σχέσεις εμπιστοσύνης σε οποιοδήποτε σημείο υπηρεσιών του νέφους στην αλυσίδα διανομής μπορεί να είναι αδύναμες, αλλά αυτό υπάρχει ώστε μια υπηρεσία να μπορεί να παρέχεται γρήγορα. Σημαντικός επιχειρηματικός κίνδυνος μπορεί να υπάρξει με κάποιο τρόπο που δεν είναι διάφανος, όταν πραγματοποιείται μια συναλλαγή στο νέφος, λόγω της απώλειας του ελέγχου στο πέρασμα ευαίσθητων δεδομένων σε άλλους οργανισμούς και την παγκοσμιοποιημένη φύση της υποδομής του νέφους. Οργανισμοί που υπογράφουν βασικές επιχειρηματικές διαδικασίες μπορεί να μην γνωρίζουν καν ότι οι «εργολάβοι» είναι ανάδοχοι έργου, ή ακόμα και αν το γνωρίζουν, οι απαιτήσεις της σύμβασης όσον αφορά τα μέτρα προστασίας των δεδομένων δεν μπορούν να αναπαραχθούν κάτω από την συμφωνημένη αλυσίδα.

Η εμπιστοσύνη κατά μήκος της αλυσίδας από τον πελάτη στους παρόχους του νέφους σε όλα τα επίπεδα μπορεί να είναι μη μεταβατική και ιδίως ο πελάτης δεν

μπορεί να εμπιστεύεται μερικούς από τους αναδόχους έργου. Πράγματι, λόγω της έλλειψης διαφάνειας οι πελάτες δεν μπορούν καν να γνωρίζουν την ταυτότητα των παρόχων του νέφους στην αλυσίδα. Ειδικότερα, τα μοντέλα «on-demand» και «pay-as-you-go» μπορεί να βασίζονται σε ανεπαρκείς σχέσεις εμπιστοσύνης, συμμετοχή τρίτων με χαλαρές πρακτικές ασφαλείας των δεδομένων, να εκθέτουν τα δεδομένα ευρέως και να κάνουν τη διαγραφή δύσκολο να εξακριβωθεί. Με σκοπό την παροχή επιπλέον χωρητικότητας σε σύντομο χρονικό διάστημα ή σε πραγματικό χρόνο, νέοι πάροχοι θα μπορούσαν να προστεθούν στην αλυσίδα όπου όμως δεν υπάρχουν επαρκείς ευκαιρίες να γίνουν σωστοί έλεγχοι σχετικά με την ταυτότητα, τις πρακτικές, τη φήμη και την αξιοπιστία τους.

4.4 Έλλειψη συναίνεσης γύρω από την προσέγγιση διαχείρισης της εμπιστοσύνης που πρέπει να χρησιμοποιείται

Υπάρχει έλλειψη συναίνεσης γύρω από το τι προσεγγίσεις διαχείρισης της εμπιστοσύνης θα πρέπει να χρησιμοποιούνται για περιβάλλοντα νέφους. Η εγγενής πολυπλοκότητα της εμπιστοσύνης, η υποκειμενικότητα κάποιων παραγόντων και η δυσκολία αναπαράστασης κάνει τη μέτρηση της εμπιστοσύνης να αποτελεί μια μεγάλη πρόκληση. Οι Artz και Gil παρέχουν πτυχές της εμπιστοσύνης που μπορούν να μετρηθούν για σκοπούς αξιολόγησης. Χρειάζονται τυποποιημένα μοντέλα εμπιστοσύνης για τον έλεγχο και τη διασφάλιση της ευθύνης, αλλά κανένα από το μεγάλο αριθμό των υπαρχόντων μοντέλων εμπιστοσύνης μέχρι σήμερα δεν είναι επαρκές για το περιβάλλον νέφους [4]. Υπάρχουν πολλά μοντέλα εμπιστοσύνης που προσπαθούν να υιοθετήσουν μερικά από τα στοιχεία που ορίζονται από τον Marsh και άλλους και υπάρχουν πολλοί μηχανισμοί αξιολόγησης της εμπιστοσύνης που στοχεύουν να τα μετρήσουν [48]. Αυτοί οι μηχανισμοί έχουν την τάση να αναπτύσσονται σε απομόνωση και υπάρχει μικρή ενοποίηση μεταξύ σκληρών και μαλακών λύσεων εμπιστοσύνης. Δεν υπάρχουν μετρήσεις για την ευθύνη, μόνο μια μελέτη πολύ υψηλού επιπέδου έως σήμερα. Επιπλέον, δεν υπάρχει καμία τρέχουσα συναίνεση σχετικά με τους

τύπους των αποδεικτικών στοιχείων που απαιτούνται για την εξακρίβωση της αποτελεσματικότητας των μηχανισμών εμπιστοσύνης. Παρά το γεγονός ότι το πρωτόκολλο εμπιστοσύνης νέφους καθορίζει ορισμένες κατηγορίες, δεν καλύπτει άλλες όπως τη νομική ευθύνη των εμπλεκόμενων μερών [13].

4.5 Εμπιστοσύνη – Συμπερασματικά

Η εμπιστοσύνη είναι ευρέως αντιληπτή ως ένα βασικό μέλημα για τους τελικούς χρήστες, τους πελάτες και τις ρυθμιστικές αρχές. Η έλλειψη εμπιστοσύνης των καταναλωτών αποτελεί βασικό ανασταλτικό παράγοντα των υπηρεσιών νέφους. Οι άνθρωποι είναι καχύποπτοι για το τι συμβαίνει στα δεδομένα τους, τη στιγμή που αυτά πηγαίνουν στο νέφος. Ανησυχούν για το ποιος μπορεί να έχει πρόσβαση, πώς θα αντιγραφούν, μοιραστούν και χρησιμοποιηθούν και αισθάνονται ότι χάνουν τον έλεγχο. Οι εταιρείες που αλλάζουν τη λειτουργία τους από τους τοπικούς υπολογιστές στη χρήση δημόσιου νέφους, δεν ενδιαφέρονται τόσο για την κατάσταση των servers, αλλά αντίθετα, για την εμπιστευτικότητα και την ασφάλεια των δεδομένων τους. Οι ρυθμιστικές αρχές φοβούνται ότι οι έλεγχοι δικαιοδοσίας και η συμμόρφωση θα αποδυναμωθούν με το νέφος. Όλα τα μέρη ανησυχούν για τη δυνητική πρόσβαση από ορισμένες ξένες κυβερνήσεις, εάν ευαίσθητα δεδομένα μετακινηθούν για να αποθηκευτούν μέσα σε αυτές τις χώρες.

Τελικά, η χρήση του νέφους είναι ένα ζήτημα ανταλλαγής μεταξύ ασφάλειας, προστασίας της ιδιωτικής ζωής, συμμόρφωσης, κόστους και ωφέλους. Η εμπιστοσύνη είναι το κλειδί για την υιοθέτηση του SaaS και η διαφάνεια είναι ένας σημαντικός μηχανισμός. Επιπλέον, οι μηχανισμοί εμπιστοσύνης πρέπει να διαδοθούν σε όλο το μήκος της αλυσίδας παροχής υπηρεσιών.

Κεφάλαιο 5
Το Υπολογιστικό Νέφος και Εφαρμογές

5.1 Εφαρμογές στα νέφη

Κατά την ανάπτυξη μιας εφαρμογής στο νέφος, θα πρέπει να αναλυθούν τα πλεονεκτήματα και τα μειονεκτήματα του κατανεμημένου συστήματος (δηλαδή του διαδικτύου στην συγκεκριμένη περίπτωση) αλλά και των θεμελιωδών χαρακτηριστικών που προσφέρουν τα νέφη. Κάθε εφαρμογή μπορεί να εκτελείται πλήρως ή μερικώς στο νέφος. Τα θεμελιώδη χαρακτηριστικά που πρέπει να προσφέρει ένα νέφος είναι τα ακόλουθα:

- Αφαιρετικότητα συστήματος και επαναπροσανατολισμός.
- Εξελιξιμότητα.
- Σύνολο προγραμματιστικών διασυνδέσεων εφαρμογών (APIs) της εφαρμογής και του συστήματος.
- Μικρές καθυστερήσεις στα τοπικά δίκτυα υπολογιστών (Local Area network-LAN) και στα δίκτυα ευρείας περιοχής (Wide Area network-WAN).

Αρχικά κατά τη μεταφορά της εφαρμογής στο νέφος, το στέλεχος ανάπτυξης θα πρέπει να εξετάσει εάν οι λειτουργίες της εφαρμογής εξυπηρετούνται καλύτερα από το νέφος ή την συνήθη τοπική ανάπτυξη. Η απάντηση εξαρτάται σ' ένα πολύ μεγάλο ποσοστό από τα χαρακτηριστικά γνωρίσματα της εφαρμογής που προσπαθεί να συντηρήσει ή να ενισχύσει. Επίσης, η θέση μιας εφαρμογής ή μιας υπηρεσίας παίζει πολύ σημαντικό ρόλο στο τρόπο με τον οποίο πρέπει να

κατασκευαστεί και να αναπτυχθεί μια εφαρμογή. Ειδικότερα, μια εφαρμογή ή μια διαδικασία που εκτελείται σ' έναν υπολογιστή γραφείου ή σε έναν εξυπηρέτη, εκτελείται συνεκτικά και ενιαία ως μια μονάδα, κάτω από τον έλεγχο ενός προγράμματος. Με λίγα λόγια μια ενέργεια προξενεί τα εξής:

1. Αρχικά, προκαλεί μια κλήση προγράμματος,
2. Εν συνεχεία, εκτελείται ο κώδικας και
3. Τελικά, επιστρέφεται ένα αποτέλεσμα.

Στη συνέχεια, όσον αφορά τις ατομικές δοσοληψίες. Ως ατομική δοσοληψία θεωρείται μία ακολουθία συμβάντων της μορφής:*αίτηση→διαδικασία→απόκριση*. Όμως καθώς η δοσοληψία εκτελείται τοπικά μέσα σε μια εφαρμογή, η διαδικασία έχει καταστάσεις και κατά συνέπεια η δοσοληψία είναι συνεπής και η κατάστασή της είναι πάντα γνωστή. Μια συνεπής δοσοληψία είτε πετυχαίνει και εν συνεχεία ολοκληρώνεται και μονιμοποιείται, είτε αποτυγχάνει και επιστρέφει στην προηγούμενη κατάσταση. Όταν δεν μπορεί να γίνει η επιστροφή στη προηγούμενη κατάσταση (φαινόμενο που ονομάζεται και rollback) λόγω πιθανής δέσμευσης της δοσοληψίας σε μια εφαρμογή πολλών χρηστών, τότε απαιτείται η διόρθωση της κατάστασης ή, η εκτέλεση κάποιας αντισταθμιστικής ενέργειας σε μεταγενέστερο χρόνο.

Μια εφαρμογή που εκτελείται ως υπηρεσία στο διαδίκτυο, αποτελείται από δυο μέρη:

- Αυτό του εξυπηρετούμενου που υποβάλλει μια αίτηση και
- Αυτό του εξυπηρέτη που αποκρίνεται στην αίτηση.

Η αίτηση είναι αποσυνδεδεμένη από την απόκριση, υπό την έννοια ότι η δοσοληψία εκτελείται σε δύο ή περισσότερες τοποθεσίες. Επίσης, σε ένα κατανεμημένο σύστημα, η δοσοληψία είναι άνευ καταστάσεων. Προκειμένου λοιπόν σε μια κατανεμημένη αρχιτεκτονική να δημιουργηθεί ένα σύστημα με καταστάσεις, πρέπει να προστεθεί μία οντότητα με τον ρόλο υπεύθυνος δοσοληψιών. Η ενδιάμεση αυτή οντότητα θα μπορεί να χρησιμοποιηθεί για τις δοσοληψίες και να αντιδρά αναλόγως όταν οι τελευταίες επιτυγχάνουν ή αποτυγχάνουν [7].

Τέλος, κατά τη μεταφορά των εφαρμογών στο νέφος διατηρούνται τα χαρακτηριστικά γνωρίσματα μιας αρχιτεκτονικής τριών επιπέδων. Επίσης, τα φυσικά συστήματα γίνονται εικονικά. Οι εικονικές μηχανές δεν είναι μόνο άνευ καταστάσεων, αλλά και η τοποθεσία όπου πραγματοποιείται η εκτέλεση του προγράμματος μπορεί να είναι διαφορετική, κάθε φορά που εκτελείται η διαδικασία.

5.2 Αξιόπιστες δοσοληψίες και οι ιδιότητές τους

Οι ιδιότητες ACID των αξιόπιστων δοσοληψιών διατυπώθηκαν από τον Jim Gray και εφαρμόστηκαν για πρώτη φορά στην τεχνολογία των βάσεων δεδομένων προς το τέλος της δεκαετίας του '70. Στην σημερινή εποχή χρησιμοποιείται από οποιαδήποτε εφαρμογή που διαβάζει και γράφει σε ένα σύνολο αποθηκευμένων δεδομένων, το όποιο περιλαμβάνει όλους τους τύπους εφαρμογής. Συγκεκριμένα, τα γράμματα της λέξης ACID προέρχονται από τις ακόλουθες τέσσερις λέξεις:

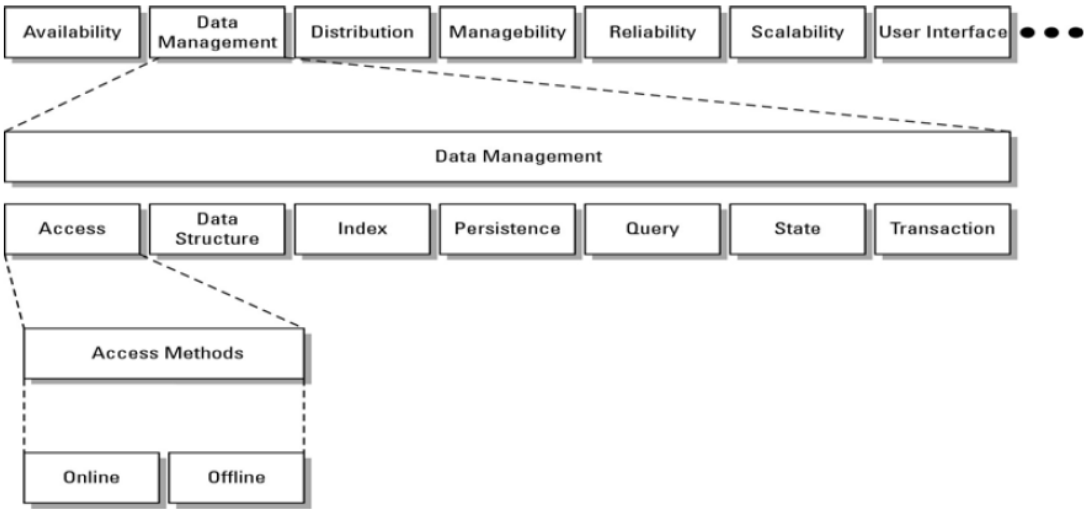
- **Ατομικότητα (Atomicity):** Όσον αφορά την ιδιότητα της ατομικότητας πρέπει να ειπωθεί πως καθορίζει μια δοσοληψία ως κάτι που δεν μπορεί να διαιρεθεί αλλά πρέπει να ολοκληρωθεί ή αντιστρόφως να εγκαταλειφθεί, ως μια ενιαία μονάδα.
- **Συνέπεια (Consistency):** Η ιδιότητα της συνέπειας δηλώνει ότι το σύστημα στο τέλος της δοσοληψίας θα πρέπει να μεταφερθεί από μια γνωστή-συνεπή κατάσταση σε μια άλλη. Επίσης, η ιδιότητα αυτή δηλώνει ότι πρέπει να διατηρηθεί η ακεραιότητα του συστήματος.
- **Απομόνωση (Isolation):** Η ιδιότητα της απομόνωσης δηλώνει ότι τα αποτελέσματα μιας δοσοληψίας δεν πρέπει να επηρεάζονται από άλλες δοσοληψίες που τυχόν εκτελούνται την ίδια στιγμή.
- **Διάρκεια (Durability):** Η ιδιότητα της διάρκειας δηλώνει ότι το σύστημα πρέπει να έχει έναν μηχανισμό ο οποίος μετά την επιτυχή πραγματοποίηση μιας δοσοληψίας τα αποτελέσματά της μένουν μόνιμα στο σύστημα [37].

5.3 Λειτουργικότητα εφαρμογής και χαρτογράφηση

Για να αποφασίσει κάποιος υπεύθυνος να μεταφέρει την εφαρμογή του στο νέφος έτσι ώστε να επωφεληθεί από την ανάπτυξη του νέφους, θα χρειαστεί να αποδομήσει τη λειτουργικότητα της συγκεκριμένης εφαρμογής στα βασικά στοιχεία της και εν συνεχεία να αναγνωρίσει τις λειτουργίες που είναι θεμελιώδεις και που μπορούν να υποστηριχθούν από το νέφος.

Επιπλέον, τα συστήματα δοσοληψιών απαιτούν τα δεδομένα μιας βάσης δεδομένων να διατηρούν την ακεραιότητα των δοσοληψιών του μοντέλου ACID. Για πολλά μη σχεσιακά συστήματα αποθήκευσης στο νέφος, (όπως η υπηρεσία Amazon Simple Storage Service (S3), η υπηρεσία Google Storage, καθώς και η υπηρεσία Windows Azure), η δυνατότητα του συστήματος να διατηρεί την ακεραιότητα των δοσοληψιών μέσω του κλειδώματος των αρχείων, δεν υποστηρίζεται άμεσα. Αυτοί οι τύποι των συστημάτων αποθήκευσης είναι ασφαλείς και αποθηκεύουν μεγάλες ποσότητες δεδομένων. Διαθέτουν όμως πολύ αργή πρόσβαση στα συγκεκριμένα δεδομένα κι επίσης δεν υποστηρίζουν επερωτήσεις και ανάκτηση πληροφορίας [49].

Στην Εικόνα 5.3, κατασκευάζεται ένα δέντρο ιδιοτήτων για ένα σύστημα δοσοληψιών όπου η λειτουργικότητα αποσυντίθεται σε διαφορετικές περιοχές λειτουργίας. Μπορεί να παρατηρήσει κάποιος πως στο ανώτερο επίπεδο βρίσκονται τα χαρακτηριστικά γνωρίσματα υψηλού επιπέδου, όπου κάποια από αυτά αφορούν τη λειτουργία της εφαρμογής ενώ κάποια άλλα όχι. Στη συνέχεια, σε καθοδική παράθεση προς το χαρακτηριστικό γνώρισμα της διαχείρισης δεδομένων, το δεύτερο επίπεδο σχετίζεται αρχικά με την προσπέλαση δεδομένων κι έπειτα με την προσπέλαση μεθόδων. Ένα κρίσιμο χαρακτηριστικό γνώρισμα της εφαρμογής αυτής είναι η ανάγκη προσπέλασης δεδομένων όταν ο εξυπηρετούμενος είναι τόσο online στο νέφος όσο και offline.



Εικόνα 5.3. Δημιουργία χάρτη χαρακτηριστικών γνωρισμάτων για την παρουσίαση της λειτουργικότητας.

Πηγή: www.google.gr/εικόνες

Η αλληλεπίδραση της εφαρμογής τόσο με το υπολογιστικό νέφος όσο και με τα δεδομένα καθορίζεται από το αν επιτρέπεται τόσο η προσπέλαση των δεδομένων online όσο και offline. Εάν η εφαρμογή μπορεί να προσπελάσει τα δεδομένα μόνο όταν ο εξυπηρετούμενος είναι online, τότε η τελευταία θα χρειάζεται ως μοναδική αποθήκη δεδομένων (data store), την πρόσβαση στον αποθηκευτικό χώρο που βασίζεται στο νέφος. Ίσως η εφαρμογή θα ήταν εξ' ολοκλήρου στο νέφος και θα βασιζόταν στην εφαρμογή πλοήγησης.

Με σκοπό να επιτραπεί τόσο η προσπέλαση των δεδομένων του νέφους όσο και η τοπική προσπέλαση δεδομένων, θα πρέπει να δημιουργηθεί μια υβριδική εφαρμογή αποτελούμενη από τα εξής τμήματα:

- Ένα τμήμα νέφους,
- Ένα τοπικό τμήμα.

Ακόμα και αν η πρόσβαση στα δεδομένα, στο τοπικό σύστημα είναι ένα απλό σύστημα αποθήκευσης, εντούτοις απαιτείται υποστήριξη στην πλευρά του εξυπηρετούμενου. Έτσι, για την υποστήριξη της πρόσβασης στα δεδομένα της εφαρμογής, μπορεί επίσης να χρειαστεί η κατασκευή ενός χαρακτηριστικού

γνωρίσματος συγχρονισμού, το οποίο προσθέτει μεγαλύτερη επιβάρυνση στην εφαρμογή.

Αυτού του είδους η χαρτογράφηση μας οδηγεί στα ακόλουθα συμπεράσματα όσον αφορά το υπολογιστικό νέφος:

- Μια εφαρμογή που χρησιμοποιεί αποθήκευση δεδομένων στο νέφος, ωφελείται περισσότερο από την ανάπτυξή της σε αυτό, σε σχέση με μια εφαρμογή που χρησιμοποιεί τοπική (offline) αποθήκευση.
- Στην περίπτωση μιας υβριδικής εφαρμογής, υπάρχουν κάποιοι παράγοντες που μπορούν να αντισταθμίσουν το κόστος της τοπικής (offline) αποθήκευσης και να κάνουν πιο λειτουργικό το νέφος. Τέτοιοι είναι η κλιμάκωση (scalability), τα έξοδα καθώς και η διάχυτη, δηλαδή ευρεία, πρόσβαση [23].

5.4 Βασικά στοιχεία εφαρμογής

Η αποδόμηση της λειτουργικότητας μιας συγκεκριμένης εφαρμογής στα βασικά στοιχεία της, αποτελεί μόνο ένα τμήμα της διαδικασίας σε ό,τι αφορά τη μεταφορά αυτής στο νέφος. Αυτό συμβαίνει διότι κάθε πλατφόρμα νέφους διαθέτει το δικό της σύνολο χαρακτηριστικών γνωρισμάτων που χρειάζεται να χαρτογραφηθούν.

Τα κύρια κριτήρια για να εξαχθεί το συμπέρασμα αν ωφελούνται οι εφαρμογές από την ανάπτυξή τους στο νέφος είναι τα ακόλουθα:

- Δεν υλοποιούν βασικές επιχειρησιακές λειτουργίες.
- Δεν υπάρχουν ευαίσθητα δεδομένα να προστατεύσει.
- Γίνονται ανεκτές υψηλές καθυστερήσεις δικτύου ή χαμηλό εύρος ζώνης δικτύου.
- Είναι εφαρμογές που δεν παρέχουν συγκεκριμένο ανταγωνιστικό πλεονέκτημα.
- Βασίζονται σε τυποποιημένες τεχνολογίες βιομηχανίας.
- Δεν χρειάζεται να είναι προσαρμοσμένες σε κάποιο πρότυπο.

- Είναι αρκετά ώριμες και κατανοητές ώστε να μπορούν να συνδεθούν επιτυχώς στο νέφος [25].

5.5 Τα βασικά στοιχεία των υπηρεσιών νέφους

Εφόσον μέχρι αυτό το σημείο ανάπτυξης, αναφέρθηκαν τα χαρακτηριστικά γνωρίσματα μιας πλατφόρμας, ώστε να ωφελείται μια εφαρμογή από την ανάπτυξή της στο νέφος, ακολουθεί η αντιστοίχιση αυτών των χαρακτηριστικών γνωρισμάτων με τα παρακάτω βασικά χαρακτηριστικά γνωρίσματα των υπηρεσιών νέφους:

- Εφαρμογές.
- Βασικές υπηρεσίες.
- Υποδομή.
- Χαρακτηριστικά γνωρίσματα πλατφορμών.
- Αποθήκευση.

Στο τρέχον στάδιο της ανάπτυξης μιας εφαρμογής, δεν είναι εφικτή η αντιστοίχιση των αναγκών της εφαρμογής μ' ένα σύνολο παρόχων υπηρεσιών νέφους. Αυτό συμβαίνει για τους λόγους ότι ο κάθε πάροχος:

- Έχει μια μοναδική λύση.
- Χρησιμοποιεί τις δικές του προγραμματιστικές διασυνδέσεις εφαρμογών (APIs).
- Παρέχει μοναδικές υπηρεσίες.

Επομένως, κάθε πάροχος υπηρεσιών νέφους απαιτείται να έχει δεξιότητες ανάπτυξης εφαρμογών, καθώς και να παρέχει ολοκλήρωση μεταξύ των νεφών. Ίσως αυτό το φαινόμενο να αλλάξει στο μέλλον καθώς αναπτύσσονται περισσότερα πρότυπα. Όμως προς το παρόν, τα στελέχη ανάπτυξης εφαρμογών πρέπει να αντιστοιχίσουν την εφαρμογή τους με τον καλύτερο πάροχο [43].

5.6 Εικονικό σύστημα

Όπως έχει αναφερθεί και προηγούμενα, το νέφος μετατρέπει τα φυσικά συστήματα σε εικονικά. Ειδικότερα, οι οργανισμοί επιλέγουν να αναπτύξουν εξ' ολοκλήρου τα συστήματα τους στο νέφος, έχοντας σαν σκοπό να μπορούν να αναδιαμορφώσουν το βασικό μέρος της διαδικασίας και να εξαλείψουν την έννοια της υποδομής.

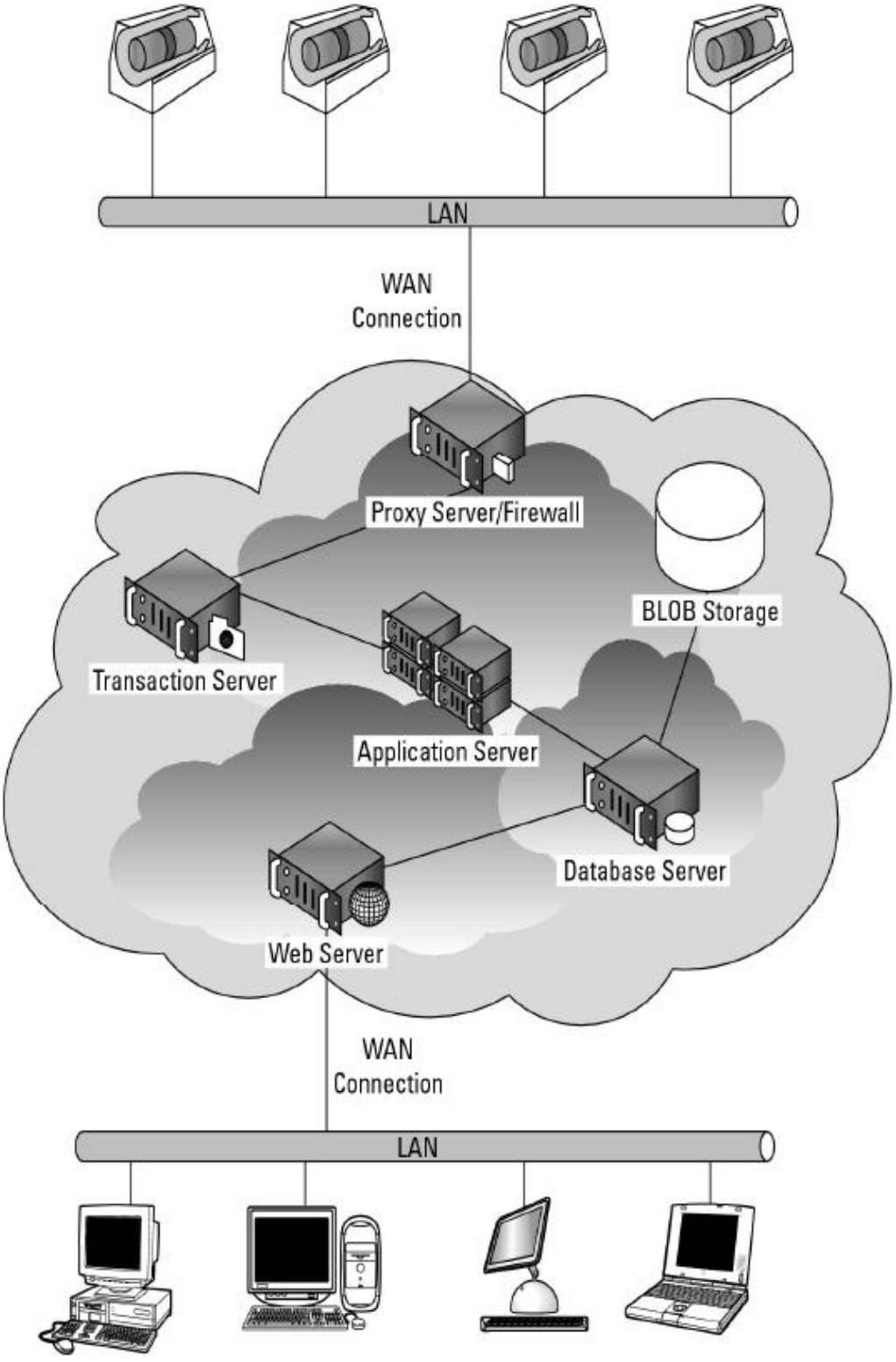
Ένα παράδειγμα του φαινομένου αυτού, αποτελεί μια υπηρεσία ιατρικής απεικόνισης. Στο παρελθόν, όπως ήταν σύνηθες, με την υπηρεσία αυτή, δημιουργούνταν απεικονίσεις ασθενών (ακτινογραφίες, τομογραφίες κ.λπ.) κι έπειτα αποθηκεύονταν σε έναν τοπικό υπολογιστή. Εν συνεχεία, αφ' ότου κάποιος αποθήκευε την εικόνα στον υπολογιστή, γινόταν αυτομάτως διαθέσιμη στο τοπικό δίκτυο του νοσοκομείου. Με τον τρόπο αυτό μπορούσε κάποιος γιατρός να τη δει και να την επεξηγήσει. Επιπλέον, όταν οι γιατροί ήταν εκτός του χώρου του νοσοκομείου, τότε θα χρειαζόταν να εισέλθουν μέσω ενός εικονικού ιδιωτικού δικτύου (Virtual Private Network-VPN) στον εξυπηρέτη του νοσοκομείου προκειμένου να προβάλλουν το αρχείο στον δικό τους υπολογιστή.

Η παραπάνω υπηρεσία απεικόνισης μπορεί να μεταβληθεί κάνοντας χρήση των δύο ακόλουθων τρόπων:

1. Αρχικά, εξαλείφεται η έννοια της υποδομής. Αυτό συμβαίνει μέσω της επανανάπτυξης της εφαρμογής μετακινώντας τις αποθηκευμένες εικόνες από το τοπικό δίκτυο LAN του νοσοκομείου στον κοινό αποθηκευτικό χώρο του νέφους. Αυτό το χαρακτηριστικό γνώρισμα εξαλείφει άμεσα την ανάγκη διατήρησης μεγάλης ικανότητας αποθήκευσης τοπικά. Έπειτα, καθώς οι χρήστες της υπηρεσίας προσπελαύνουν τις εικόνες, ενεργοποιείται ένα χαρακτηριστικό γνώρισμα που απαντάται στα δίκτυα παράδοσης περιεχομένου (Content Delivery Networks) και το οποίο τυπικά ενσωματώνει και ο πάροχος της υπηρεσίας νέφους. Βάσει του χαρακτηριστικού αυτού, το δίκτυο τοποθετεί τα αντίγραφα εικόνων που χρησιμοποιήθηκαν πρόσφατα σε τοποθεσίες που είναι πιο κοντά στους αναγνώστες κι έτσι το σύστημα γίνεται αρκετά γρηγορότερο.

2. Στο δεύτερο στάδιο, εξαλείφεται η τοπική επεξεργασία που σχετίζεται με τις μηχανές απεικόνισης, δηλαδή με τη συλλογή των στοιχείων και των δεδομένων.

Επιπροσθέτως, στο νέο σύστημα όπως απεικονίζεται και στην Εικόνα 3, τα αρχεία δημιουργούνται τοπικά και μεταφέρονται στο νέφος. Επίσης οι εικονικές μηχανές επεξεργάζονται τις απεικονίσεις. Ακόμα, το σύστημα ενσωματώνει λειτουργικότητα ουράς μηνυμάτων, έτσι ώστε να παρέχεται μία ομαλή ροή αιτήσεων προς τον εξυπηρέτη. Όσον αφορά τις χρονικές περιόδους που διακινείται το μέγιστο φορτίο, το σύστημα δημιουργεί αυτόματα νέα στιγμιότυπα για να χειριστεί το φόρτο εργασίας [50].



Εικόνα 5.6. Εφαρμογή που αναπτύσσεται εξ' ολοκλήρου στο νέφος.

Πηγή: www.google.gr/εικόνες

Τέλος, όταν ο εξυπηρέτης της εφαρμογής ολοκληρώσει την επεξεργασία απεικόνισης ακολουθεί την εξής διαδικασία:

- Αρχικά, ενημερώνει την ουρά αναμονής μηνυμάτων,
- Στη συνέχεια, καταγράφει το αποτέλεσμα σε μια βάση δεδομένων, και
- Τέλος, παρουσιάζει το αποτέλεσμα σε μια ιστοσελίδα, η οποία κι αυτή με τη σειρά της διατίθεται μέσω του νέφους.

Το σύστημα που αναπτύσσεται στο νέφος είναι πιο αποδοτικό, διότι το σύστημα εκτελεί τις επεξεργασίες πάντα στο βέλτιστο φόρτο εργασίας του. Επίσης, η υποδομή, ο αποθηκευτικός χώρος και το σύστημα ουράς εξαλείφουν μεγάλο μέρος του κόστους και της λειτουργικής πολυπλοκότητας.

Στη συνέχεια, οι απεικονίσεις είναι διαθέσιμες, πάντα μέσω ενός προγράμματος πλοήγησης και επειδή το σύστημα έχει ικανότητα κλιμάκωσης, η υπηρεσία απεικόνισης μπορεί να επεκταθεί και σε άλλες ιστοσελίδες. Τέλος, ένα πολύ σημαντικό χαρακτηριστικό έχει να κάνει με την εξοικονόμηση χρόνου. Δηλαδή όταν αποφασιστεί να γίνει μετασχηματισμός των εικόνων σε διαφορετικές μορφοποιήσεις (formats), η διαδικασία αυτή μπορεί να πραγματοποιηθεί στον κεντρικό εξυπηρέτη και όχι στα διαφορετικά συστήματα απεικόνισης.

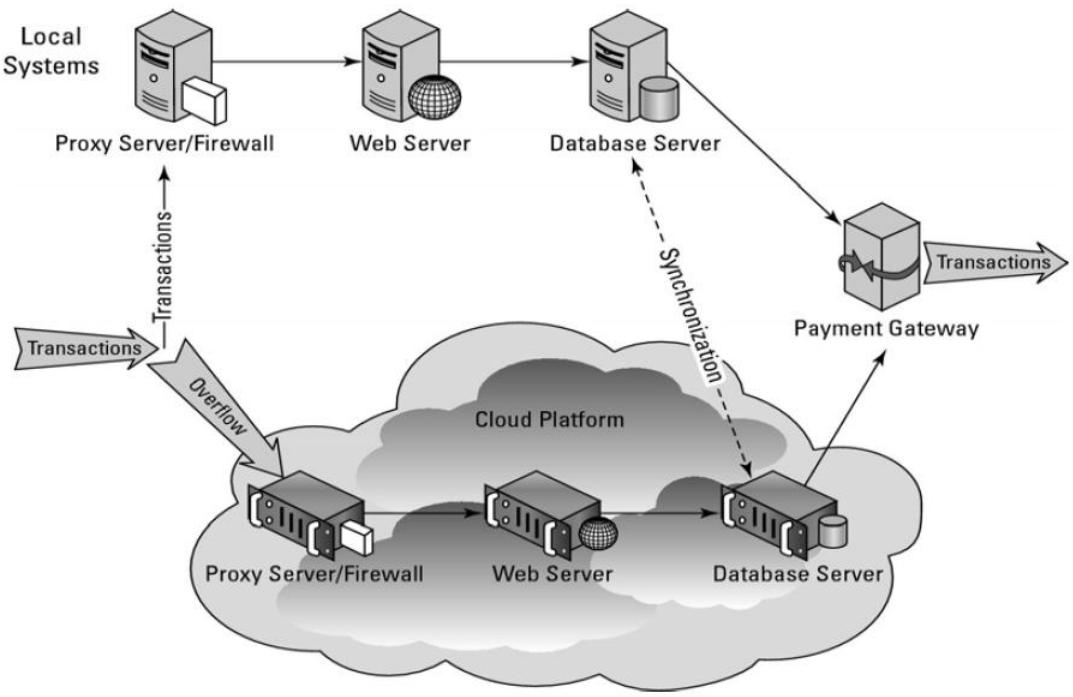
5.7 Cloud bursting (έκρηξη νέφους)

Οι περισσότερες εφαρμογές νέφους είναι υβριδικές, μιας και ένα μέρος τους βρίσκεται σ' ένα τοπικό σύστημα, ενώ ένα άλλο μέρος τους βρίσκεται στο νέφος. Ένας από τους πιο σημαντικούς λόγους για τον οποίο είναι επιθυμητό αυτό το γεγονός (το οποίο γεγονός ονομάζεται *έκρηξη νέφους*), έχει να κάνει με το ότι το νέφος μπορεί να εξυπηρετήσει ως επιπρόσθετη χωρητικότητα σε περιόδους μεγάλου φόρτου εργασίας.

Παραδείγματα τέτοιων συστημάτων (με μεγάλο όγκο εργασίας σε μικρές χρονικές περιόδους) αποτελούν τα συστήματα επεξεργασίας δοσοληψιών και πιο συγκεκριμένα τα συστήματα κρατήσεων. Σε ένα σύστημα κρατήσεων, υπάρχει ένα συγκεκριμένο επίπεδο, το οποίο γενικά είναι χαμηλό, όπου

πραγματοποιούνται δοσοληψίες όλες τις χρονικές στιγμές. Σε συγκεκριμένες χρονικές περιόδους όμως (όπως για παράδειγμα στις περιόδους αργιών, διακοπών, κ.λπ.), η ζήτηση αυξάνεται σημαντικά. Έτσι, αν το σύστημα δημιουργούσε μια υποδομή με σκοπό το χειρισμό της μέγιστης αυτής ζήτησης, τότε η υποδομή αυτή θα υποχρησιμοποιείτο το μεγαλύτερο χρονικό διάστημα [38].

Επίσης, τα περισσότερα υβριδικά συστήματα σχεδιάζονται με απώτερο σκοπό την κλωνοποίηση του τοπικού συστήματος στο νέφος. Συχνά, υπάρχει ένα μικρό μέρος δραστηριότητας που εξελίσσεται στο μέρος του συστήματος, το οποίο βρίσκεται στο νέφος, αλλά όσο αυξάνεται η ζήτηση, τόσο το συγκεκριμένο μέρος του συστήματος παίρνει επιπρόσθετους πόρους από το νέφος. Η Εικόνα 5.7(α) παρουσιάζει ένα απλό σύστημα κρατήσεων που έχει στηθεί για έκρηξη νέφους.



Εικόνα 5.7 (α). Εφαρμογή που διαχειρίζεται την υπερχείλιση δοσοληψιών σ' ένα σύστημα κρατήσεων (παράδειγμα έκρηξης νέφους).

Πηγή: www.google.gr/εικόνες

Συχνά τα συστήματα κρατήσεων απαιτούν οι δοσοληψίες όχι μόνο να έχουν την ιδιότητα της ατομικότητας, αλλά και το σύστημα να είναι συνεπές κατά την εκτέλεση παραλλήλων δοσοληψιών. Για να ικανοποιηθεί αυτή η ανάγκη, πρέπει να δημιουργηθεί ένας επόπτης δοσοληψιών. Στην εικόνα παρουσιάζεται ως διακεκομμένη γραμμή μεταξύ των δύο εξυπηρετών βάσεων δεδομένων, με όνομα "Synchronization". Ο μηχανισμός αυτός έχει σκοπό την εκτέλεση κλειδώματος εγγραφών σε μία βάση δεδομένων.

Στα περισσότερα συστήματα κρατήσεων, το μεγαλύτερο μέρος της συμφόρησης παράγεται στην ιστοσελίδα του Διαδικτύου καθώς οι χρήστες περιηγούνται στο περιεχόμενό της. Για τον λόγο αυτό, προκειμένου να αντιμετωπιστεί η συμφόρηση αυτή προκύπτουν οι εξής λύσεις:

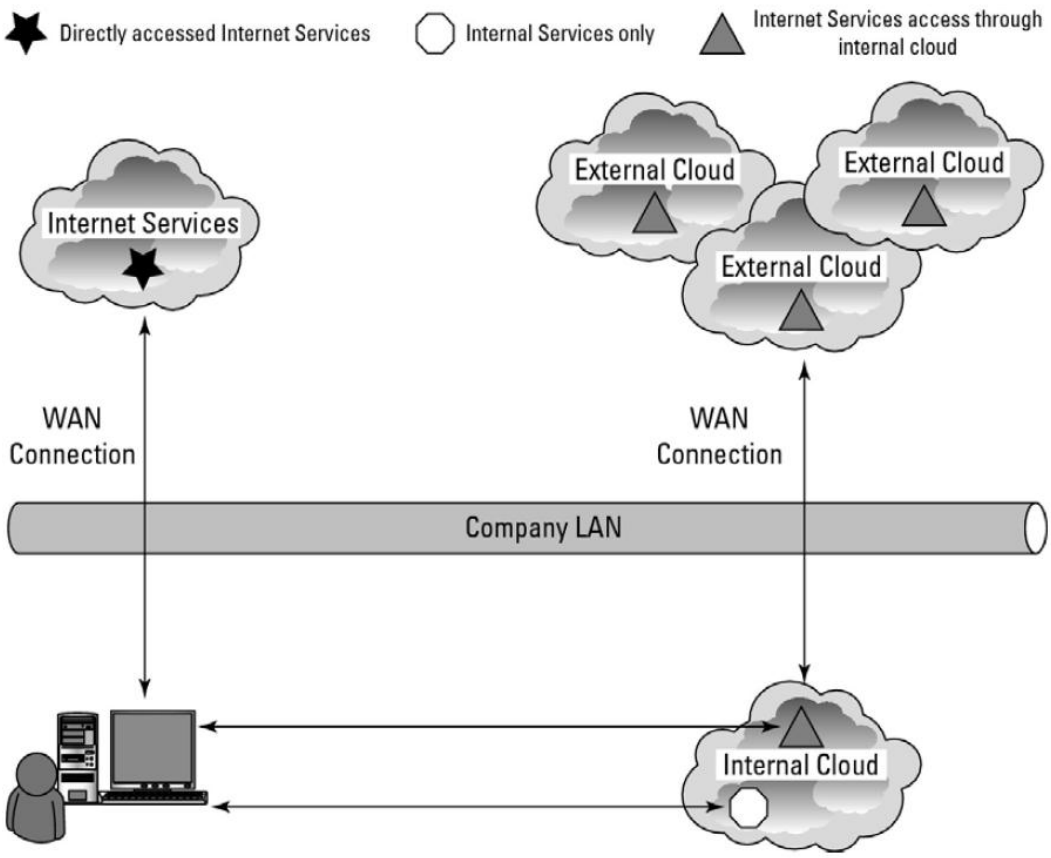
- Αναδημιουργία της ιστοσελίδας προκειμένου να δημιουργηθούν επιπρόσθετα στιγμιότυπα εξυπηρετών φόρτου εργασίας.
- Βελτιστοποίηση στην ιστοσελίδα μέσω της δημιουργίας κάποιου στατικού περιεχομένου ώστε να μην χρειάζονται συνεχώς άσκοπες δοσοληψίες με δυναμικό περιεχόμενο.
- Τέλος, ένα πολύ σημαντικό βήμα αποτελεί ο συγχρονισμός των αλλαγών μεταξύ των τοπικών υπολογιστών και των εξυπηρετών του νέφους προκειμένου να διατηρούνται οι τρέχουσες πληροφορίες.

Άλλο ένα μεγάλο πρόβλημα που αντιμετωπίζουν τα συστήματα κρατήσεων, είναι ο συγχρονισμός των πληρωμών και η επικοινωνία με τις επιχειρήσεις πιστωτικών καρτών καθώς και τους χρηματοπιστωτικούς οργανισμούς. Μια πιθανή λύση είναι να μετακινηθεί ολόκληρος ο συγχρονισμός στο νέφος, έτσι ώστε η επεξεργασία των πληρωμών να μην μπορεί να επηρεάσει τα υπόλοιπα μέρη του συστήματος. Σημειώνεται επίσης ότι δεν παίζει κανένα ρόλο το γεγονός ότι ένας εικονικός εξυπηρέτης εκτελεί τις διαδικασίες πληρωμών, καθώς και το ότι η διαδικασία αυτή δεν έχει καταστάσεις [5].

Τέλος άξιο λόγου είναι πως οι αρχιτεκτονικές νέφους προσφέρουν αρκετά πλεονεκτήματα, που εκτιμάται ότι προοδευτικά θα υιοθετηθούν από μεγάλους οργανισμούς, ως βασικά μέρη της σχεδίασής τους. Για παράδειγμα, στην Εικόνα 5.7(β), παρατηρούνται τα ακόλουθα:

- Ένα εσωτερικό νέφος παρέχει υπηρεσίες δοσοληψιών μεγάλης ταχύτητας στο τοπικό δίκτυο LAN.
- Ένα εξωτερικό νέφος παρέχει υπηρεσίες όσον αφορά άλλες ανάγκες των χρηστών.
- Το νέφος της επιχείρησης αναπαράγεται σε πολλαπλές ιστοσελίδες.

Επιπλέον, οι υπηρεσίες αυτές εξαρτώνται από διάφορους παράγοντες, όπως είναι το κόστος, οι καθυστερήσεις αλλά και η ευκολία.



Εικόνα 5.7(β). Παράδειγμα χρηστών σε μεγάλους οργανισμούς

Πηγή: www.google.gr/εικόνες

5.8 Το μέλλον του υπολογιστικού νέφους και προοπτικές

5.8.1 Αξιοπιστία – οικονομία – ασφάλεια – ευκολία

Όπως είναι αναμενόμενο, μελλοντικά το υπολογιστικό νέφος θα γίνει περισσότερο αξιόπιστο, πιο οικονομικό για τους χρήστες, ασφαλέστερο αλλά και πιο εύκολο στη χρήση. Οι επιχειρήσεις, εξαιτίας και των δύσκολων συγκυριών στα οικονομικά, θα στρέφονται σε λύσεις υπολογιστικού νέφους, καθώς το κόστος είναι χαμηλότερο από αυτό της αγοράς και της συντήρησης ιδιόκτητων εφαρμογών και λειτουργιών. Επίσης, οι οικονομίες κλίμακας οδηγούν προς τα κάτω τις δαπάνες των παρόχων νεφών. Δεδομένου ότι οι πάροχοι νέφους χτίζουν ολοένα και μεγαλύτερα κέντρα δεδομένων, απαιτούν καλύτερες τιμές από τις εταιρείες ενέργειας. Κυρίως βέβαια συνεχίζουν να χρησιμοποιούν όσο το δυνατόν περισσότερο λογισμικό ανοικτού-κώδικα και ο σκληρός ανταγωνισμός θα αναγκάσει τις τιμές να διατηρηθούν σε χαμηλά επίπεδα.

Οι πελάτες, λόγω των αυξημένων απαιτήσεών τους, αλλά και του ανταγωνισμού, θα αναγκάσουν τους παρόχους νεφών να υποσχεθούν ισχυρότερα συμφωνητικά παροχής υπηρεσιών (Service Level Agreement - SLAs) στα οποία θα πρέπει να εμμείνουν. Οι περισσότεροι πάροχοι νέφους θα διατηρούν πολλές εγκαταστάσεις, κάθε μια με την πλεονάζουσα ικανότητα να αντισταθμίσει τις παραβιάσεις υλικού ή δικτύου μετακινώντας το φόρτο εργασίας προς διαφορετικούς εξυπηρέτες ή σε εξ ολοκλήρου διαφορετικές εγκαταστάσεις.

Αναφορικά με την ασφάλεια, το νέφος διαθέτει μεγαλύτερη εξειδίκευση στον τομέα αυτό της ασφάλειας απ’ ό,τι οι παραδοσιακές μέθοδοι (μεμονωμένη ανάπτυξη από εταιρείες). Έτσι, με την πάροδο του χρόνου θα επεκταθούν ακόμη περισσότερο οι προσπάθειες που γίνονται για να καταστούν τα νέφη ασφαλέστερα. Μέχρι και τα δημόσια νέφη θα παρέχουν καλύτερη ασφάλεια δεδομένων. Καθώς η μετάδοση των δεδομένων και η αποθήκευσή τους στις εγκαταστάσεις αποθήκευσης νέφους αναμένεται να παραμένουν

κρυπτογραφημένες σε όλους τους τύπους νέφους, η ασφάλεια των δεδομένων στα κέντρα δεδομένων μη-νεφών θα βελτιωθεί δεδομένου ότι θα υιοθετηθούν οι καλύτερες πρακτικές που αρχικά δοκιμάστηκαν στα δημόσια και στα ιδιωτικά νέφη.

Τέλος, η ευκολία χρήσης του υπολογιστικού νέφους θα συνεχίσει να βελτιώνεται, όπως άλλωστε συμβαίνει και με τα περισσότερα λογισμικά με το πέρασμα του χρόνου. Αυτό θα συμβεί διότι όλα τα ανταγωνιστικά συστήματα λογισμικού τείνουν προς αυτή την κατεύθυνση και έτσι είναι σχεδόν βέβαιο ότι η χρήση του νέφους θα γίνει πολύ πιο φιλική προς τον χρήστη.

5.8.2 Αύξηση των εξυπηρετών στα κέντρα δεδομένων νέφους

Τα μεγάλα κέντρα δεδομένων νέφους προβλέπεται ότι θα περιλαμβάνουν 500.000 εξυπηρέτες, που θα κοστίζουν $1 δισεκατομμύριο μέχρι το 2020. Ένας μικρός κατάλογος από τους μεγάλους παρόχους νέφους, συμπεριλαμβανομένων των Amazon, Apple, Google, Microsoft, Oracle, IBM, ακόμα και το Facebook, αποτελούν μια κατηγορία από μόνοι τους όταν πρόκειται για το μέγεθος του κέντρου δεδομένων τους.

Όλοι αυτοί οι πάροχοι νέφους χτίζουν κέντρα δεδομένων που έχουν 50.000–100.000 εξυπηρέτες. Ένα τέτοιο κέντρο κοστίζει περίπου $53 εκατομμύρια ετησίως. Αυτό αποτελεί περίπου το 45% του συνολικού κόστους του κέντρου δεδομένων. Το 25% πηγαίνει στη διανομή ενέργειας και την ψύξη ($18 εκατομμύρια/έτος), ένα 15% είναι για το κόστος ηλεκτρικής ενέργειας ($9 εκατομμύρια/έτος) και τέλος ένα 15% είναι δαπάνες δικτύου.

5.8.3 Μειωμένο κόστος εν συγκρίσει με τα εταιρικά κέντρα δεδομένων

Το όχι μικρό κόστος των κέντρων δεδομένων των παρόχων του υπολογιστικού νέφους είναι χαμηλότερο από το κόστος των εταιρικών κέντρων δεδομένων. Αυτό συμβαίνει διότι τα κέντρα δεδομένων των παρόχων του νέφους έχουν τεράστιες

οικονομίες κλίμακας, καθώς και σημαντικές φοροαπαλλαγές και συνεχίζουν να μειώνουν τις δαπάνες τους κάθε έτος.

Επίσης, τα μεγάλα κέντρα δεδομένων νέφους υλοποιούν πολύπλοκα λογισμικά, τα οποία χρησιμεύουν ώστε να μετακινούν τον φόρτο εργασίας από μια εγκατάσταση σε κάποια άλλη σε περίπτωση αστοχίας. Προσπαθούν με αυτό τον τρόπο, καθώς και με άλλες τεχνικές να μειώσουν το επιπλέον κόστος. Τα επόμενα χρόνια το χάσμα μεταξύ των εταιρικών κέντρων αποθήκευσης δεδομένων και των παρόχων κέντρων αποθήκευσης δεδομένων σε νέφη θα συνεχίσει να διευρύνεται. Υπολογίζεται ότι μέχρι το 2020, οι δαπάνες παρόχων νέφους θα είναι λιγότερες από το 25% σε σχέση με τα εταιρικά κέντρα δεδομένων.

5.8.4 Μείωση της αναλογίας διαχειριστών προς εξυπηρέτες

Μέχρι το 2020, η αναλογία των διαχειριστών προς τους εξυπηρέτες, θα ανέλθει από 1:1.000 σε 1:10.000. Αυτό θα συμβεί διότι τα μεγάλα κέντρα δεδομένων επενδύουν ιδιαίτερα σε λογισμικό που αυτοματοποιεί τις διάφορες λειτουργίες. Ένα τυπικό εταιρικό κέντρο στοιχείων αναπτύσσει δραστηριότητες σε μια αναλογία περίπου ενός μέλους προσωπικού για κάθε 100 εξυπηρέτες, ενώ οι καλύτεροι πάροχοι νέφους αναπτύσσουν δραστηριότητες με αναλογία 1:1.000.

Τα κέντρα δεδομένων νέφους δουλεύουν τόσο αποτελεσματικά, για το λόγο ότι έπρεπε να χτίσουν υψηλά επίπεδα αυτοματισμού στη λειτουργία τους για να προσφέρουν ένα βασικό πακέτο νέφους. Ένας τρόπος με τον οποίο θα μπορέσουν να πετύχουν υψηλά επίπεδα αυτοματοποίησης, είναι με την τυποποίηση των πλατφορμών τους. Βέβαια μόνο μερικές διαφορετικές πλατφόρμες μπορούν να προμηθευτούν από την Amazon. Αλλά ένα τυπικό εταιρικό κέντρο δεδομένων, έχει έναν τεράστιο αριθμό εφαρμογών (συχνά χιλιάδες) με κυριολεκτικά εκατοντάδες διαφορετικές πιθανές ρυθμίσεις του υλικού και του λογισμικού. Η επιδείνωση αυτής της πολυπλοκότητας έχει σαν αποτέλεσμα, οι προβλέψεις για τη χρήση μοντέλων και οι κλιμακούμενες απαιτήσεις να είναι συνήθως αβέβαιες. Το τελικό αποτέλεσμα αυτής της σταθερής κίνησης για περισσότερη αυτοματοποίηση, που μισθώνει τους καλύτερους ανθρώπους και δημιουργεί

μεγαλύτερα κέντρα δεδομένων, θα οδηγήσει τους παρόχους νέφους σε μια αναλογία ενός διαχειριστή για κάθε δέκα χιλιάδες εξυπηρέτες στην επόμενη δεκαετία.

5.8.5 Η εξάπλωση του ανοικτού κώδικα

Όπως και σε αρκετούς πλέον τομείς της επιστήμης των υπολογιστών, έτσι και το νέφος του μέλλοντος, αναμφίβολα θα κυριαρχείται από συστήματα ανοικτού λογισμικού. Τα συστήματα αυτά έχουν οδηγήσει την μέχρι τώρα εξέλιξη του υπολογιστικού νέφους. Βέβαια αυτό λειτουργεί αμφίδρομα καθώς η γρήγορη πρόοδος του νέφους τροφοδοτεί και την εξέλιξη του ανοικτού λογισμικού.

Το Linux είναι το λειτουργικό σύστημα που επιλέγεται στο νέφος. Κάποιοι πάροχοι νέφους εκτελούν το ανοιχτό λογισμικό RedHat Linux. Επίσης, μια άλλη επικρατούσα επιλογή ανοικτού λογισμικού είναι το Xen το οποίο χρησιμοποιείται από χιλιάδες εξυπηρέτες της Amazon που υποστηρίζουν το EC2. Κάποιες άλλες εναλλακτικές επιλογές είναι η Microsoft και το VMware, το κόστος των οποίων δεν είναι αμελητέο.

Η δύναμη που διαθέτει το ανοιχτό λογισμικό είναι ισχυρή. Αυτό γίνεται διότι οι δαπάνες απόκτησης και χορήγησης αδειών του λογισμικού ανοικτού κώδικα, είναι 80% χαμηλότερες από τις συγκρίσιμες ιδιόκτητες προσφορές. Τέλος, το νέφος είναι ιδανικό για τους προγραμματιστές ανοικτού κώδικα, λόγω του ότι έχουν τη δυνατότητα να το χρησιμοποιήσουν για ανάπτυξη, δοκιμή και αποθήκευση με χαμηλό κόστος.

5.8.6 Η αύξηση της χρήσης SaaS από τα βασικά πρότυπα του Ιστού

Τα επόμενα χρόνια αναμένεται να αυξηθεί η χρήση του λογισμικού ως υπηρεσία (SaaS-Software as a Service) μέσω των βασικών προτύπων του ιστού. Οι επιχειρήσεις είναι πιο εύκολο να υιοθετήσουν πρότυπα SaaS, καθ' ότι το μόνο που απαιτείται για την χρήση τους είναι ένα πρόγραμμα πλοήγησης. Ακόμη, για το λογισμικό ως υπηρεσία δεν απαιτούνται πρόσθετα πρότυπα καθώς

χρησιμοποιούνται τα ίδια πρότυπα πάνω στα οποία δημιουργούνται οι βασικοί δικτυακοί τόποι και οι εφαρμογές ιστού.

Δεδομένου ότι η HTML 5 υποστηρίζεται ευρέως από τα προγράμματα πλοήγησης, οι εφαρμογές SaaS θα εκμεταλλευθούν τα χαρακτηριστικά γνωρίσματά της. Έτσι, θα προσφέρουν στους χρήστες μια πιο διαδραστική εμπειρία, εξαλείφοντας τα όποια παράπονα αυτών κατά τη μετάβασή τους στις εφαρμογές αυτές.

Επίσης, σύμφωνα με μελέτη της Gartner, το μέγεθος της αγοράς λογισμικού ως υπηρεσία (SaaS), θα ανέρχεται στα $16 δισεκατομμύρια μέχρι το 2013. Η IDC συνεχίζει στην έκθεση της ότι το ετήσιο ποσοστό αύξησης για το SaaS είναι στο 40%. Περισσότερες από 76% των αμερικανικών εταιρειών χρησιμοποιούν τουλάχιστον μια εφαρμογή SaaS. Περίπου το 45% των επιχειρήσεων ξοδεύουν τουλάχιστον 25% των προϋπολογισμών για την Τεχνολογία (IT) σε SaaS. Οι επιχειρήσεις αυτές μετατοπίζουν ήδη τους χρήστες τους στο νέφος, ακόμη και αν δεν είναι ακόμα πλήρως έτοιμες να μετατοπίσουν την υποδομή τους στο νέφος [75].

5.8.7 Η κυβερνητική πρωτοβουλία στην υιοθέτηση νεφών

Μια άλλη πολύ σημαντική παράμετρος που εξετάζεται, είναι ο ρόλος που θα διαδραματίσουν οι κυβερνήσεις στην υιοθέτηση νέφους. Το υπολογιστικό νέφος αναπτύσσει αυτήν την περίοδο μεγάλο ρόλο στην ομοσπονδιακή κυβέρνηση των ΗΠΑ, αυτό άλλωστε φανερώνει το γεγονός ότι ο προϋπολογισμός της Τεχνολογίας (IT) της Αμερικάνικης κυβέρνησης είναι $76 δισεκατομμύρια. Η NASA χρησιμοποιεί το υπολογιστικό νέφος και τα κοινωνικά μέσα για να γίνει αποδοτικότερη και να μειώσει τα κόστη. Άλλα σημαντικά κυβερνητικά έργα νέφους περιλαμβάνουν τον στρατό της Αμερικής, το υπουργείο οικονομικών και πολλά άλλα.

Στα πλάισια της Ελλάδας, έχει παρουσιαστεί ο «οδικός χάρτης» για την υιοθέτηση και υλοποίηση του κυβερνητικού cloud. Ο κ. Μαρκόπουλος (2011), αναφέρθηκε κατ' αρχήν στην κατάσταση που υπάρχει στον δημόσιο τομέα όσον αφορά τις τεχνολογικές υποδομές. Όπως ανέφερε χαρακτηριστικά: "Δυόμισι

δισεκατομμύρια ευρώ, περίπου το ένα τρίτο των δαπανών του προγράμματος Κοινωνία της Πληροφορίας καταναλώθηκε σε hardware και μάλιστα σε πολλαπλές νησίδες. Κάθε δήμος, κάθε μουσείο, κάθε περιφέρεια, κάθε νομαρχία έχει ένα computer room. Ο περισσότερος εξοπλισμός μάλιστα υποχρησιμοποιείται. Τα επίπεδα χρήσης για τους servers φτάνουν στο 3-5%. Προφανώς υπάρχει έλλειψη διαλειτουργικότητας, τόσο σε επίπεδο διαμοίρασης πόρων όσο και σε επίπεδο λογισμικού". Για την διόρθωση της κατάστασης αυτής, η υιοθέτηση του κυβερνητικού cloud αναφέρθηκε ως η ενδεδειγμένη λύση.

Ο σχεδιασμός για το κυβερνητικό cloud περιλαμβάνει:

- Δημιουργία 2-3 μεγάλων κέντρων δεδομένων της δημόσιας διοίκησης. Το πρώτο αφορά το χώρο της οικονομίας και των οικονομικών και θα βρίσκεται στη Γενική Γραμματεία Πληροφοριακών Συστημάτων. Το δεύτερο αφορά το χώρο της Παιδείας, των εκπαιδευτικών Ιδρυμάτων και των Πανεπιστημίων και βρίσκεται στο ΕΔΕΤ. Το τρίτο θα αφορά τη δημόσια διοίκηση εν γένει και θα τρέχει από την ΚτΠ ΑΕ. Ήδη τα δύο εξ' αυτών έχουν εγκριθεί. Η δημιουργία των πρώτων κέντρων δεδομένων θα ξεκινούσε στις αρχές του 2012.
- Δημιουργία ενός disaster recovery site. Απαραίτητο για την μη απώλεια των δεδομένων.
- Μετά από την κατασκευή των κέντρων δεδομένων θα αρχίσει η προσθήκη εφαρμογών των φορέων που υλοποιούν δημόσιες οι υπηρεσίες.
- Θα εξασφαλιστεί η λειτουργική υποστήριξη των δημόσιων κέντρων δεδομένων, κάτι το οποίο θα μπορούσε να είναι και στην ευθύνη του ιδιωτικού τομέα.
- Η διαδικασία θα ξεκινήσει με τη λογική του Infrastructure as a Service και τη δημιουργία εικονικών μηχανών πάνω στις οποίες θα «κάθονται» οι δημόσιες υπηρεσίες.
- Διασύνδεση των δημόσιων κέντρων δεδομένων ώστε να επιτευχθεί η δυναμική μεταφορά πόρων αλλά και η διασύνδεση με τα υπόλοιπα κέντρα δεδομένων και computer rooms του δημόσιου.

- Σε συνεργασία με τους πιο ώριμους φορείς θα προχωρήσει και η υλοποίηση platform as a service υπηρεσιών αλλά και η υλοποίηση του «λογισμικού ως υπηρεσία».

Επιπλέον, λόγω του ότι ιστορικά η κυβέρνηση δεν υπήρξε ποτέ ηγέτης στη χρήση της τεχνολογίας πληροφοριών, αυτή τη φορά τα πράγματα δείχνουν διαφορετικά. Οι επιχειρήσεις θα βρεθούν στην ασυνήθιστη θέση να προσπαθούν να προλάβουν τις εξελίξεις που παρουσιάζουν οι κυβερνητικοί οργανισμοί στο τομέα αυτό, μετά και την παρακίνηση του κράτους στον ιδιωτικό τομέα ώστε να συμβάλλει προς την κατεύθυνση του cloud [73] .

Κεφάλαιο 6
Επίλογος

Συμπεράσματα

Σύμφωνα με τα όσα αναλύθηκαν παραπάνω και θα διαπίστωσε ο αναγνώστης, το υπολογιστικό νέφος αποτελεί μια νέα τεχνολογία με πολλές υποσχέσεις αλλά και τους ειδικούς να μην μπορούν να κρύψουν τις επιφυλάξεις τους. Από την μια μεριά υπάρχουν οι κίνδυνοι και από την άλλη τα πλεονεκτήματα που προσφέρει το υπολογιστικό νέφος, που ωστόσο είναι σημαντικά. Αποτελεί εξέλιξη των σημερινών δικτύων και υπόσχεται πολύ σοβαρές αλλαγές που θα λύσει τα χέρια επιχειρήσεων, οργανισμών, εταιρειών, αλλά και ιδιωτών. Κάποια από τα οφέλη είναι η αποτελεσματικότητα σε σχέση με το κόστος. Παραδοσιακά, οι εταιρίες και οι δημόσιοι οργανισμοί επενδύουν πολλά χρήματα στην δημιουργία των υποδομών πληροφορικής, πληρώνοντας διακομιστές, λογισμικά και άδειες χρήσεως για πολλαπλούς χρήστες. Την ίδια στιγμή, το υπολογιστικό νέφος προσφέρει υπηρεσίες σε πολύ φθηνότερες τιμές, μειώνει την ανάγκη για επενδύσεις στην συντήρηση και κάνει αναβαθμίσεις μιας και αυτές είναι οι βασικές λειτουργίες του Παρόχου Υπολογιστικού Νέφους. Επίσης, η γρήγορη ανάπτυξη και κλιμάκωση, όταν μία εταιρία αποφασίσει να λειτουργήσει βασιζόμενη στο υπολογιστικό νέφος, μπορεί να αναπτύξει το σύστημά της και να το κάνει πλήρως λειτουργικό μέσα σε μερικά λεπτά. Τα αντίγραφα ασφαλείας και η αποκατάσταση δεδομένων, η ανταγωνιστικότητα, η ευκολία στην εκμάθηση και η φιλικότητα προς το περιβάλλον, μιας και οι πόροι χρησιμοποιούνται όταν είναι απαραίτητο, είναι μερικά ακόμη οφέλη.

Η ασφάλεια και η προστασία δεδομένων ίσως αποτελούν τις δυο μεγαλύτερες προκλήσεις σχετικά με το υπολογιστικό νέφος και ταυτόχρονα δύο από τους σημαντικότερους λόγους για τους οποίους δεν υιοθετείται άμεσα. Εφόσον τα δεδομένα μιας εταιρίας ή ενός δημόσιου οργανισμού αποθηκεύονται στο νέφος, διασκορπίζονται σε διάφορες τοποθεσίες. Ο χρήστης του υπολογιστικού νέφους

παραχωρεί δεδομένα και πληροφορίες, οι οποίες είναι ενδεχομένως προσωπικές, ευαίσθητες και απόρρητες. Ο πάροχος του νέφους είναι υπεύθυνος για την συντήρηση και την προστασία των δεδομένων αυτών και γι' αυτό πρέπει να είναι αξιόπιστος. Στην περίπτωση των κυβερνητικών οργανισμών η αποθήκευση των δεδομένων τους εκτός συνόρων συνήθως απαγορεύεται διά νόμου. Το υβριδικό νέφος μπορεί να χρησιμοποιηθεί ως αντίμετρο για την αποθήκευση των ευαίσθητων δεδομένων στο κέντρο δεδομένων του ίδιου του καταναλωτή και στο οποίο επιτρέπεται η πρόσβαση. Φυσικά οι μηχανισμοί ασφαλείας ανάμεσα στον πάροχο του νέφους και στον καταναλωτή θα πρέπει να είναι ισχυροί και προσεκτικά σχεδιασμένοι.

Η εύρεση και η υλοποίηση μιας αποτελεσματικής στρατηγικής που θα καλύπτει όλα αυτά τα ζητήματα, θα βοηθήσει τις εταιρείες να κατακτήσουν τον απόλυτο στόχο: να κάνουν δηλαδή τις υπηρεσίες νέφους να λειτουργούν όπως το δικό τους τμήμα ασφάλειας IT και να βρουν τρόπους να διασφαλίσουν και να μεγιστοποιήσουν τις επενδύσεις τους στο νέφος.

Μία προσέγγιση βάσει προτύπων θα καταστήσει ευκολότερη την υποστήριξη ευελιξίας από την πλευρά των παρόχων, καθώς και την παροχή διευρυμένων υπηρεσιών νέφους, ενώ θα είναι πιο εύκολο για τις εταιρείες να αξιολογήσουν τους παρόχους και να εμπιστευτούν τις υποσχέσεις τους για ασφάλεια και μυστικότητα.

Σε εποχές όπου η οικονομία δοκιμάζεται, όπως και η σημερινή άλλωστε, φαίνεται ότι η επιλογή χρήσης τεχνολογιών υπολογιστικού νέφους μπορεί να εξοικονομήσει αρκετά χρήματα στον κρατικό προϋπολογισμό. Αυτό όμως δεν είναι κάτι που θα αποτρέψει την συνέχιση της προσεκτικής εκτίμησης κόστους/οφέλους και της σχετικής άσκησης έρευνας αναφορικά με την διαχείριση κίνδυνων.

Λεξικό Αγγλικών Όρων

API (Application Programming Interface): Διεπαφή προγραμματισμού εφαρμογών

Authorization: Εξουσιοδότηση

Bandwidth: Εύρος ζώνης

CAPEX (Capital Expenditure): Κεφαλαιουχικές δαπάνες

CIOs (Chief Information Officers): Προϊστάμενοι Πληροφοριακών Συστημάτων

Cloud Bursting: Έκρηξη νέφους

Cloud computing: Υπολογιστικό νέφος

Cloud Validation Assessment: Επικύρωση αξιολόγησης νέφους

Community cloud: Νέφος κοινότητας

Content Delivery Network: Δίκτυο παράδοσης περιεχομένου

CPU (Central Processing Unit): Κεντρική μονάδα επεξεργασίας

CSP (Content Service Provider): Περιεχόμενο υπηρεσίας παρόχου

CSPs (Center for Security Policy): Κέντρο για την πολιτική ασφαλείας

Data Store: Αποθήκη δεδομένων

DNS (Domain Name System): Σύστημα ονομάτων τομέα

Elasticity: Ελαστικότητα

Hardware: Υλικό

HTTP (Hypertext Transfer Protocol): Πρωτόκκολο μεταφοράς υπερκειμένου

Hybrid cloud: Υβριδικό νέφος

Hypervisor: Επόπτης

IaaS (Infracture as a Service): Υποδομή ως υπηρεσία

IDC (International Data Corporation): Διεθνείς εταιρεία δεδομένων

IDM (Identity Management): Διαχείριση ταυτότητας

Internet: Διαδίκτυο

IT (Information Technology): Τεχνολογία πληροφοριών

LAN (Local Area Network): Τοπικό δίκτυο υπολογιστών

MIT (Massachusetts Institute of Technology): Τεχνολογικό Ινστιτούτο Μασαχουσέτης

Multiple lease: Πολλαπλή μίσθωση

Multitenancy: Πολυμίσθωση

MVNO (Mobile Virtual Network Operator): Φορέας εικονικού δικτύου κινητής

NaaS (Network as a Service): Δίκτυο ως υπηρεσία

NAT (Network Address Translation): Μετάφραση διευθύνσεων δικτύου

NFV (Network Functions Virtualization): Λειτουργίες εικονοποίησης δικτύου

NIST (National Institute of Standards and Technology): Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας

OPEX (Operational Expenditure): Λειτουργικές δαπάνες

OS (Operating System): Λειτουργικό σύστημα

PaaS (Platform as a Service): Πλατφόρμα ως υπηρεσία

Private cloud: Ιδιωτικό νέφος

Public cloud: Δημόσιο νέφος

RBAC (Role-Based Access Control): Έλεγχος πρόσβασης βάση ρόλου

Router: Δρομολογητής

S3 (Simple Storage Service): Υπηρεσία απλής αποθήκευσης

SaaS (Software as a Service): Λογισμικό ως υπηρεσία

SAML (Security Assertion Markup Language): Γλώσσα ασφαλείας

Server: Διακομιστής

SLA (Service Level Agreement): Συμφωνία σε επίπεδο υπηρεσιών

SOA (Service Oriented Architecture): Υπηρεσίες προσανατολισμένες στην αρχιτεκτονική

SSL (Secure Socket Layer): Ασφαλές στρώμα υποδοχής

Synchronization: Συγχρονισμός

Virtualization: Εικονοποίηση

VM (Virtual Machine): Εικονική μηχανή

VMM (Virtual Machine Monitor): Επόπτης εικονικής μηχανής

VPN (Virtual Private Network): Εικονικό ιδιωτικό δίκτυο

WAN (Wide Area Network): Δίκτυο ευρείας περιοχής

Web browser: Δικτυακός περιηγητής

WS (Web Service Security): Ασφάλεια διαδικτυακών υπηρεσιών

XACML (Extensible Access Control Markup Language): Γλώσσα επεκτάσικου ελέγχου πρόσβασης

XML (Extendable Markup Language): Επεκτάσιμη γλώσσα σήμανσης

Βιβλιογραφία

[1] "What is Cloud Computing?". *Amazon Web Services*. 2013-03-19. Retrieved 2013-03-20.

[2] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.

[3] Ádám Kapovits (14 June 2011). "The role of virtualisation in future network architectures". Retrieved 16 September 2013.

[4] Artz D, Gil Y (2007) A survey of trust in computer science and the Semantic Web. Web Semantics: Science, Services and Agents on the World Wide Web, 5:58–71.

[5] Ashish Sarin, Portlets in Action, Manning Publications Co., pp. 640, September, 2011.

[6] Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," infoTECH, August 24, 2011". It.tmcnet.com. 2011-08-24. Retrieved 2011-12-02.

[7] Barrie Sosinsky, Cloud Computing Bible, Wiley Publishing, 2011.

[8] Brodkin, J.: Gartner: Seven cloud-computing security risks. In: Infoworld 2008 (2008),http://www.infoworld.com/d/security-central/gartner-sevencloudcomputing- security-risks-53?page=0,1

[9] Cloud Industry Forum (2011) Cloud UK: Adoption and Trends 2011.

[10] Cloud Industry Forum (2011) Cloud UK: Adoption and Trends 2011.

[11] Cloud Security Alliance (2010) Top Threats to Cloud Computing. v1.0, March.

[12] Costa, Paulo; Migliavacca, Matteo; Pietzuch, Peter; Wolf, Alexander. "NaaS: Network-as-a-Service in the Cloud". Imperial College London. Retrieved 16 December 2012.

[13] CSA (2012) Cloud Trust Protocol.

[14] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009, [Online], Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, [Accessed: 08-July-2011].

[15] Dan Sullivan (2014-01-14). "Cost of the Cloud: A Developer's Guide to Reducing Your AWS Bill". Retrieved 2014-11-27.

[16] E., Mathisen, “Security challenges and solutions in cloud computing,” in Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, 2011, pp. 208-212.

[17] Edwards, J. (2009). Cutting through the fog of cloud security. Computerworld. Framingham: Feb 23, 2009. Vol. 43, Iss. 8; pg. 26, 3 pgs.

[18] Edwards, J. (2010). Defending the cloud - and your business. Webhostingunleashed.com. Retrieved on March 9, 2010 from http://www.webhostingunleashed.com/features/defendingcloud-090208/

[19] European Commission (2011) Attitudes on Data Protection and Electronic Identity in the European Union. June. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[20] Forrester Research, Inc (2011) Ignoring Cloud Risks: A Growing Gap between I&O and the Business. March.

[21] Fujitsu Research Institute (2010) Personal data in the cloud: A global survey of consumer attitudes. http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personaldata-in-the-cloud.pdf

[22] Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley; 2005:227–229.

[23] Gautam Shroff, Enterprise Cloud Computing: Technology, Architecture, Applications, Cambridge University Press, 2010.

[24] George Reese, Cloud Application Architectures, O’Reilly, 2009.

[25] George Reese, Cloud Application Architectures, O’Reilly, 2009.

[26] Global Netoptex Incorporated. “Demystifying the cloud. Important opportunities, crucial choices.” pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[27] Greene, T. (2009). New attacks on cloud services call for due diligence. Network World. Southborough: Sep 14, 2009. Vol. 26, Iss. 28; pg. 8, 1 pgs. Retrieved from http://www.networkworld.com/newsletters/vpn/2009/090709cloudsec2.html

[28] Hashizume K, Yoshioka N, Fernandez EB: Three misuse patterns for Cloud Computing. In Security engineering for Cloud Computing: approaches and Tools.

Edited by: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M. Pennsylvania, United States: IGI Global; 2013:36–53.

[29] Hoover, J. N. (2008, August 16). Outages force cloud computing user to rethink tactics. InformationWeek. Retrieved on March 26, 2010 from http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=210004236

[30] Horrigan JB (2008) Use of cloud computing applications and services. Pew Internet & American Life project memo, Sept.

http://www.sdncentral.com/whats-network-functions-virtualization-nfv/

[31] IDC (2009) Enterprise Panel, September. http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate

[32] IDC (2010) Cloud Computing Attitudes, Survey, Doc.#223077.

[33] Information Security Magazine. 2009. The three cloud computing risks to consider. Issue: June 2009. Retrieved from http://www.arma.org/press/ARMAnews/Infosecurity.pdf

[34] Jaeger P, Lin J, Grimes J (2008) Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology & Politics, 5.

[35] Jasti A, Shah P, Nagaraj R, Pendse R: Security in multi-tenancy cloud. In IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. Washington, DC, USA: IEEE Computer Society; 2010:35–41.

[36] Jasti A, Shah P, Nagaraj R, Pendse R: Security in multi-tenancy cloud. In IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. Washington, DC, USA: IEEE Computer Society; 2010:35–41.

[37] Jericho Forum - Position Paper, Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, April 2009.

[38] Jothy Rosenberg and Arthur Mateos, The Cloud at your Service – The when, how, and why of enterprise cloud computing, Manning Publications Co., 2011.

[39] Karthick Ramachandran, Thomas Margoni and Mark Perry, “Clarifying Privacy in the Clouds” in CYBERLAWS 2011 : The Second International Conference on Technical and Legal Aspects of the e-Society, IARIA,2011.

[40] Kaur, P., Kaushal, S.: Security concerns in cloud computing. In: Accepted For International Conference on High Performance Architecture And Grid Computing-2011. Chitkara University, Rajpura (2011)

[41] Kobielus, J. (2009). Storm clouds ahead. Network World. Southborough: Mar 2, 2009. Vol. 26, Iss. 9; pag. 24, 3

[42] Kristin Bent (22 August 2013). "Aryaka Lifts Curtain On Cloud Network-As-A-Service Offering". *CRN*. Retrieved 16 September 2013.

[43] Lamia Youseff, Maria Butrico, Dilma Da Silva, Toward a Unified Ontology of Cloud Computing, GCE, 2008.

[44] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." *IEEE Xplore*, pp 23-31, Jun. 2009.

[45] Maches, B. (2010, January 25). The Impact of cloud computing on corporate IT governance. HBCWire.com. Retrieved on March 4, 2010 from http://www.hpcwire.com/specialfeatures/cloud_computing/features/The-Impact-of-Cloud-Computing-on-Corporate-IT-Governance-82623252.html

[46] Mariana Carroll, Paula Kotzé, Alta van der Merwe (2012). "Securing Virtual and Cloud Environments". In I. Ivanov et al. *Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy*. Springer Science+Business Media. doi:10.1007/978-1-4614-2326-3

[47] Markoff, J. Barboza, D. (2010, February 18), 2 China Schools Said to Be Tied to Online Attacks. Retrieved from http://www.nytimes.com/2010/02/19/technology/19china.html

[48] Marsh S (1994). Formalising Trust as a Computational Concept. Doctoral dissertation, University of Stirling.

[49] Mell P, Grance T (2009) A NIST definition of cloud computing. National Institute of Standards and Technology. NIST SP 800-145. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[50] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, "Above the Clouds: A Berkley View on Cloud Computing", Electrical Engineering and Computer Sciences University of California at Berkeley, 2009

[51] Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.

[52] NIST, "*NIST.gov - Computer Security Division - Computer Security Resource Center*". DOI=http://csrc.nist.gov/groups/SNS/cloud-computing/.

[53] Oestreich, Ken, (2010-11-15). "Converged Infrastructure". *CTO Forum*. Thectoforum.com. Retrieved 2011-12-02.

[54] Perez, S. (2009). The Cloud Isn't Safe?! (Or Did Black Hat Just Scare Us?). August 5, 2009.ReadWriteWeb. Retrieved from http://www.readwriteweb.com/archives/the_cloud_isnt_safe_or_did_blackhat_just_scare_us.php

[55] Peter Mell και Tim Grance, The NIST Definition of Cloud Computing, NIST, September 2011.

[56] R., Trope, C., Ray, "The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges ", [Online], Available: http://ftp.documation.com/references/ABA10a/PDfs/3_1.pdf, 2009, [Accessed: 15-Jul-2011].

[57] Ramgovind, S., Eloff, M.M., Smith, E.: The management of security in cloud computing. In: The Proceedings of IEEE Conference on Information Security for South Africa-2010 (2010)

[58] Reuben JS: A survey on virtual machine Security. Seminar on Network Security; 2007. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007

[59] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." *KM World*, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[60] S. Farrell, "Portable Storage and Data Loss," Internet Computing, IEEE, vol. 12, no. 3, pp. 90-93, 2008.

[61] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul., 2010.

[62] Smith, R. (2009). Computing in the cloud. Research Technology Management, 52(5), 65- 68. Retrieved March 17, 2010, from ABI/INFORM Global. (Document ID: 1864072981).

[63] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Application, 1–11 (2010)

[64] Takabi, H., Joshi, J.B.D.: Security and privacy challenges in cloud computing environment. IEEE Journal on Security and Privacy 8(6) (November 2010)

[65] Talbot, D. (2009). Vulnerability seen in Amazon's cloud-computing. Technology Review. Friday, October 23, 2009. Retrieved on March 4, 2010 from http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf

[66] The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[67] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "*Cloud Security and Privacy*", s.l. ; O'Reilly, 2009.

[68] Tweney A, Crane S. (2007) Trustguide2: An exploration of privacy preferences in an online world. Expanding the Knowledge Economy, IOS Press.

[69] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) (2001) Title V, s 505.

[70] Uusitalo I, Karppinen K, Arto J, Savola R (2010) Trust and Cloud Services - An Interview Study. In: Proc. CloudCom 2010, IEEE.

[71] Wei Chen, Hongyi Lu, Li Shen, Zhiying Wang, Nong Xiao, and Dan Chen, "A Novel Hardware Assisted Full Virtualization Technique," in Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for, 2008, pp. 1292-1297.

[72] Kandukuri, Paturi, and Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing Bangalore, India, Sep. 21-25, 2009, pp. 517- 520.

[73] Μαρκόπουλος Α (2011) Έτσι θα εισάγουμε το cloud computing στο δημόσιο. Διαθέσιμο στο: http://www.neo2.gr/web/neo2.gr/home2/-/asset_publisher/78mX/content/%CE%B1-%CE%BC%CE%B1%CF%81%CE%BA%CE%BF%CF%80%CE%BF%CF%85%CE%BB%CE%BF%CF%82:-%CE%B5%CF%84%CF%83%CE%B9-%CE%B8%CE%B1-%CE%B5%CE%B9%CF%83%CE%B1%CE%B3%CE%BF%CF%85%CE%BC%CE%B5-%CF%84%CE%BF-cloud-computing-%CF%83%CF%84%CE%BF-%CE%B4%CE%B7%CE%BC%CE%BF%CF%83%CE%B9%CE%BF?redirect=%2Fweb%2Fneo2.gr%2Fwelcome

[75] Μελέτη της Gartner , Διαθέσιμο στο: διαθέσιμη http://www.gartner.com/technology/home.jsp