ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Τμήμα Μηχανικών Η/Υ, Τηλεπικοινωνιών και Δικτύων

Διπλωματική Εργασία του φοιτητή:

Ευθυμιάδη Δημητρίου

Με τίτλο:

«Μελέτη του πλαισίου της Νεφοϋπολογιστικής»

Επιβλέποντες καθηγητές:

Μποζάνης Παναγιώτης

Κατσαρός Δημήτριος

Βόλος 2011

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή και πρόεδρο του τμήματος Μηχανικών Η/Υ, Τηλεπικοινωνιών και Δικτύων, κ. Μποζάνη Παναγιώτη για την καθοδήγησή του κατά τη διάρκεια της εκπόνησης της Διπλωματικής μου Εργασίας, καθώς και για το σύνολο της διάρκειας των σπουδών μου. Επίσης, θα ήθελα να ευχαριστήσω θερμά την οικογένεια και τους φίλους μου για την υποστήριξη και την βοήθεια τους σε όλο αυτό το διάστημα.

Περιεχόμενα

Κεφάλαιο 4 Υπηρεσίες Cloud Computing

Κεφάλαιο 5 Χαρακτηριστικά Cloud Computing

Κεφάλαιο 6 Αδυναμίες του Cloud Computing

Κεφάλαιο 1

Εισαγωγή

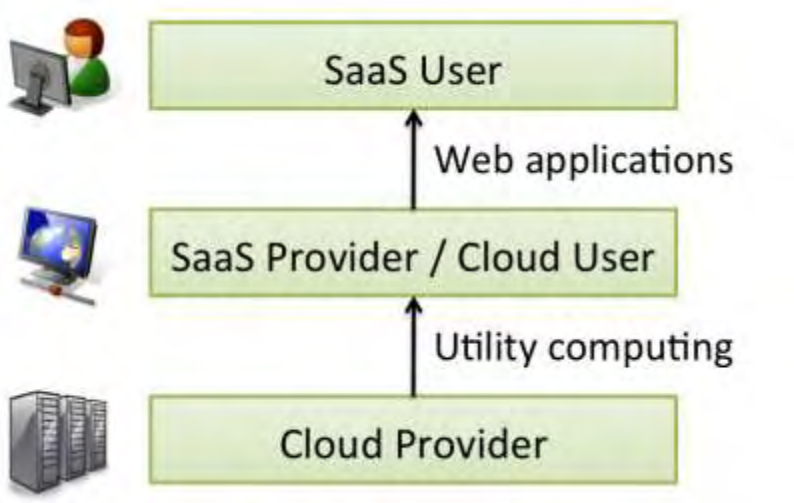
Περιεχόμενα

1.1 Εισαγωγικά στοιχεία

Το cloud computing[1] είναι το επόμενο στάδιο στην εξέλιξη του internet. Παρέχει τα μέσα από τα οποία τα πάντα παραδίδονται στον χρήστη ως μια υπηρεσία , όπου και όποτε αυτή χρειαστεί. Το cloud computing αναφέρεται τόσο στις εφαρμογές που παραδίδονται ως υπηρεσίες πάνω από το διαδίκτυο, όσο και στο υλικό και το λογισμικό των συστημάτων στα κέντρα δεδομένων (data centers) τα οποία παρέχουν αυτές τις υπηρεσίες. Οι υπηρεσίες , αυτές κάθε αυτές αναφέρονται ως Λογισμικό ως Υπηρεσία (Software as a Service - SaaS). Το υλικό καθώς και το λογισμικό του κέντρου δεδομένων (data center) αποτελεί αυτό που αποκαλούμε "νέφος" (cloud). Όταν ένα cloud είναι διαθέσιμο στο ευρύ κοινό με έναν pay-as-you-go τρόπο, αποκαλείται "δημόσιο νέφος" (public cloud), ενώ η υπηρεσία που πωλείται είναι Utility Computing. Με τον όρο "ιδιωτικό νέφος" (private cloud) αναφερόμαστε στα εσωτερικά κέντρα δεδομένων μιας επιχείρησης η κάποιου άλλου οργανισμού , τα οποία δεν γίνονται διαθέσιμα στο ευρύ κοινό.

Από την πλευρά του υλικού, υπάρχουν 3 διαφορετικές απόψεις καινούριες στο Cloud Computing:

- Η ψευδαίσθηση της ύπαρξης άπειρων υπολογιστικών πόρων που είναι διαθέσιμοι κατ'απαίτηση, κάτι που επιτρέπει στους χρήστες του cloud computing να σταματήσουν τον σχεδιασμό μακροχρόνιων προβλέψεων.
- Η εξάλειψη της εκ των προτέρων δέσμευσης των χρηστών του Cloud, κάτι που επιτρέπει στις εταιρίες να αυξάνουν τους υλικούς πόρους μόνο όταν αυξηθούν οι ανάγκες τους.
- Η δυνατότητα πληρωμής των πόρων που χρησιμοποιούνται σε βραχυπρόθεσμη βάση, (επεξεργαστές ανά ώρα και αποθηκευτικά μέσα ανά μέρα) και η αποδέσμευσή τους όταν δεν είναι πλέον απαραίτητοι.



Εικόνα 1.1 : Χρήστες και Πάροχοι του Cloud Computing [1]

1.2 Απλοϊκή Δομή του Cloud Computing

Το Cloud Computing μπορεί να οπτικοποιηθεί ως μια πυραμίδα[2] αποτελούμενη από 3 τμήματα:

Η Cloud Εφαρμογή :

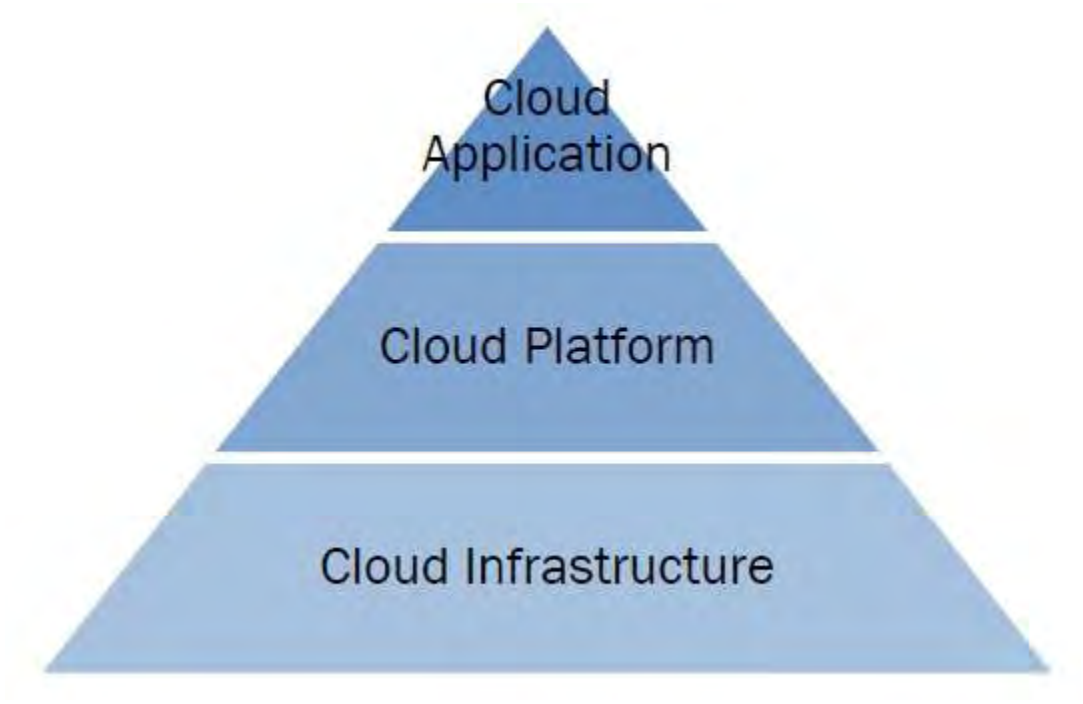
Είναι η κορυφή της πυραμίδας, όπου οι εφαρμογές εκτελούνται και αλληλεπιδρούν μέσω ενός web browser, hosted desktop ή απομακρυσμένο πελάτη. Το σήμα κατατεθέν των εμπορικού εφαρμογών cloud computing, είναι ότι οι χρήστες δεν θα χρειαστεί ποτέ να αγοράσουν ακριβές άδειες χρήσεις για αυτές, αντίθετα το κόστος ενσωματώνεται στη συνδρομή. Ακόμη, μια εφαρμογή cloud δεν απαιτεί την εγκατάσταση και εκτέλεση της στον προσωπικό υπολογιστή του κάθε χρήστη, αφαιρώντας έτσι το επιπρόσθετο βάρος της συντήρησης λογισμικού, της διαρκούς λειτουργίας του και της τεχνικής υποστήριξης.

Η Cloud Πλατφόρμα:

Είναι το μεσαίο επίπεδο της πυραμίδας, το οποίο παρέχει μια υπολογιστική πλατφόρμα ή ένα πλαίσιο (framework) ως μια υπηρεσία. Μια πλατφόρμα cloud computing δεσμεύει δυναμικά , ρυθμίζει τις παραμέτρους, αναδιαμορφώνει και αποδεσμεύει εξυπηρετητές όπως απαιτείται έτσι ώστε να μπορούν να ανταπεξέλθουν ανάλογα με αυξήσεις ή μειώσεις στη ζήτηση. Στην πραγματικότητα κάτι τέτοιο αποτελεί ένα μοντέλο κατανεμημένου υπολογισμού, όπου πολλές οι υπηρεσίες συνεργάζονται για να ανταποκριθούν σε κάποιο αίτημα εφαρμογής ή υποδομής.

Η Υποδομή του Cloud :

Είναι το θεμέλιο της πυραμίδας το οποίο παρέχει υποδομές μέσω εικονοποίησης. Η εικονοποίηση επιτρέπει τον διαχωρισμό μιας ξεχωριστής αυτόνομης οντότητας υλικού σε ανεξάρτητα, αυτόνομα περιβάλλοντα τα οποία μπορούν να ιεραρχηθούν σε CPU,RAM, δίσκους και άλλα στοιχεία. Η υποδομή περιλαμβάνει εξυπηρετητές, δίκτυα καθώς και διάφορες άλλες συσκευές υλικού οι οποίες παραδίδονται είτε ως “Web Services”, “farms” ή "cloud centers". Όλα αυτά τα στοιχεία είναι διασυνδεδεμένα με άλλα για ανθεκτικότητα και επιπρόσθετη χωρητικότητα.



Εικόνα 1.2 : Η απλοϊκή δομή του Cloud Computing. [2]

1.3 Υπηρεσίες που χρησιμοποιούν το Cloud

Υπάρχουν πολλές υπηρεσίες[3] που μπορούν να παραδοθούν μέσω του Cloud Computing, εκμεταλλευόμενες το κατανεμημένο μοντέλο του cloud:

Hosted Desktops:

Τα Hosted Desktops απομακρύνουν την ανάγκη ύπαρξης παραδοσιακών desktop PC σε ένα περιβάλλον γραφείου. Ένα hosted desktop δείχνει και συμπεριφέρεται όπως ένα συμβατικό desktop PC, αλλά το λογισμικό και τα δεδομένα που χρησιμοποιούν οι χρήστες στεγάζονται σε ένα απομακρυσμένο, υψηλής ασφαλείας κέντρο δεδομένων (data center) και όχι στον δικό τους υπολογιστή. Οι χρήστες μπορούν απλά να έχουν πρόσβαση στα hosted desktops τους μέσω μιας σύνδεσης στο διαδίκτυο από οποιοδήποτε μέρος του κόσμου , χρησιμοποιώντας είτε ένα PC ή laptop, ή για τη μέγιστη αποδοτικότητα μια εξειδικευμένη συσκευή όπως ένας thin client.

Hosted Email:

Καθώς όλο και περισσότεροι οργανισμοί αναζητούν μια ασφαλή και αξιόπιστη λύση για τη διαχείριση των emails η οποία δεν θα έχει υπερβολικό κόστος, στρέφονται όλο και περισσότερο στην λύση του Microsoft Exchange® . Αυτή η υπηρεσία επιτρέπει στους οργανισμούς, είτε μεγάλης είτε μικρής κλίμακας, να απολαμβάνουν τα οφέλη της χρήσης λογαριασμών MS Exchange® χωρίς να πρέπει οι ίδιοι να επενδύσουν σε δαπανηρές εγκαταστάσεις. Τα Email αποθηκεύονται κεντρικά σε εξυπηρετητές παρέχοντας γρήγορη πρόσβαση από οποιοδήποτε μέρος. Αυτό επιτρέπει στους χρήστες να έχουν πρόσβαση σε email, ημερολόγιο, επαφές και διαμοιραζόμενα αρχεία χρησιμοποιώντας πληθώρα μέσων όπως το Outlook®, Outlook Mobile Access (OMA) και Outlook Web Access (OWA).

Hosted Telephony (VOIP):

Το VOIP (Voice Over IP) είναι ένα μέσο μεταφοράς τηλεφωνικών κλήσεων και υπηρεσιών διά μέσου ψηφιακών δικτύων. Το VOIP δεν διαφέρει και τόσο από την παραδοσιακή τηλεφωνία, καθώς ένα τηλέφωνο που χρησιμοποιεί VOIP λειτουργεί όπως ακριβώς ένα συμβατικό, έχοντας όμως σαφή πλεονεκτήματα σχετικά με το κόστος. Ένα hosted VOIP σύστημα αντικαθιστά τις δαπανηρές τηλεφωνικές εγκαταστάσεις με ένα απλό και αποδοτικό εναλλακτικό μέσο το οποίο είναι διαθέσιμο μέσω μιας μηνιαίας συνδρομής.

Cloud Storage:

Το Cloud Storage κερδίζει έδαφος λόγω των πλεονεκτημάτων που παρέχει, όπως το χαμηλό κόστος επένδυσης, την πρόσβαση από οπουδήποτε αλλά και την μη απαραίτητη διαχείριση και συντήρηση από τον ίδιο τον χρήστη. Στην ουσία είναι η παράδοση της αποθήκευσης δεδομένων ως υπηρεσία, από κάποιον τρίτο πάροχο υπηρεσιών, με πρόσβαση

μέσω διαδικτύου και χρέωση ανάλογα με την χωρητικότητα που χρησιμοποιήθηκε σε ένα ορισμένο εκ των προτέρων χρονικό διάστημα (πχ. ένας μήνας).

Dynamic Servers:

Οι Dynamic Servers είναι η νέα γενιά του περιβάλλοντος των εξυπηρετητών, αντικαθιστώντας τους συμβατικούς dedicated εξυπηρετητές. Ένας πάροχος της συγκεκριμένης υπηρεσίας δίνει στους χρήστες της πρόσβαση σε πόρους που δίνουν την αίσθηση ενός dedicated εξυπηρετητή ενώ ταυτόχρονα παραμένουν πλήρως επεκτάσιμοι. Ο χρήστης μπορεί να ελέγξει άμεσα την επεξεργαστική ισχύ και τον χώρο που χρησιμοποιεί, κάτι που σημαίνει ότι δεν χρειάζεται να πληρώσει για υλικό το οποίο δεν χρησιμοποιεί.

1.4 Γιατί Cloud Computing?

Υπάρχουν πολλοί λόγοι που όλο και περισσότεροι οργανισμοί, ανεξαρτήτου κλίμακας, υιοθετούν το μοντέλο του cloud computing, εγκαταλείποντας το παραδοσιακό client-server μοντέλο. Το cloud computing παρέχει έναν τρόπο αύξησης της χωρητικότητας , της διεκπαιρεωτικής ικανότητας ή την πρόσθεση νέων λειτουργιών και δυνατοτήτων "on the fly" χωρίς την απαίτηση νέων επενδύσεων σε υποδομές, εκπαίδευση προσωπικού ή εξασφάλιση της απαραίτητης άδειας για τη χρήση ενός νέου λογισμικού. Σε γενικές γραμμές μπορεί να βοηθήσει τις εταιρίες-οργανισμούς να εξοικονομήσουν ένα αξιοσημείωτο ποσό χρημάτων.

Αφαίρεση/Μείωση κεφαλαιουχικών δαπανών:

Οι πελάτες μπορούν να εξοικονομήσουν μεγάλο ποσοστό κεφαλαίων ακολουθώντας το μοντέλο του cloud computing . Οι κεφαλαιουχικές δαπάνες σε προϊόντα IT μειώνουν το διαθέσιμο κεφάλαιο για σημαντικές λειτουργίες και επενδύσεις. Το cloud computing προσφέρει ένα απλό υπηρεσιακό κόστος το οποίο είναι ευκολότερο να προϋπολογιστεί από μήνα σε μήνα και αποτρέπει τη σπατάλη χρημάτων σε περιουσιακά στοιχεία των οποίων η αξία συνήθως υποτιμάται με το πέρασμα του χρόνου.

Μειωμένα κόστη διαχείρισης:

Οι υπηρεσίες που βασίζονται στο cloud computing μπορούν να αναπτυχθούν εξαιρετικά γρήγορα και να συντηρούνται, να διαχειρίζονται και να αναβαθμίζονται απομακρυσμένα από τον πάροχο της υπηρεσίας. Η τεχνική υποστήριξη παρέχεται όλο το εικοσιτετράωρο από τους παρόχους της υπηρεσίας μειώνοντας την ανάγκη για προσωπικό και για τα κόστη εκπαίδευσής του.

Βελτιωμένη χρήση πόρων:

Ο συνδυασμός πόρων σε μεγάλα clouds μειώνει το κόστος και μεγιστοποιεί την ωφέλιμη χρήση με την παράδοση των πόρων μόνο εκεί όπου χρειάζονται. Ο διαμοιρασμός υπολογιστικής ισχύος ανάμεσα σε πολλαπλούς χρήστες (tenants) μπορεί να βελτιώσει τα ποσοστά ωφέλιμης χρήσης αφού οι εξυπηρετητές δεν παραμένουν αδρανείς , κάτι που μπορεί να μειώσει το κόστος σημαντικά ενώ αυξάνει το ρυθμό της ανάπτυξης εφαρμογών. Μια παρενέργεια αυτής της προσέγγισης είναι η δραματική αύξηση της χωρητικότητας του υπολογιστή καθώς οι χρήστες δεν χρειάζεται να κάνουν σχεδιασμούς για την αποφυγή των φορτίων αιχμής.

Επεκτασιμότητα κατ'απαίτηση:

Δυο από τα σημαντικότερα πλεονεκτήματα που προσφέρει το cloud computing είναι η επεκτασιμότητα και η ευελιξία, επιτρέποντας στους πελάτες να αντιδρούν γρήγορα στις διαρκώς μεταβαλλόμενες ανάγκες, προσθέτοντας ή αφαιρώντας χωρητικότητα , ανταποκρινόμενοι στις πραγματικές και όχι στις προβλεπόμενες απαιτήσεις.

Γρήγορη και εύκολη υλοποίηση:

Εφόσον δεν υπάρχει η ανάγκη αγοράς υλικού ή κάποιας άδειας χρήσης ενός λογισμικού, μια εταιρία μπορεί να αποκτήσει μια υπηρεσία cloud μέσα σε λίγα λεπτά.

Βελτιώνει την ανταγωνιστικότητα των μικρότερων επιχειρήσεων:

Το cloud computing επιτρέπει σε μικρότερες επιχειρήσεις να ανταγωνιστούν τις μεγαλύτερες επί ίσοις όροις. Η ενοικίαση υπηρεσιών IT αντί για την επένδυση σε υλικό και λογισμικό επιτρέπει τη χρησιμοποίηση των κεφαλαίων σε άλλα ζωτικής σημασίας προγράμματα.

Πρόσβαση από παντού.

Οι βασισμένες στο cloud (cloud-based) υπηρεσίες επιτρέπουν την πρόσβαση σε εφαρμογές και δεδομένα από οποιαδήποτε τοποθεσία μέσω μιας σύνδεσης στο διαδίκτυο. Ακόμη, αφού και οι εφαρμογές και τα δεδομένα βρίσκονται στο cloud, πολλαπλοί χρήστες μπορούν να δουλέψουν πάνω στο ίδιο project την ίδια στιγμή.

Ανάνηψη από καταστροφές/backup:

Πρόσφατες μελέτες υποδεικνύουν ότι το 90% των επιχειρήσεων δεν διαθέτουν μηχανισμούς ανάνηψης από καταστροφές καθιστώντας τες ευάλωτες σε τυχόν ατυχή περιστατικά. Οι πάροχοι cloud παρέχουν ένα φάσμα υπηρεσιών ανάνηψης όπως cloud backup ή έχοντας υπολογιστές και υπηρεσίες άμεσα διαθέσιμες σε περίπτωση προβλήματος.

1.5 Βιβλιογραφία κεφαλαίου

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, *"Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley,Tech. Rep*, 2009.

[2]Cloud Computing For Dummies, HP Special Edition, Wiley Publishing Inc.

[3]White Paper: Introduction to cloud computing, ThinkGrid Business IT On Demand

Κεφάλαιο 2

SLA και SOA

Περιεχόμενα

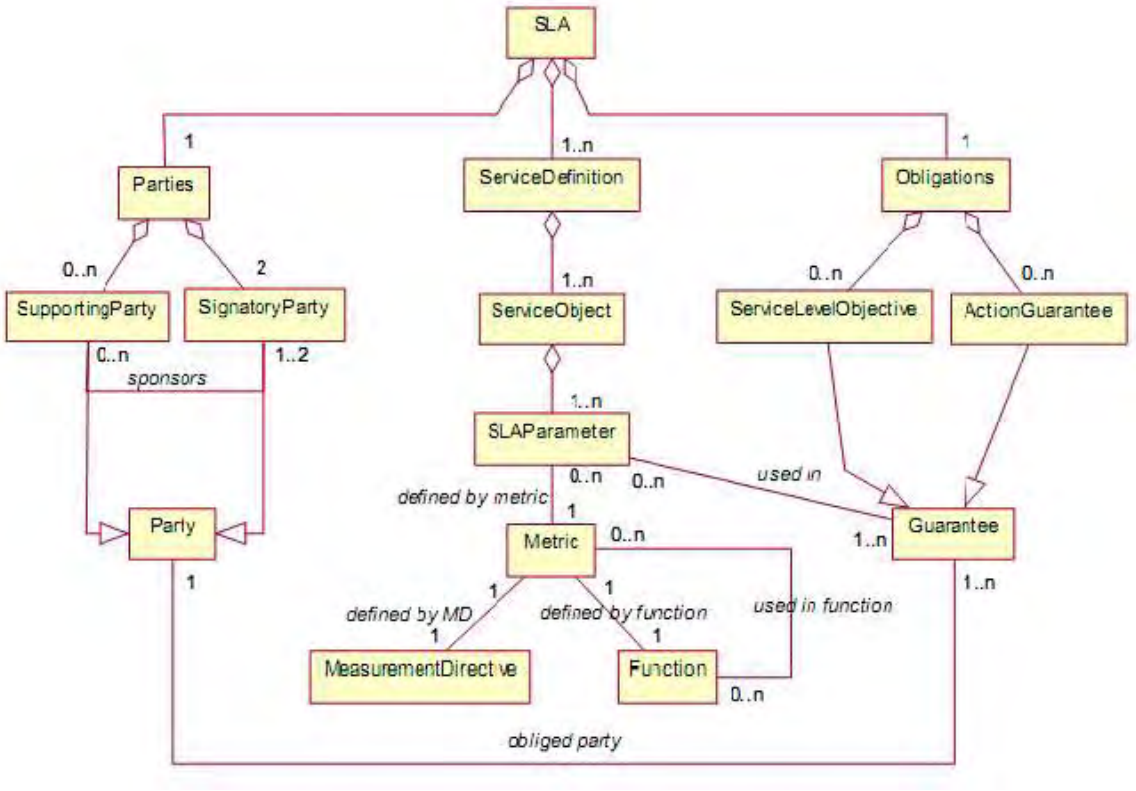
2.1 Συμφωνίες Επιπέδου Υπηρεσίας (Service Level Agreements)

Καθώς όλο και περισσότεροι πελάτες αναθέτουν τις διεργασίες τους σε παρόχους cloud υπηρεσιών, εμφανίζεται μια καινούρια άποψη που διέπει τις σχέσεις ανάμεσα σε καταναλωτές και παρόχους, τις Συμφωνίες Επιπέδου Υπηρεσίας[4] (Service Level Agreements-SLA). Εξαιτίας της δυναμικής φύσης του cloud, είναι απαραίτητος ο αδιάκοπος έλεγχος στα χαρακτηριστικά της Ποιότητα της Υπηρεσίας (Quality of Service-QoS), έτσι ώστε να επιβληθούν τα SLAs. Μετά από μια διαδικασία διαπραγμάτευσης, ο πελάτης και ο πάροχος καταλήγουν σε μια συμφωνία, η οποία αναφέρεται ως SLA. Αυτή η συμφωνία αποτελεί το θεμέλιο για το αναμενόμενο επίπεδο της παρεχόμενης υπηρεσίας ανάμεσα σε πελάτη και πάροχο. Η αρχιτεκτονική που χρησιμοποιείται για την διαχείριση των SLAs ανάμεσα στους πελάτες και τους παρόχους των cloud υπηρεσιών βασίζεται στο Web Service Level Agreements (WSLA).

2.1.1 Web Service Level Agreements-WSLA Framework

Το WSLA αποτελείται από ένα σύνολο εννοιών και μια XML γλώσσα. Αποτελείται από 3 κυρίως οντότητες:

- ***Εμπλεκόμενα μέρη (Parties):*** Το WSLA περιέχει περιγραφές που αφορούν τον πάροχο της υπηρεσίας, τον πελάτη της υπηρεσίας και κάποια τρίτα πρόσωπα. Το έργο αυτών των τρίτων προσώπων μπορεί να ποικίλει, από την μέτρηση παραμέτρων υπηρεσίας έως την λήψη μέτρων για παραβιάσεις που αφορούν είτε την πλευρά του παρόχου είτε του πελάτη.
- ***SLA παραμέτρους:*** Στο WSLA οι SLA παράμετροι καθορίζονται από μετρήσεις οι οποίες είναι στη γενικότερη περίπτωση συναρτήσεις. Υπάρχουν 2 κύριοι τύποι μετρήσεων. 1) Μετρήσεις πόρων οι οποίες ανακτώνται απευθείας από τον πάροχο και χρησιμοποιούνται ως έχουν, χωρίς περαιτέρω επεξεργασία, για παράδειγμα η καταμέτρηση συναλλαγών. 2) Σύνθετες μετρήσεις οι οποίες αναπαριστούν ένα συνδυασμό από πολλές μετρήσεις πόρων υπολογισμένες από ένα συγκεκριμένο αλγόριθμο. Για παράδειγμα οι συναλλαγές ανά ώρα συνδυάζουν τις 2 μετρήσεις πόρων του αριθμού των συναλλαγών και του χρόνου λειτουργίας.
- ***Στόχοι Επιπέδου Υπηρεσίας (Service Level Objectives-SLOs):*** Είναι ένα σύνολο από εκφράσεις που έχουν την γνωστή δομή if... then. Το if περιέχει προϋποθέσεις και το then περιέχει τις δράσεις. Μια δράση αναπαριστά το τι ένα πρόσωπο έχει συμφωνήσει να κάνει όταν οι προϋποθέσεις γίνουν αληθείς.



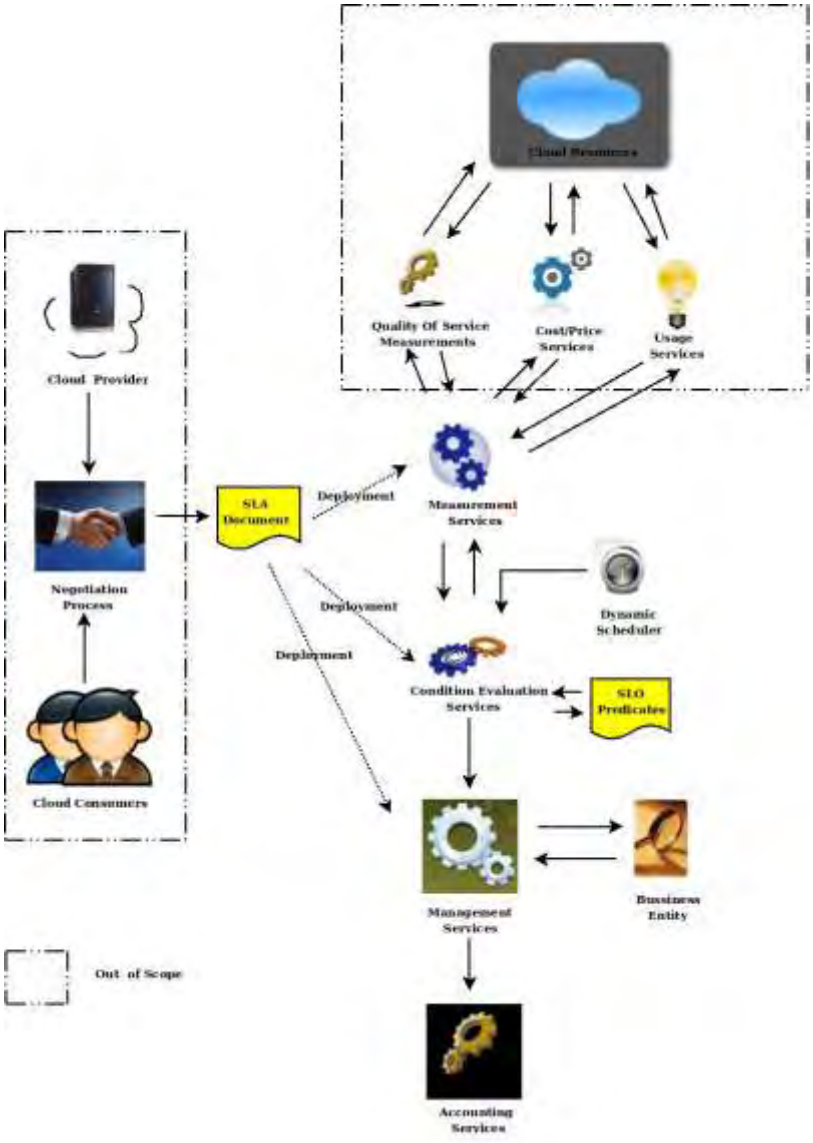
Εικόνα 2.1 : Οι κύριες έννοιες του WSLA σε ένα διάγραμμα UML. [4]

2.1.2 WSLA Αρχιτεκτονική

Οι παρακάτω πτυχές του cloud επηρεάζουν την απευθείας χρήση του WSLA[5]:

- Το cloud είναι εξ' ορισμού δυναμικό και η χρησιμοποίηση των πόρων αλλάζει κάθε στιγμή. Οπότε κάθε σύστημα το οποίο προσπαθεί να επιβάλλει ένα SLA πρέπει να λάβει υπόψιν αυτή τη δυναμική του φύση.
- Εξαιτίας της ανησυχίας αναφορικά με την ασφάλεια των δεδομένων τους και την εξασφάλιση της ιδιοτικότητας οι καταναλωτές μπορεί να διστάσουν να αποκαλύψουν συγκεκριμένες πληροφορίες στους παρόχους cloud.
- Οι υπηρεσίες cloud υπόκεινται σε διακυμάνσεις φόρτου και οι παραβιάσεις των SLA είναι πιθανότερο να συμβούν κατά τη διάρκεια αυτών των φάσεων. Η φύση αυτών των διακυμάνσεων είναι απρόβλεπτη και έτσι ένα στατικό μοντέλο για την αξιολόγηση των προϋποθέσεων δεν είναι επαρκές.

Η αρχιτεκτονική του WSLA παρουσιάζεται στην εικόνα. Σε αυτήν την αρχιτεκτονική υπάρχει η προϋπόθεση ότι ο πάροχος του cloud και ο πελάτης έχουν ήδη συμμετάσχει στη διαδικασία διαπραγμάτευσης και έχουν ένα συμφωνημένο σύνολο από παραμέτρους υπηρεσίας:



Εικόνα 2.2 : Αρχιτεκτονική του WSLA. [4]

Παρακάτω περιγράφονται 3 συνήθεις υπηρεσίες WSLA και κάποιες από τις προσαρμογές που απαιτούνται για το περιεχόμενο του cloud:

- ***Υπηρεσίες μετρήσεων:*** Είναι υπεύθυνες για τις μετρήσεις των παραμέτρων πόρων των παρόχων κατά το χρόνο της εκτέλεσης. Όμως η παράμετροι υπηρεσίας όπως η ρυθμαπόδοση και ο χρόνος απόκρισης αλλάζουν συνεχώς λόγω της μεταβαλλόμενης ζήτησης από την πλευρά του πελάτη. Στο περιεχόμενο του cloud οι παράμετροι που αφορούν την χρήση και το κόστος είναι επίσης δυναμικές λόγω της φύσης του pay-as-you-go και της ελαστικότητας που προσφέρει το cloud. Οπότε οι υπηρεσίες που μετρούν τα δεδομένα χρήσης και του κόστους/τιμής προστίθενται στο σύνολο των υπηρεσιών μέτρησης στο περιεχόμενο του cloud.
- ***Υπηρεσία Αξιολόγησης Συνθήκης:*** Αυτή η υπηρεσία είναι υπεύθυνη για την ανάκτηση των αποτελεσμάτων από τις υπηρεσίες μέτρησης και την αξιολόγηση των SLOs. Εάν υπάρχουν παραβιάσεις καλείται η υπηρεσία διαχείρισης. Λόγω της δυναμικής φύσης του cloud η αξιολόγηση της συνθήκης πρέπει να εκτελείται συχνότερα από ότι σε ένα παραδοσιακό framework υπηρεσίας. Στο περιεχόμενο του cloud οι συνθήκες θα πρέπει να είναι απλούστερες για γρηγορότερη κύκλους αποτίμησης.
- ***Υπηρεσία Διαχείρισης:*** Αυτή η υπηρεσία είναι υπεύθυνη για τη λήψη σωστών αποφάσεων σε περίπτωση παραβίασης των SLOs. Η υπηρεσία διαχείρισης χειρίζεται κυρίως οικονομικές ποινές παρόμοιες με αυτές του πραγματικού κόσμου.

2.2 Υπηρεσιοστραφής Αρχιτεκτονική (Service Oriented Architecture-SOA)

Η Υπηρεσιοστραφής (Service-oriented) αρχιτεκτονική (SOA) είναι ένα ευέλικτο σύνολο από αρχές σχεδίασης που χρησιμοποιούνται κατά τις φάσεις της ανάπτυξης συστημάτων. Το SOA είναι ένα σχέδιο σύνδεσης των επαγγελματικών πόρων με υπολογιστικούς (κυρίως οργανισμούς, εφαρμογές και δεδομένα) κατ'απαίτηση έτσι ώστε να επιτύχει τα επιθυμητά αποτελέσματα για τους πελάτες της υπηρεσίας. Η OASIS[6] δίνει τον έξης ορισμό για την SOA:

Είναι ένα παράδειγμα οργάνωσης και αξιοποίησης από κατανεμημένες δυνατότητες οι οποίες μπορεί να βρίσκονται κάτω από τον έλεγχο διαφορετικών ιδιοκτητών και παρέχει ένα ομοιόμορφο μέσο προσφοράς, ανακάλυψης, αλληλεπίδρασης και χρήσης δυνατοτήτων για να παράξει τα επιθυμητά αποτελέσματα που θα είναι συνεπή με τις προϋποθέσεις και προσδοκίες που έχουν τεθεί.

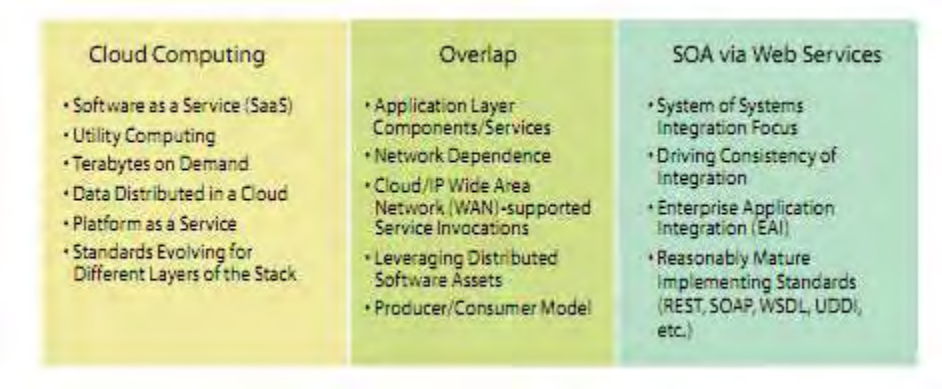
2.2.1 Χαρακτηριστικά SOA:

Η υπηρεσιοστραφής (Service-oriented)[7] αρχιτεκτονική, είναι ένα ειδικό είδος αρχιτεκτονικής λογισμικού με πολλά μοναδικά χαρακτηριστικά. Το ποιο σημαντικό μέρος της SOA είναι ότι ξεχωρίζει την υλοποίηση της υπηρεσίας από την διεπαφή της. Με άλλα λόγια ξεχωρίζει το "γιατί" από το "πως". Οι πελάτες της υπηρεσίας δεν ενδιαφέρονται για το πως η υπηρεσία εκτελεί τα αιτήματα τους, απλά περιμένουν το αποτέλεσμα.

- ***Ανακαλύψημα και δυναμικά δεσμευόμενα (Discoverable and dynamically bound):*** Το SOA υποστηρίζει την αρχή της ανακάλυψης υπηρεσίας. Ένας πελάτης υπηρεσίας που χρειάζεται την υπηρεσία ανακαλύπτει ποια υπηρεσία χρειάζεται βασιζόμενος σε ένα σύνολο κριτηρίων κατά το χρόνο εκτέλεσης.
- ***Αυτοπεριοριζόμενα και αρθρωτά (Self-contained and Modular):*** Ένα από τα ποιο σημαντικά χαρακτηριστικά του SOA είναι η αρχή της άρθρωσης (modular). Μια υπηρεσία υποστηρίζει ένα σύνολο από διεπαφές, οι οποίες πρέπει να σχετίζονται μεταξύ τους στο πλαίσιο της μονάδας (module).
- ***Διαλειτουργικότητα:*** Η SOA υποστηρίζει την ικανότητα των συστημάτων που χρησιμοποιούν διαφορετικές πλατφόρμες να επικοινωνούν μεταξύ τους.
- ***Χαλαρή σύζευξη (Loose Coupling):*** Υπάρχουν 2 είδη σύζευξης (coupling) η χαλαρή και η σφικτή(tight). Οι χαλαρά συζευγμένες μονάδες (loosely coupled modules) έχουν πολύ λίγες γνωστές εξαρτήσεις αντίθετα με τις σφικτά συζευγμένες (tightly coupled). Όλες οι αρχιτεκτονικές λογισμικού θέλουν να πετύχουν loose coupling ανάμεσα στα modules. Η SOA υποστηρίζει το loose-coupling ανάμεσα σε πελάτες υπηρεσίας και παρόχους κα την ιδέα πολύ λίγων γνωστών εξαρτήσεων ανάμεσα σε πελάτες και παρόχους.
- ***Διαφάνεια τοποθεσίας:*** Οι πελάτες της υπηρεσίας δεν γνωρίζουν την τοποθεσία της υπηρεσίας μέχρις ότου να εντοπίσουν την εγγραφή της. Η αναζήτηση και η δυναμική δέσμευση (binding) σε μια υπηρεσία κατά το χρόνο εκτέλεσης επιτρέπει στην υλοποίηση της υπηρεσίας να μετακινείται σε διαφορετικές τοποθεσίες χωρίς να το γνωρίζει ο πελάτης.
- ***Συνθετικότητα:*** Η συνθετικότητα μιας υπηρεσίας σχετίζεται με την αρθρωτή κατασκευή (modular structure) της. Η αρθρωτή κατασκευή επιτρέπει στις υπηρεσίες να μπορούν να αυτό-συναρμολογηθούν σε εφαρμογές για τις οποίες ο υπεύθυνος ανάπτυξης λογισμικού δεν είχε γνώση κατά τη διαδικασία της σχεδίασης.
- ***Αυτό-Ανάνηψη (Self-Healing):*** Ένα σύστημα με αυτό-ανάνηψη έχει την ικανότητα να ανανήψει από λάθη χωρίς ανθρώπινη παρέμβαση κατά το χρόνο της εκτέλεσης.

2.2.2 Ομοιότητες SOA-Cloud Computing

Το cloud computing και το SOA έχουν σημαντικά επικαλυπτόμενα χαρακτηριστικά[8].



Εικόνα 2.3 : Επικαλυπτόμενα χαρακτηριστικά μεταξύ cloud computing και υπηρεσιοστραφούς αρχιτεκτονικής. [8]

Το cloud computing και το SOA μοιράζονται τα χαρακτηριστικά του service orientation. Υπηρεσίες πολλών τύπων είναι διαθέσιμες σε ένα κοινό δίκτυο από όπου μπορούν να χρησιμοποιηθούν από τους πελάτες.

- ***Εξάρτηση από φυσικά δίκτυα (Network dependence):*** Και τα 2 βασίζονται σε ένα φυσικό δίκτυο για να συνδέσουν καταναλωτές και παρόχους , και με αυτό το σκεπτικό έχουν την ίδια θεμελιώδη αδυναμία, όταν το δίκτυο δεν είναι διαθέσιμο.
- ***Forms of outsourcing***: Και τα 2 απαιτούν τύπους συμβολαιακών σχέσεων ανάμεσα σε πελάτες και παρόχους.
- ***Πρότυπα (Standards):*** Και τα 2 παρέχουν σε έναν οργανισμό τη δυνατότητα επιλογής ομαδικών προτύπων για δυνατότητες προσβάσιμες μέσω δικτύου.

2.3 Βιβλιογραφία κεφαλαίου

[1] Pankesh Patel, Ajith Ranabahu1, Amit Sheth: *Service Level Agreement in Cloud Computing*

[2] Emmanuel Marilly, Olivier Martinot, Htlkne Papini, Danny Goderis: *Service level Agreements: A Main Challenge For Next Generation Networks*

[3] Mohammad Hadi Valipour, Bavar Amirzafari, Khashayar Niki Maleki and Negin Daneshpour: *A Brief Survey of Software Architecture Concepts and Service Oriented Architecture*

[4] Systems Engineering at MITRE : Service-Oriented Architecture (SOA) Series

[5] Organization for the advancement of structured information standards.
[Online]. Available: http://www.oasis-open.org

Κεφάλαιο 3

Η οντολογία του Cloud

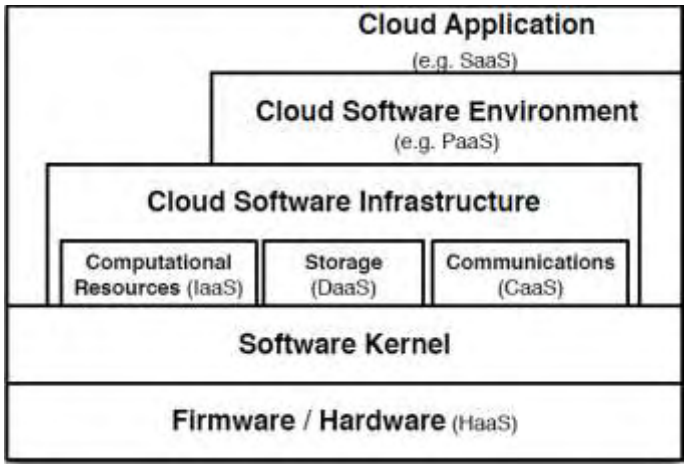
Περιεχόμενα

3.1 Εισαγωγικά στοιχεία

Η τεχνολογία του cloud computing έχει δανειστεί τα βασικά της στοιχεία από διάφορες άλλες περιοχές και έννοιες της επιστήμης των υπολογιστών. Το Grid[9] και Cluster Computing από την μια και η εικονοποίηση (virtualization) από την άλλη είναι πιθανότατα οι πιο προφανείς προγενέστερες τεχνολογίες που ενέπνευσαν το cloud computing. Παρόλα αυτά όμως πολλές άλλες τεχνολογίες βοήθησαν έμμεσα στην ανάπτυξη του cloud computing με τη σημερινή του μορφή. Τεχνολογίες όπως το peer-to-peer, SOA και το autonomic computing. Με βάση αυτά τα στοιχεία είναι απαραίτητη μια θεμελιώδης κατανόηση της έκτασης των λειτουργιών των οποίων το cloud computing κληρονομεί από αυτές τις περιοχές και τα μοντέλα της επιστήμης των υπολογιστών έτσι ώστε να γίνει απολύτως κατανοητή η δομή αυτής της νέας τεχνολογίας αλλά και να καθοριστούν οι προοπτικές και οι περιορισμοί της. Για να γίνουν όλες αυτές οι έννοιες ευκολότερα αντιληπτές απαιτείται η μελέτη των διαφορετικών μελών που αποτελούν το cloud , τα χαρακτηριστικά τους καθώς και η εξάρτηση τους από άλλα μοντέλα της επιστήμης των υπολογιστών. Ο καθορισμός της οντολογίας του cloud επιτρέπει την καλύτερη κατανόηση των σχέσεων ανάμεσα στα μέρη του και τη σύνθεση νέων συστημάτων με σκοπό την επίτευξη διάφορων επιθυμητών χαρακτηριστικών όπως η επεκτασιμότητα, η ευελιξία, η μείωση του κόστους κ.α. .

3.2 Η οντολογία του Cloud

Τα συστήματα του cloud computing εντάσσονται σε μια από τις 5 παρακάτω κατηγορίες[10]: εφαρμογές, περιβάλλοντα λογισμικού, υποδομές λογισμικού, λογισμικό kernel και υλικό. Προφανώς στο χαμηλότερο επίπεδο του cloud βρίσκεται το επίπεδο υλικού το οποίο είναι στην πραγματικότητα τα φυσικά μέρη του συστήματος. Στο υψηλότερο επίπεδο βρίσκονται οι εφαρμογές , οι οποίες στην ουσία είναι οι διεπαφές ανάμεσα στο cloud και τον απλό χρήστη της υπηρεσίας μέσα από web browsers και thin τερματικά συστήματα.



Εικόνα 3.1 : Η οντολογία του Cloud, χωρισμένη σε πέντε στρώματα. [10]

3.2.1 Το στρώμα της εφαρμογής Cloud.

Το επίπεδο εφαρμογής του cloud είναι αυτό το οποίο "βλέπουν" οι τελικοί χρήστες του. Συνήθως οι χρήστες προσπελαύνουν τις υπηρεσίες που προσφέρονται από αυτό το επίπεδο μέσω web-portals και τις περισσότερες φορές είναι υποχρεωμένοι να καταβάλλουν κάποιο αντίτιμο για να τις χρησιμοποιήσουν. Αυτό το μοντέλο έχει αποδειχθεί αρκετά ελκυστικό στους χρήστες, καθώς τους απαλλάσσει από το βάρος της συντήρησης του λογισμικού, της συνεχούς λειτουργίας και το κόστος υποστήριξης. Επιπρόσθετα, εξάγει την υπολογιστική εργασία από τον προσωπικό υπολογιστή του χρήστη, στα data centers όπου είναι εγκατεστημένες οι cloud εφαρμογές, κάτι το οποίο με τη σειρά του μειώνει τους περιορισμούς σχετικά με το υλικό που απαιτείται από την πλευρά του χρήστη, επιτρέποντας τον να απολαμβάνει πραγματικά μεγάλη απόδοση ακόμα και για τις πιο απαιτητικές σε επεξεργαστική ισχύ και μνήμη εργασίες, χωρίς την απαίτηση μεγάλων επενδύσεων στα τοπικά τους μηχανήματα.

Όσων αφορά τους παρόχους των cloud υπηρεσιών, το συγκεκριμένο μοντέλο απλοποιεί τις όποιες εργασίες για την αναβάθμιση ή συντήρηση του λογισμικού τους, ενώ παράλληλα τους εξασφαλίζει την προστασία των πνευματικών τους δικαιωμάτων. Αφού μια cloud εφαρμογή εγκαθίσταται στην υποδομή του παρόχου, και όχι στα τοπικά μηχανήματα του τελικού χρήστη της υπηρεσίας, οι υπεύθυνοι ανάπτυξης της εφαρμογής έχουν τη δυνατότητα εφαρμόσουν patches στο σύστημα καθώς και να προσθέσουν νέες λειτουργίες σε αυτό χωρίς να απαιτείται κάποια εγκατάσταση μιας μεγάλης ενημέρωσης (update) η κάποιου service pack από την πλευρά του χρήστη. Η ρύθμιση των παραμέτρων και ο έλεγχος της εφαρμογής με αυτό το μοντέλο είναι αναμφισβήτητα λιγότερο περίπλοκη αφού το περιβάλλον είναι περιορισμένο, π.χ. το

data center του παρόχου. Ακόμα και σε σχέση με το περιθώριο κέρδους του παρόχου, αυτό το μοντέλο παρέχει στον πάροχο μια συνεχή ροή από έσοδα, το οποίο μπορεί να αποδειχθεί πολύ πιο επικερδές σε βάθος χρόνου. Αυτό το μοντέλο παρέχει πολλά πλεονεκτήματα στους χρήστες αλλά και στους παρόχους των cloud εφαρμογών, και αναφέρεται ως Software As A Service (SaaS). Το Salesforce[11] Customer Relationships Manager (CRM) και το Google Apps είναι 2 παραδείγματα του SaaS.

Οι cloud εφαρμογές μπορούν να αναπτυχθούν στο περιβάλλον λογισμικού, ή στα τμήματα της υποδομής του cloud. Επιπρόσθετα οι εφαρμογές cloud μπορούν να συντεθούν «ως μια υπηρεσία» (as a service) από άλλες υπηρεσίες cloud που προσφέρονται από διαφορετικά συστήματα cloud, χρησιμοποιώντας τις έννοιες του SOA. Για παράδειγμα μια εφαρμογή μισθοδοσίας μπορεί να χρησιμοποιεί μια άλλη υπηρεσία λογιστικής SaaS για να υπολογίσει τους φόρους που εκπίπτουν για κάθε υπάλληλο στο σύστημά της, χωρίς να χρειαστεί να ενσωματώσει αυτήν την υπηρεσία στο αυτό κάθε αυτό λογισμικό μισθοδοσίας. Από αυτήν την άποψη, οι εφαρμογές cloud οι οποίες στοχεύουν σε υψηλότερα επίπεδα της στοίβας των υπηρεσιών του cloud, είναι απλούστερες και έχουν μικρότερο χρόνο διάθεσής τους στην αγορά. Επίσης, είναι περισσότερο ανθεκτικές σε λάθη αφού όλες οι αλληλεπιδράσεις τους με το cloud γίνονται μέσα από δοκιμασμένα APIs. Ωστόσο, αφού αυτές οι εφαρμογές έχουν αναπτυχθεί για υψηλότερο επίπεδο της στοίβας του cloud , έχουν περιορισμένη ευελιξία, κάτι που μπορεί να περιορίσει την ικανότητα των υπεύθυνων ανάπτυξης να βελτιστοποιήσουν την απόδοση της εφαρμογής τους.

Παρόλες τις επωφελείς παροχές αυτού του μοντέλου, υπάρχουν αρκετά θέματα σχετικά με την ανάπτυξή των εφαρμογών που εμποδίζουν την καθολική υιοθέτηση του. Πιο συγκεκριμένα η ασφάλεια και η διαθεσιμότητα της εφαρμογής cloud είναι 2 από τα σοβαρότερα προβλήματα αυτού του μοντέλου, τα οποία προς το παρόν περιορίζονται με τη χρήση επιεικών Service Level Agreements (SLAs). Ακόμη, η αντιμετώπιση των διακοπών είναι ένα σοβαρό θέμα το οποίο χρήστες και πάροχοι SaaS υπηρεσιών πρέπει να ξεπεράσουν, ειδικά όσων αφορά διακοπές δικτύου και αποτυχίες του συστήματος. Ένα ακόμη θέμα που καθυστερεί την υιοθέτηση του SaaS είναι η ενσωμάτωση κάποιων παλαιάς τεχνολογίας εφαρμογών στο cloud και η μεταφορά των δεδομένων του χρήστη σε αυτό. Προτού λοιπόν οι πάροχοι υπηρεσιών cloud πείσουν τους χρήστες να στραφούν από της εφαρμογές που εκτελούνται στο desktop τους σε εφαρμογές cloud , πρέπει να αντιμετωπίσουν τις ανησυχίες των τελικών χρηστών σχετικά με την ασφάλεια της αποθήκευσης εμπιστευτικών πληροφοριών στο cloud, την αυθεντικοποίηση και εξουσιοδότηση των χρηστών, το up-time της υπηρεσίας , την απόδοση, την ανάκαμψη από βλάβες καθώς και την παροχή αξιόπιστων SLAs για τις cloud εφαρμογές τους.

3.2.2 Το στρώμα περιβάλλοντος λογισμικού του Cloud.

Το δεύτερο επίπεδο της οντολογίας του cloud είναι το επίπεδο του περιβάλλοντος λογισμικού του cloud. Οι χρήστες αυτού του επιπέδου είναι οι υπεύθυνοι ανάπτυξης εφαρμογών του cloud. Οι πάροχοι των περιβαλλόντων λογισμικού cloud παρέχουν στους υπευθύνους ανάπτυξης εφαρμογών ένα programming-language-level περιβάλλον με ένα σύνολο από καλά ορισμένα APIs για να διευκολύνουν την αλληλεπίδραση μεταξύ των περιβαλλόντων και των εφαρμογών cloud, αλλά και για την επιτάχυνση της ανάπτυξης και της υποστήριξης επεκτασιμότητας αυτών των cloud εφαρμογών. Η υπηρεσία που παρέχεται από τα συστήματα cloud αυτού του επιπέδου αναφέρεται συνήθως ως «Πλατφόρμα Ως Υπηρεσία» (Platform As A Service-PaaS). Ένα παράδειγμα συστήματος αυτής της κατηγορίας είναι το Google App Engine, το οποίο παρέχει ένα περιβάλλον λειτουργίας βασισμένο στην python και APIs για τις εφαρμογές οι οποίες αλληλεπιδρούν με το περιβάλλον λειτουργίας cloud της Google. Ένα ακόμη παράδειγμα είναι η γλώσσα SalesForce Apex[12] η οποία επιτρέπει στους προγραμματιστές των cloud εφαρμογών να σχεδιάζουν τις εφαρμογές τους ανάλογα με τη λογική των εφαρμογών, τη διάταξη σελίδας και τις αναφορές των πελατών.

Οι προγραμματιστές απολαμβάνουν αρκετά πλεονεκτήματα από την ανάπτυξη των cloud εφαρμογών τους για ένα περιβάλλον προγραμματισμού cloud, όπως αυτόματη κλιμάκωση και ισοστάθμιση του φόρτου αλλά και ενσωμάτωση σε άλλες υπηρεσίες, όπως υπηρεσίες αυθεντικοποίησης, υπηρεσίες e-mail κλπ., οι οποίες παρέχονται σε αυτούς μέσω του παρόχου PaaS. Με αυτόν τον τρόπο το μεγαλύτερο βάρος της ανάπτυξης cloud εφαρμογών μπορεί να μετριαστεί και ο χειρισμός του γίνεται στο επίπεδο περιβάλλοντος. Επιπλέον, οι προγραμματιστές έχουν την δυνατότητα να ενσωματώνουν άλλες υπηρεσίες στις εφαρμογές τους κατ'απαίτηση. Αυτό με τη σειρά του κάνει την ανάπτυξη εφαρμογών cloud λιγότερο περίπλοκη, επιταχύνει τον χρόνο ανάπτυξης και ελαττώνει στο ελάχιστο τα λάθη λογικής της εφαρμογής.

3.2.3 Το στρώμα υποδομής λογισμικού του Cloud

Το επίπεδο υποδομής λογισμικού του cloud παρέχει θεμελιώδεις πόρους στα άλλα υψηλότερου επιπέδου στρώματα, τα οποία με τη σειρά τους μπορούν να χρησιμοποιηθούν για την κατασκευή νέων περιβαλλόντων λογισμικού cloud ή cloud εφαρμογών. Οι υπηρεσίες cloud που προσφέρονται σε αυτό το επίπεδο μπορούν να κατηγοριοποιηθούν ως εξής: υπολογιστικοί πόροι, αποθηκευτικά μέσα και επικοινωνίες.

3.2.3.1 Υπολογιστικοί Πόροι

Οι Εικονικές Μηχανές (Virtual Machines-VMs) είναι ο πιο συνήθης τρόπος παροχής υπολογιστικών πόρων στους χρήστες σε αυτό το επίπεδο, συνήθως αυτού του είδους οι υπηρεσίες αναφέροντα ως «Υποδομή Ως Υπηρεσία» (Infrastructure As A Service-IaaS). Η εικονοποίηση είναι η καταλυτική τεχνολογία για αυτό το μέρος του cloud, η οποία προσδίδει στους χρήστες πρωτοφανή ευελιξία στη ρύθμιση των παραμέτρων τους, προστατεύοντας ταυτόχρονα την φυσική υποδομή του data center του παρόχου. Η πρόσφατη πρόοδος στην εικονοποίηση λειτουργικών συστημάτων έκανε εφικτή την ιδέα της IaaS. Αυτό έγινε επιτρεπτό κυρίως από 2 τεχνολογίες εικονοποίησης: παραεικονοποίηση (paravirtualazation) και υποβοηθούμενη από το υλικό εικονοποίηση (hardware-assisted virtualization). Παρόλο που και οι 2 τεχνολογίες εικονοποίησης έχουν πετύχει απομόνωση της απόδοσης ανάμεσα σε εικονικές μηχανές που ανταγωνίζονται για κοινούς πόρους, η παρεμβολή της απόδοσης ανάμεσα σε VMs που μοιράζονται την ίδια κρυφή μνήμη (cache) και TLB δεν μπορεί ακόμα να αποφευχθεί. Ακόμα η εμφάνιση πολυπύρηνων μηχανημάτων στους servers έχει επιδεινώσει αυτό το πρόβλημα, καθώς η έλλειψη αυστηρής απομόνωσης της απόδοσης ανάμεσα σε VMs που μοιράζονται τον ίδιο φυσικό κόμβο έχει ως αποτέλεσμα την ανικανότητα των παρόχων cloud υπηρεσιών να παρέχουν ισχυρές εγγυήσεις στους πελάτες τους σχετικά με την απόδοση. Αντιθέτως τους παρέχουν μη ικανοποιητικές SLAs με σκοπό να πετύχουν ανταγωνιστική τιμολόγηση των υπηρεσιών τους. Τέτοιες αδύναμες εγγυήσεις δυστυχώς μπορούν να περάσουν σε ανώτερα στρώματα της στοίβας και να επηρεάσουν τα SLAs των συστημάτων cloud που βρίσκονται πάνω από τα SLAs του IaaS.

3.2.3.2 Αποθήκευση Δεδομένων

Ο δεύτερος πόρος υποδομής είναι ο χώρος αποθήκευσης, ο οποίος επιτρέπει στους χρήστες να αποθηκεύουν τα δεδομένα τους σε απομακρυσμένους δίσκους και να έχουν πρόσβαση από παντού όποτε το θελήσουν. Αυτή η υπηρεσία είναι γνωστή ως «Αποθήκευση Δεδομένων Ως Υπηρεσία» (Data Storage As A Service-DaaS) και επιτρέπει στις εφαρμογές cloud να κλιμακώνονται πέρα από τους περιορισμούς των servers. Τα συστήματα αποθήκευσης δεδομένων αναμένεται να πληρούν αρκετές αυστηρές προϋποθέσεις σχετικά με τη διατήρηση των δεδομένων και πληροφοριών των χρηστών συμπεριλαμβανομένων της υψηλής διαθεσιμότητας, αξιοπιστίας, απόδοσης, αναπαραγωγής και εγκυρότητας δεδομένων, αλλά λόγω της αντικρουόμενης φύσης αυτών των απαιτήσεων κανένα σύστημα δεν τις παρέχει όλες μαζί. Για παράδειγμα η διαθεσιμότητα, η κλιμάκωση και η εγκυρότητα των δεδομένων μπορούν να θεωρηθούν ως 3 αντικρουόμενοι στόχοι. Ενώ αυτά τα χαρακτηριστικά είναι

δύσκολο να πληρούνται σε ένα γενικό σύστημα αποθήκευσης δεδομένων, οι πάροχοι DaaS πήραν το θάρρος να ευνοήσουν κάποιο από τα χαρακτηριστικά σε βάρος κάποιου άλλου, υποδηλώνοντας την επιλογή τους μέσω του SLA τους. Αυτές οι υλοποιήσεις έχουν δανειστεί τις θεμελιώδεις ιδέες τους από διαδικασίες έρευνας και συστήματα παραγωγής. Μερικά παραδείγματα συστημάτων αποθήκευσης δεδομένων είναι: κατανεμημένα συστήματα αρχείων (πχ. GFS), αναπαραγμένες σχεσιακές βάσεις δεδομένων (RDBMS) και key-value stores[13] (Dynamo). Το RDBMS για παράδειγμα επιλέγει να παρουσιάσει ένα αυστηρότερο μοντέλο συνοχής εις βάρος της διαθεσιμότητας των δεδομένων, ενώ τα key-value stores έχουν θέσει ως σημαντικότερη την διαθεσιμότητα των δεδομένων σε σχέση με το μοντέλο συνοχής τους. Από αυτήν την άποψη το DaaS cloud έχει κληρονομήσει τα διαφορετικά χαρακτηριστικά των συστημάτων αποθήκευσης δεδομένων . Μερικά παραδείγματα εμπορικών συστημάτων DaaS είναι το S3 της Amazon και το EMC Storage Managed Service[14].

3.2.3.3 Επικοινωνίες

Καθώς η ανάγκη για εγγυημένη ποιότητα υπηρεσίας (QoS) αυξάνεται για τα συστήματα cloud , η επικοινωνία αποτελεί ένα ζωτικής σημασίας μέρος της υποδομής του cloud. Τα συστήματα cloud είναι υποχρεωμένα να παρέχουν κάποιες δυνατότητες επικοινωνίας οι όποιες είναι υπηρεσιοστραφείς (service-oriented), διαμορφώσιμες, προγραμματιζόμενες, προβλέψιμες και αξιόπιστες. Βαδίζοντας προς αυτόν τον στόχο, η ιδέα της «Επικοινωνίας ως Υπηρεσία» (Communication As A Service-CaaS) αναδείχτηκε για να υποστηρίξει τέτοιου είδους απαιτήσεις, καθώς και ασφάλεια δικτύου, εγγυημένη καθυστέρηση μηνύματος, κρυπτογράφηση επικοινωνίας και παρακολούθηση του δικτύου. Ένα πρόσφατο παράδειγμα συστήματος που ανήκει στο CaaS είναι το Connected Service Framework[15] (CSF) της Microsoft. Τα συστήματα τηλεφωνίας VOIP, τα συστήματα τηλεσυνδιασκεψης και βινετοσυνδιασκεψης καθώς και τα συστήματα instant-messaging είναι υποψήφιες υπηρεσίες cloud οι όποιες μπορούν να συντεθούν από CaaS και μπορούν με τη σειρά τους να παρέχουν σύνθετες λύσεις cloud υπηρεσιών για άλλες κοινές υπηρεσίες.

3.2.3.4 Kernel Λογισμικού

Το συγκεκριμένο στρώμα του cloud παρέχει τη βασική διαχείριση λογισμικού για τους φυσικούς servers που συνθέτουν το cloud. Τα software kernels σε αυτό το στρώμα μπορούν να υλοποιηθούν ως ένα OS kernel, hypervisor, virtual machine monitor και/ή clustering middleware. Συνήθως οι εφαρμογές grid computing αναπτύσσονται και εκτελούνται σε αυτό το στρώμα σε πολλές συστάδες διασυνδεμένων μηχανημάτων. Όμως λόγω της απουσίας

εικονοποίησης στο grid computing οι εργασίες είναι στενά συνδεδεμένες με την υποδομή υλικού, και η παροχή σημείων έλεγχου και εξισορρόπησης φόρτου είναι μια πολύπλοκη διεργασία.

Τα 2 πιο επιτυχημένα grid middleware τα οποία χρησιμοποιούν τους φυσικούς πόρους για να παρέχουν ένα επιτυχημένο περιβάλλον ανάπτυξης για Grid εφαρμογές είναι αναμφισβήτητα το Globus[16] και το Condor[17]. Το πεδίο ερευνάς στο grid computing είναι τεράστιο και πολλά σχέδια τα όποια αναπτύχτηκαν με βάση το Grid χρησιμοποιούνται τώρα στο Cloud computing. Όμως επιπρόσθετη ερεύνα σχετικά με το grid computing μπορεί να ενσωματωθεί και στην ερεύνα για το cloud. Για παράδειγμα τα μικροοικονομικά μοντέλα του grid computing είναι ίσως τα αρχικά μοντέλα για τη μελέτη της τιμολόγησης, της μέτρησης και τις ισορροπίας μεταξύ ζήτησης-προσφοράς στον τομέα του cloud computing.

3.2.3.5 Hardware και Firmware

Το χαμηλότερο στρώμα της οντολογίας του cloud είναι το αυτό κάθε αυτό φυσικό υλικό και διακόπτες που σχηματίζουν τη ραχοκοκαλιά του cloud. Με αυτό το σκεπτικό οι Χρήστες αυτού το στρώματος είναι συνήθως μεγάλες επιχειρήσεις και που έχουν μεγάλες απαιτήσεις σε τεχνολογία πληροφορίας η όποιες χρειάζονται υπομίσθωση Υλικού ως Υπηρεσία (Hardware As A Service-HaaS). Για αυτό το σκοπό ο πάροχος του HaaS χειρίζεται, διαχειρίζεται και αναβαθμίζει το υλικό εκ μέρους των πελατών του για όσο χρόνο διαρκεί η υπομίσθωση. Αυτό το μοντέλο έχει πολλά πλεονεκτήματα για τις εταιρίες που το χρησιμοποιούν, αφού δεν χρειάζεται να επενδύσουν στην κατασκευή και διαχείριση κάποιου ιδιοκτήτου data center. Εν τω μεταξύ οι πάροχοι HaaS έχουν την τεχνογνωσία καθώς και την αποδοτική υποδομή για να στεγάσουν τα συστήματα. Ένα από τα πιο πρώιμα παραδείγματα HaaS είναι το συμβόλαιο υπομίσθωσης της Morgan Stanley με την IBM το 2004. Τα SLAs σε αυτό το μοντέλο είναι πιο αυστηρά, αφού οι επιχειρήσεις έχουν προκαθορισμένο φόρτο εργασίας τα χαρακτηριστικά του όποιου επιβάλλουν αυστηρές απαιτήσεις απόδοσης.

Cloud Layer	Examples of Commercial Cloud Systems
Cloud Application Layer	Google Apps and Salesforce Customer Relation Management (CRM) system
Cloud Software Environment	Google App Engine and Salesforce Apex System
Cloud Software Infrastructure	*Computational Resources*: Amazon's EC2, Enomalism Elastic Cloud.
	Storage: Amazon's S3, EMC Storage Managed Service.
	Communication: Microsoft Connected Service Framework (CSF).
Software Kernel	Grid and Cluster Computing Systems like Globus and Condor.
Firmware / Hardware	IBM-Morgan Stanley's Computing Sublease, and IBM's Kittyhawk Project.

Πίνακας 3.1: Παραδείγματα σύγχρονων συστημάτων Cloud Computing και η κατάταξή τους σε κάθε στρώμα της οντολογίας του cloud. [10]

3.3 Βιβλιογραφία Κεφαλαίου

[1] Lamia Youseff, Maria Butrico Dilma Da Silva : *Toward a Unified Ontology of Cloud Computing*

[2] M. P. Papazoglou και W.-J. Heuvel, *"Service oriented architectures: approaches, technologies and research issues"*

[3] Salesforce.com. http://salesforce.com

[4] "GOOGLE App Engine," http://code.google.com/appengine.

[5] "Apex: Salesforce on-demand programming language and framework," http://developer.force.com/.

[6] "EMC Managed Storage Service," http://www.emc.com/.

[7] S. Ghemawat, H. Gobioff, και S.-T. Leung, "The google file system"

[8] "Amazon elastic compute cloud," http://aws.amazon.com/ec2/.

[9] "Microsoft Connected Service Framework, http://www.microsoft.com/serviceproviders/solutions/connectedservicesframework.mspx

[10] I. Foster and C. Kesselman, "Globus: A metacomputing infrastructure toolkit," *International Journal of Supercomputer Applications*, 1997.

[11] T. Tannenbaum and M. Litzkow, "The condor distributed processing system," *Dr. Dobbs Journal*, February 1995.

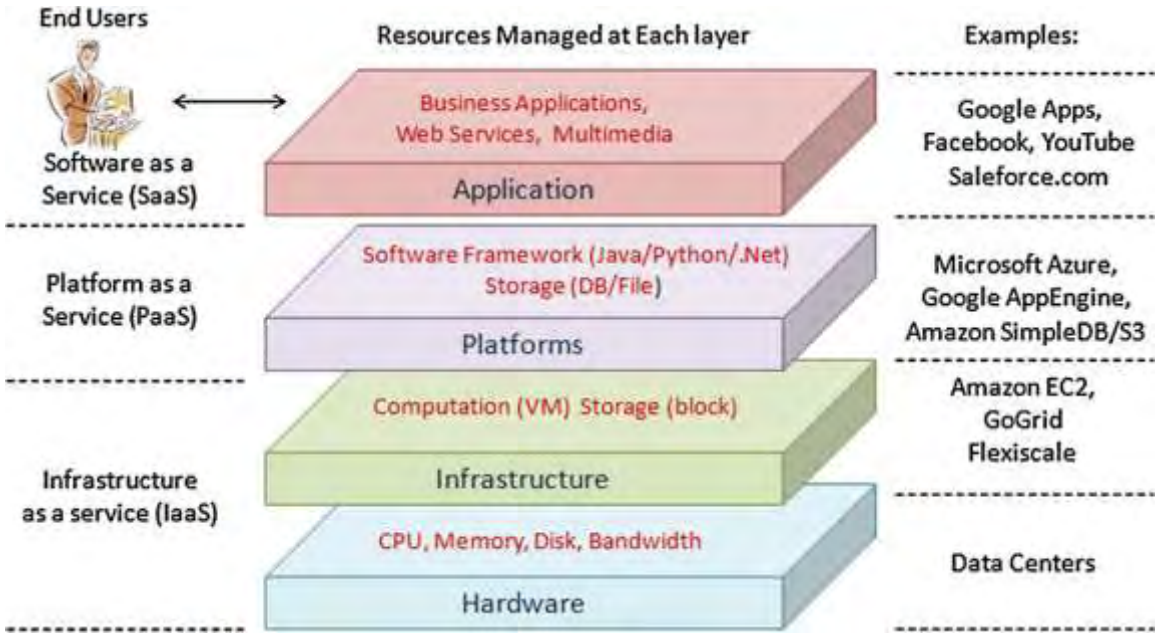
Κεφάλαιο 4

Υπηρεσίες Cloud Computing

Περιεχόμενα

4.1 Εισαγωγή

Οι κυριότερες διαφορές μεταξύ των υπηρεσιών cloud computing σχετίζονται με τον τύπο της υπηρεσίας που προσφέρεται[18]. Για παράδειγμα , χώρος αποθήκευσης, υπολογιστική δύναμη, πλατφόρμες για ανάπτυξη λογισμικού η On-line εφαρμογές όπως το e-mail και εργαλεία αναλύσεων. Βασιζόμενο σε αυτές τις διαφορές το *National Institute of Standards and Technology* (NIST)[19] έχει προτείνει 3 διαφορετικές κατηγορίες υπηρεσιών cloud computing.



Εικόνα 4.1: Οι τρεις κυριότερες κατηγορίες cloud υπηρεσιών. [18]

4.2 Υποδομή ως Υπηρεσία (Infrastructure As A Service-IaaS)

Οι υπηρεσίες υποδομής του cloud τυπικά προσφέρουν πλατφόρμες εικονοποίησης, οι οποίες είναι εξέλιξη του εικονικού ιδιωτικού (virtual-private) server. Οι πελάτες αγοράζουν τους πόρους αντί να εγκαθιστούν servers, λογισμικό και χώρο για το data center και χρεώνονται με βάση τους πόρους που κατανάλωσαν. Αναπτύσσουν το δικό τους λογισμικό σε εικονικές μηχανές ενώ ταυτόχρονα το ελέγχουν και το διαχειρίζονται. Τα εικονικά μηχανήματα μπορούν να νοικιαστούν για όσο καιρό είναι απαραίτητο, ακόμη και για μια ώρα. Ο αριθμός των εικονικών μηχανημάτων μπορεί να αυξομειώνεται δυναμικά ανάλογα με τις απαιτήσεις του καταναλωτή. Η χρέωση είναι βασισμένη σε αυτόν τον αριθμό, καθώς και τη διάρκεια και

τυχόν επιπρόσθετες υπηρεσίες που χρησιμοποιήθηκαν όπως περισσότερος χώρος αποθήκευσης. Οι πάροχοι συνήθως έχουν data centers σε πολλαπλές τοποθεσίες ώστε να προσφέρουν γρήγορη πρόσβαση από οποιοδήποτε σημείο του κόσμου. Οι διαπαφές web επιτρέπουν τον έλεγχο της cloud υπηρεσίας.

Μερικοί πάροχοι δίνουν τη δυνατότητα στους πελάτες τους να συνδέουν τα εικονικά μηχανήματα στο τοπικό δίκτυο της εταιρίας μέσω VPN (Virtual Private Network), ώστε να κάνουν το δίκτυο τους να μοιάζει με μια μεγάλη κλιμακούμενη υποδομή IT. Αυτού του είδους οι λύσεις ονομάζονται hybrid clouds καθώς συνδέουν το εσωτερικό, ιδιωτικό δίκτυο της εταιρίας/πελάτη με το δημόσιο δίκτυο του παρόχου της IaaS υπηρεσίας.

Ένας πρωτοπόρος στην εικονοποίηση και στην παροχή υπολογιστικής δύναμης είναι η Amazon. Το Elastic Cloud της Amazon (EC2) είναι μια από τις ποιο ευρέως χρησιμοποιούμενες πλατφόρμες υποδομών.

Οι υπηρεσίες on-line αποθήκευσης και backup βρίσκονται επίσης στην κατηγορία IaaS. Όπως οι περισσότερες πλατφόρμες εικονοποίησης, υπάρχουν αρκετές λύσεις σχετικά με την αποθήκευση δεδομένων που απευθύνονται σε μεγάλες εταιρίες, υπάρχουν όμως και ειδικές υπηρεσίες αποθήκευσης που μπορούν να χρησιμοποιηθούν και ατομικά. Οι υπηρεσίες που χρησιμοποιούν οι μεγάλες εταιρίες κυμαίνονται από προσωρινές μέχρι μόνιμες και από επιπρόσθετο αποθηκευτικό χώρο στη γενική του μορφή έως υπηρεσίες που έχουν ως στόχο την αποθήκευση βάσεων δεδομένων, οι οποίες χρεώνονται όχι μόνο για το χώρο αποθήκευσης που χρησιμοποιείται αλλά και για τον αριθμό των ερωτήσεων προς τη βάση.

Level	Found characteristics
1. Service	IaaS
2. License	Proprietary base framework
3. User group	Corporate use
4. Payment	Pay-per-use
5. Agreements	SLA (incl. compensation)
6. Security	PKI
7. Standards	Public API
8. Openness	Moderate
a. Supported OSs	Non-preconf.or prec. with Linux, Windows Server or OpenSolaris
b. Supported applications/ frameworks	Non-prec. or prec. with databases e.g. MySQL, Oracle; batch processing, e.g. Hadoop; web hosting e.g. Apache HTTP, IIS/Asp.Net
c. Dev. tools	Command-line tools, developer API
d. Virtualization	Xen

Πίνακας 4.1: Τα χαρακτηριστικά του EC2 της Amazon. [18]

4.3 Πλατφόρμα ως Υπηρεσία (Platform As A Service-PaaS)

Οι πάροχοι PaaS υπηρεσιών προσφέρουν μια υψηλού επιπέδου υποδομή λογισμικού, στην όποια οι πελάτες μπορούν να αναπτύξουν λεπτομερέστερες κλάσεις εφαρμογών και υπηρεσίες χρησιμοποιώντας τα εργαλεία, τα περιβάλλοντα και τις γλώσσες προγραμματισμού που υποστηρίζονται από τον πάροχο. Οι παροχές περιλαμβάνουν τη χρήση των βαθύτερων υποδομών όπως servers, δίκτυα, αποθηκευτικούς χώρους ή λειτουργικά συστήματα, πάνω στα οποία οι χρήστες δεν έχουν δικαίωμα έλεγχου καθώς βρίσκονται σε χαμηλότερο επίπεδο από αυτό της πλατφόρμας.

Οι υπηρεσίες πλατφόρμας είναι περισσότερο στοχευόμενες σε συγκεκριμένα πεδία, όπως η ανάπτυξη εφαρμογών web, και είναι άμεσα εξαρτημένες από την γλωσσά προγραμματισμού. Οι πελάτες περνούν ένα ξεχωριστό περιβάλλον για να ελέγξουν και να αναπτύξουν η να εγκαταστήσουν μόνιμα τις εφαρμογές τους. Το App Engine της Google είναι στοχευόμενο στις παραδοσιακές εφαρμογές web προσφέροντας ένα περιβάλλον Java η Python. Στην πλατφόρμα Azure της Microsoft οι εφαρμογές αναπτύσσονται με τη βοήθεια .NET βιβλιοθηκών.

Level	Found characteristics
1. Service	PaaS
2. License	Proprietary
3. User group	Corporate use
4. Payment	Pay-per-use, free promotion offers
5. Agreements	SLA
6. Security	Unknown
7. Standards	Supports SOAP and REST API [10]
8. Openness	Basic
a. Supported languages/env.	.Net, PHP
b. Supported OSs	Windows
c. Supported applications/ frameworks	Live Services, MS .NET Services, MS SQL Services, MS SharePoint, and MS Dynamics CRM Services

Πίνακας 4.2: Τα χαρακτηριστικά του Azure της Microsoft. [18]

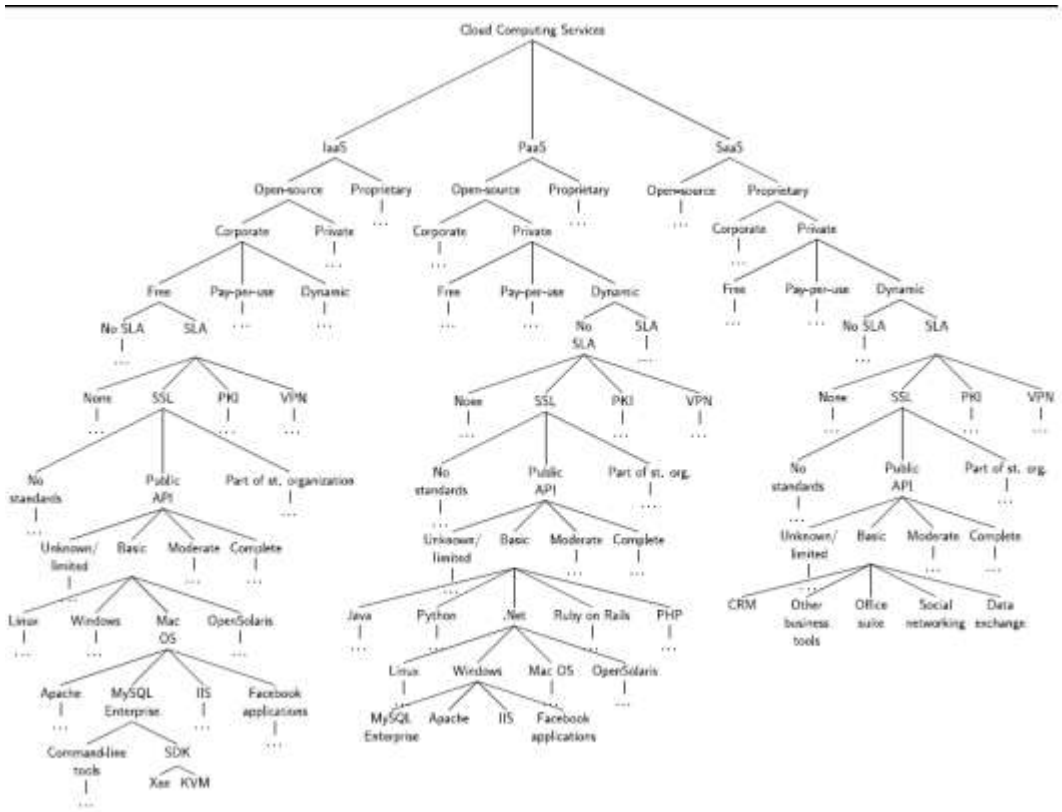
Level	Found characteristics
1. Service	SaaS
2. License	Proprietary
3. User group	Corporate and private use
4. Payment	Free (private use), 50$ per account per year (corporate use)
5. Agreements	No SLA (private); SLA (corporate)
6. Security	HTTPS/SSL
7. Standards	No standards (Single-sign-on API for corporate use)
8. Openness	Moderate
a. Domain	Office suite, incl. email, calender, etc.

Πίνακας 4.3: Τα χαρακτηριστικά του Google Apps. [18]

4.4 Λογισμικό ως Υπηρεσία (Software As A Service-SaaS)

Οι υπηρεσίες λογισμικού τυπικά παρέχουν συγκεκριμένες προϋπάρχουσες εφαρμογές οι οποίες εκτελούνται σε μια υποδομή του cloud. Μια πολύ γνωστή SaaS υπηρεσία είναι το web-based e-mail. Οι περισσότερες υπηρεσίες παροχής λογισμικού cloud είναι web-based εφαρμογές, οι οποίες μπορούν αν προσπελαστούν από ποικίλες συσκευές client μέσω μιας thin client[20] διεπαφής, όπως ένας web browser. Οι πελάτες αυτών των υπηρεσιών δεν διαχειρίζονται και δεν ελέγχουν την βαθύτερη υποδομή ή την πλατφόρμα καθώς υπάρχουν περιορισμένες δυνατότητες διαμόρφωσης από την πλευρά του χρήστη.

Μια υπηρεσία παροχής λογισμικού cloud για εταιρική χρήση είναι το SalesForce.com το οποίο παρέχει εργαλεία για την ανάλυση των επιχειρήσεων και την διαχείριση των σχέσεων των πελατών. Πολλές δημοφιλείς υπηρεσίες παροχής λογισμικού για ιδιωτική χρήση είναι επίσης το Google Apps[21], που περιλαμβάνει εφαρμογές όπως ημερολόγια, διαχείριση επαφών, e-mail, chat λειτουργιές καθώς και το Google Docs, ένα πακέτο εφαρμογών που επιτρέπει πρόσβαση και διαμοιρασμό εγγράφων .



Εικόνα 4.2: Το δέντρο των υπηρεσιών του Cloud Computing. [18]

Εικόνα 4.3: Παραδείγματα Cloud Computing Υπηρεσιών. [18]

4.5 Κύρια χαρακτηριστικά των Cloud Υπηρεσιών

Όπως συζητήθηκε παραπάνω υπάρχουν πολλές υπηρεσίες cloud computing που διαφέρουν μεταξύ τους κυρίως λογά του είδους της υπηρεσίας που προσφέρουν, μοιράζονται όμως αρκετά κοινά χαρακτηριστικά.

4.5.1 Τύπος Άδειας Χρήσης

Οι περισσότερες υπηρεσίες cloud computing χρησιμοποιούν ιδιόκτητο λογισμικό και άδειες χρήσης (licenses). Όμως αρκετοί πάροχοι could υπηρεσιών χρησιμοποιούν open-source λογισμικό και πλατφόρμες. Το Amazon χρησιμοποιεί την open-source τεχνολογία Xen[22] ενώ το η παροχή PaaS της Google έχει αναπτυχτεί γύρω από την open-source γλωσσά προγραμματισμού Python, παρόλα αυτά ο πυρήνας των cloud computing υπηρεσιών και οι επιπρόσθετες υπηρεσίες έχουν κρατηθεί «κλειστές» (closed-source). Μεγάλο ποσοστό λογισμικού που χρησιμοποιείται για τον έλεγχο του cloud είναι βασισμένο στην open-source λογική καθώς και μικρότερες υπηρεσίες cloud computing , αφού οι πιο αδύναμοι «παίκτες» δεν έχουν την δυνατότητα και την επιρροή να «σπρώξουν» ιδιόκτητο λογισμικό στην αγορά.

Ο τύπος του license παίζει επίσης ρολό όταν προσφέρονται υπηρεσίες πλατφόρμας και υποδομής. Οι πάροχοι IaaS δεν αντιμετωπίζουν προβλήματα με τις άδειες λογισμικού όταν νοικιάζουν τους εικονικούς servers τους χωρίς κάποιο λειτουργικό σύστημα εγκατεστημένο. Όταν όμως συμπεριλαμβάνουν λειτουργικά συστήματα και πακέτα εφαρμογών μπορούν να

δημιουργηθούν πιθανά προβλήματα σχετικά με το πως θα πρέπει ένας πελάτης να χρεωθεί όταν χρησιμοποιεί την υπηρεσία για μικρό χρονικό διάστημα.

4.5.2 Απευθυνόμενες ομάδες χρηστών

Μερικές υπηρεσίες cloud computing διαφοροποιούνται ανάμεσα στην εταιρική και την ιδιωτική χρήση. Οι περισσότερες παροχές IaaS και PaaS είναι προσανατολισμένες στις εταιρίες ενώ οι παροχές SaaS απευθύνονται σε εταιρίες, ιδιώτες η και στα 2, όπως το Google Apps, κάτι όμως που δεν εμποδίζει την αγορά υπηρεσιών που προορίζονται για εταιρίες από ιδιώτες.

Ένας επιπλέον διαχωρισμός μεταξύ στον εταιρικό και ιδιώτη χρήστη μπορεί γίνει ανάμεσα στους κινητούς και σταθερούς χρήστες. Οι κινητοί χρήστες προσπελαύνουν της cloud computing υπηρεσίες τους από οπουδήποτε και με οποιαδήποτε συσκευή, ενώ οι σταθεροί χρήστες βρίσκονται σε συγκεκριμένο σημείο και συνήθως χρησιμοποιούν την ιδία συσκευή για να συνδεθούν στην υπηρεσία.

4.5.3 Ασφάλεια και Ιδιοτικότητα

Η ασφάλεια και η ιδιοτικότητα είναι σημαντικά χαρακτηριστικά, ειδικά όταν ευαίσθητα δεδομένα βρίσκονται αποθηκευμένα στους cloud servers. Η απώλεια η διαρροή δεδομένων μπορεί όχι μόνο να προκαλέσει μείωση των κερδών αλλά και να επιφέρει νομικές κυρώσεις. Οι νομοί της Ε.Ε. για την προστασία των δεδομένων για παράδειγμα δηλώνουν, ότι τα δεδομένα μπορεί να αποθηκεύονται σε χώρες με επαρκή προστασία και ότι για συγκεκριμένα δεδομένα είναι απαραίτητο να είναι γνωστή η φυσική τοποθεσία τους, κάτι το όποιο δεν είναι πάντα δυνατό όταν χρησιμοποιούνται τεχνολογίες cloud computing. Λόγω της έλλειψης προτύπων, η ασφάλεια του cloud, ιδιοτικότητα και δικαιώματα ιδιοκτησίας των δεδομένων προσεγγίζονται διαφορετικά από κάθε πάροχο.

Για αυτούς τους λόγους ,η κρυπτογράφηση και η αυθεντικοποίηση πρέπει να χρησιμοποιούνται για όλες τις υπηρεσίες cloud. Η κρυπτογράφηση μπορεί να προφυλάξει για παράδειγμα από τη υποκλοπή ανάμεσα σε εικονικές μηχανές σε επίπεδο δικτύου.

Οι περισσότερες cloud υπηρεσίες μπορούν να προσπελαστούν από ένα web-browser, και το πρότυπο HTTP χρησιμοποιείται για τη σύνδεση στο cloud. Για την παροχή κρυπτογράφησης και ασφαλούς ταυτοποίησης του server χρησιμοποιείται το SSL/TLS (Secure Socket Layer/Transport Layer Security) πρωτόκολλο. Επιπλέον προσεγγίσεις με σκοπό την ταυτοποίηση και εξουσιοδότηση περιλαμβάνουν τα PKI (Public Key Infrastructure) και X.509 SSL πιστοποιητικά[23]. Για παράδειγμα το EC2 της Amazon χρησιμοποιεί δημοσιά κλειδιά, ενώ για hybrid clouds χρησιμοποιούνται VPNs.

4.5.4 Συστήματα Πληρωμών

Το σύστημα πληρωμής που χρησιμοποιείται για το cloud computing είναι ένα από τα χαρακτηριστικά που το ξεχωρίζουν. Η κυρία διαφορά από την παραδοσιακή μορφή χρέωσης είναι ότι οι υπηρεσίες cloud χρεώνονται με βάση τη δυναμική τους χρήση, αντί για την χρέωση ενός σταθερού πόσου ανά μηνά η ανά χρόνο. Οι πόροι που μετρούνται μπορεί να είναι ο αριθμός των εικονικών συσκευών , το μέγεθος του χώρου αποθήκευσης, το bandwidth, ο χρόνος υπολογισμού, οι πόροι που απαιτήθηκαν (RAM/CPU), αλλά και ως και συνδυασμός όλων αυτών.

Οι υπηρεσίες cloud computing μπορεί να χρησιμοποιούν διαφορετικές μεθόδους πληρωμής ανάλογα με το είδος των πόρων που χρησιμοποιούνται. Το πιο συχνά χρησιμοποιούμενο μοντέλο τιμολόγησης είναι το pay-per-use[24], στο οποίο οι μονάδες πόρων ή μονάδες πόρων ανά χρόνο αντιστοιχίζονται με μια σταθερή τιμή. Κάποιες υπηρεσίες cloud παρέχονται δωρεάν όπως το Google Docs και το Google App Engine. Οι πελάτες του EC2 της Amazon χρεώνονται μηνιαίως για τους πόρους που χρησιμοποίησαν συμφώνα με το μοντέλο pay-per-use.

4.5.5 Προτυποποίηση

Η τυποποίηση αναφέρεται στην χρήση κοινών APIs και αρχιτεκτονικών καθώς και τεχνικών προτύπων. Αυτά τα πρότυπα μπορούν είτε να εγκριθούν και να διατηρηθούν από έναν οργανισμό όπως η ANSI ή το ISO, ή μπορούν υλοποιήσουν μια κοινώς χρησιμοποιούμενη , συνήθη διεπαφή[25] (defector standards).

Μέχρι σήμερα δεν υπάρχουν επαρκώς ορισμένα και ευρέως αποδεκτά πρότυπα παρόλο που κάτι τέτοιο θα ωφελούσε τους πελάτες του cloud computing και τους προγραμματιστές του. Η ύπαρξη προτύπων θα προκαλούσε την βελτίωση της διαλειτουργικότητας και θα επέτρεπε μια πιθανή εξατομίκευση λόγω της τεχνολογικής διαφάνειας.

Η τυποποίηση μπορεί να εφαρμοστεί σε αρχιτεκτονικές cloud, πρωτόκολλα cloud, προσδιοριστικά υπηρεσιών cloud , γλώσσες περιγραφής καθώς και SLAs. Υπάρχουν πολλοί οργανισμοί που επιχειρούν να δημιουργήσουν τέτοια πρότυπα όπως το Cloud Computing Interoperability Forum, το οποίο προσπαθεί να αναπτύξει ένα πλαίσιο που να επιτρέπει 2 η περισσότερα clouds να ανταλλάσουν πληροφορίες . Στους σπόνσορες του προγράμματος περιλαμβάνονται η IBM, Sun Microsystems, Intel και Cisco. Το Open Cloud Standards Incubator της DTMF[26] στοχεύει επίσης στη δημιουργία προτύπων για την αλληλεπίδραση ανάμεσα σε 2 cloud.

4.5.6 Επίσημες Συμφωνίες

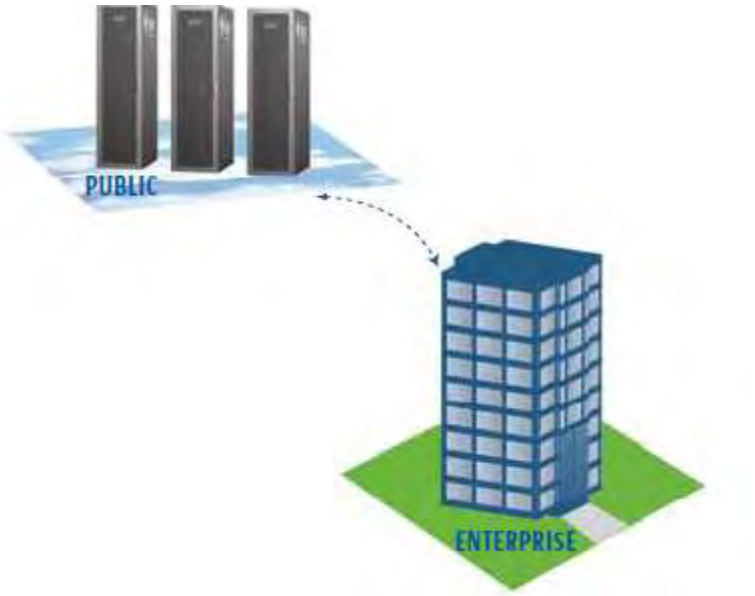
Οι ποιο ευρέως χρησιμοποιούμενες επίσημες συμφωνίες είναι τα SLAs τα όποια καθορίζουν επίσημα τι επίπεδο υπηρεσιών πρέπει να αναμένει ο πελάτης, και τα όποια θα πρέπει να αντιμετωπίζουν την καθυστέρηση (latency) και το QoS. Τυπικά τα SLAs περιλαμβάνουν τεχνικές προδιαγραφές από μετρά όπως το uptime η το Round Trip Time (RTT). Τα περισσότερα SLAs δηλώνουν επίσης τι ποσό αποζημίωσης μπορεί να περιμένει ο πελάτης σε περίπτωση αποτυχίας.

4.6 Τύποι Cloud

Υπάρχουν πολλά στοιχειά που πρέπει να λυθούν ειπούν κατά την μεταφορά μιας εταιρικής εφαρμογής στο περιβάλλον cloud. Για παράδειγμα, κάποιοι πάροχοι υπηρεσιών ενδιαφέρονται περισσότερο για την μείωση του λειτουργικού κόστους, ενώ κάποιοι άλλοι προτιμούν την αυξημένη αξιοπιστία και ασφάλεια. Με το ίδιο σκεπτικό υπάρχουν διαφορετικά ειδή clouds[27] κάθε ένα από τα όποια με πλεονεκτήματα και μειονεκτήματα.

- ***Δημοσιά (Public) Clouds***: Τα public clouds εκτελούνται από τρίτους, και εφαρμογές από διαφορετικούς πελάτες είναι πιθανό να συνυπάρχουν στους ιδίους servers, συστήματα αποθήκευσης και δίκτυα. Τα public clouds συνήθως φιλοξενούνται μακριά από τις εγκαταστάσεις των πελατών και παρέχουν έναν τρόπο μείωσης του ρίσκου και του κόστους από την πλευρά του πελάτη, παρέχοντας μια ευέλικτη, και πολλές φόρες προσωρινή επέκταση στην υποδομή της κάθε επιχείρησης. Ένα από τα πλεονεκτήματα του public cloud είναι ότι μπορεί να έχει πολύ μεγαλύτερο μέγεθος από ότι κάποιο private cloud μιας εταιρίας, προσφέροντας έτσι την ευχέρεια στους χρήστες του να αυξομειώνουν το μέγεθος του ανάλογα με τις απαιτήσεις της συγκεκριμένης χρονικής στιγμής, μεταφέροντας έτσι το επιχειρηματικό ρίσκο για την αγορά υποδομών από την επιχείρηση στον πάροχο της cloud υπηρεσίας. Τα μέρη ενός public cloud μπορούν να διαχωριστούν για την αποκλειστική χρήση από έναν και μόνο πελάτη, δημιουργώντας έτσι ένα εικονικό ιδιωτικό datacenter. Αντί να περιορίζεται στην εγκατάσταση στιγμιότυπων εικονικών μηχανών, ένα εικονικό, ιδιωτικό datacenter προσφέρει στους πελάτες μεγαλύτερη

"ορατότητα" μέσα στην υποδομή του, δηλαδή επιτρέπει στους πελάτες να χειρίζονται, περά από μια εικονική μηχανή, τους servers, συστήματα αποθήκευσης, συσκευές δικτύου, και την τοπολογία του δικτύου. Ακόμα η δημιουργία ενός εικονικού ιδιωτικού datacenter με όλα τα στοιχειά του να στεγάζονται στην ιδία εγκατάσταση βοηθού στη μείωση του προβλήματος της τοπικότητας των δεδομένων καθώς το bandwidth είναι πολύ μεγαλύτερο και συνήθως δωρεάν όταν συνδέονται πόροι στην ιδία εγκατάσταση. Παρόλα αυτά όμως τα public clouds υστερούν στον πιο εξειδικευμένο έλεγχο των δεδομένων, των δικτύων και των ρυθμίσεων ασφάλειας του cloud, κάτι που παρεμποδίζει την αποτελεσματικότητα τους σε πολλά επιχειρηματικά σενάρια.



Εικόνα 4.4: Ένα δημόσιο (public) cloud παρέχει υπηρεσίες σε πολλαπλούς πελάτες και συνήθως αναπτύσσεται σε μια εγκατάσταση που περιέχει και άλλες οντότητες (colocation facility). [27]

- ***Ιδιωτικά (Private) Clouds:*** Τα Private clouds δημιουργούνται για την αποκλειστική χρήση από έναν πελάτη, παρέχοντας τον μέγιστο έλεγχο στα δεδομένα, την ασφάλεια και το QoS. Η εταιρία/πελάτης έχει στην ιδιοκτησία της την απαραίτητη υποδομή και έχει τον έλεγχο για τον τρόπο με τον όποιο οι εφαρμογές αναπτύσσονται πάνω της. Τα Private Clouds μπορούν να αναπτυχτούν και να διαχειριστούν από το προσωπικό της ίδιας της εταιρίας η από κάποιον πάροχο cloud. Σε αυτό το μοντέλο "ιδιωτικής φιλοξενίας" μια εταιρία παροχής μπορεί να εγκαταστήσει, να ρυθμίσει και να χειριστεί την

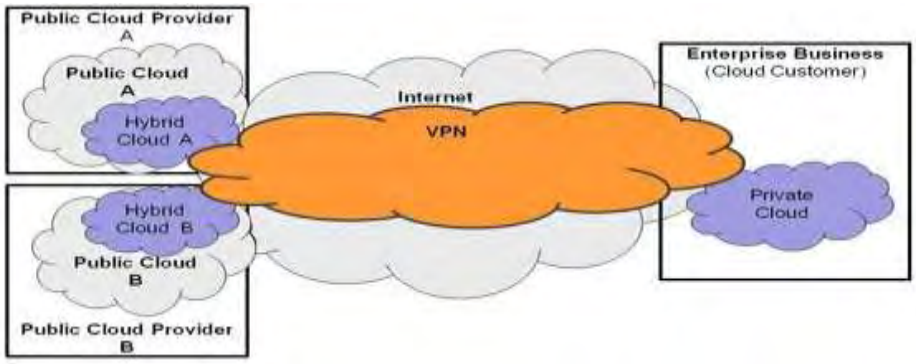
υποδομή του Private cloud μέσα στο εταιρικό datacenter του πελάτη, δίνοντας έτσι στις εταιρίες/πελάτες ένα υψηλότερο επίπεδο χρησιμοποίησης των πόρων του cloud και ταυτόχρονα παρέχοντας την απαιτουμένη τεχνογνωσία για την εγκατάσταση και λειτουργία του περιβάλλοντος. Παρόλα αυτά όμως τα Private Clouds συχνά θεωρούνται παρόμοια με τα παραδοσιακά, ιδιόκτητα server farms, ενώ δεν παρέχουν πλεονεκτήματα όπως την μειωμένη εκ των πρότερων κεφαλαιουχική δαπάνη.

Εικόνα 4.5: Τα ιδιωτικά clouds μπορούν να φιλοξενηθούν σε μια colocation εγκατάσταση, η σε ένα εταιρικό κάντρο δεδομένων. Μπορούν να υποστηριχτούν από την εταιρία, τον πάροχο του cloud, ή από κάποιο τρίτο πρόσωπο. [27]

- ***Υβριδικά (Hybrid) Clouds:*** Τα Hybrid Clouds συνδυάζουν τα μοντέλα των Public και Private clouds προσπαθώντας να αντιμετωπίσουν τα μειονεκτήματα του κάθε μοντέλου ξεχωριστά. Σε ένα hybrid cloud, ένα μέρος της υπηρεσίας εκτελείται σε private clouds ενώ το υπόλοιπο εκτελείται σε Public clouds. Η ικανότητα αύξησης της απόδοσης ενός Private Cloud χρησιμοποιώντας τους πόρους ενός Public cloud μπορεί να χρησιμοποιηθεί για τη διατήρηση του επιπέδου της υπηρεσίας με περίπτωσης γρήγορης διακύμανσης του φόρτου εργασίας. Αυτό παρατηρείται πιο συχνά με τη χρήση clouds αποθήκευσης για την υποστήριξη Web 2.0 εφαρμογών.. Το μειονέκτημα τους είναι η αυξημένη πολυπλοκότητα στη σχεδίαση τους, καθώς πρέπει να προσδιοριστεί ο καλύτερος διαμοιρασμός των τμημάτων του ανάμεσα σε public και private clouds.

Εικόνα 4.6: Τα υβριδικά clouds συνδυάζουν τα μοντέλα των δημοσίων και των ιδιωτικών clouds, και μπορούν να είναι ιδιαίτερα αποδοτικά όταν και τα δυο είδη cloud στεγάζονται στην ίδια εγκατάσταση. [27]

- ***Εικονικά Ιδιωτικά (Virtual Private) Cloud:*** Μια εναλλακτική λύση για την αντιμετώπιση των περιορισμών των public και private clouds είναι το VPC, το όποιο είναι στην ουσία μια πλατφόρμα που εκτελείται πάνω από τα public clouds. Η μεγαλύτερη διαφορά είναι ότι το VPC αξιοποιεί την τεχνολογία VPN η όποια επιτρέπει στους παρόχους υπηρεσιών να σχεδιάζουν την δική τους τοπολογία και ρυθμίσεις ασφάλειας, όπως τους κανόνες ενός firewall. Το VPC είναι στην ουσία ένα πιο ολοκληρωμένο σχέδιο καθώς δεν ικανοποιεί μόνο servers και εφαρμογές αλλά και το δίκτυο επικοινωνίας που βρίσκεται από κάτω τους.



Εικόνα 4.7: Η επικοινωνία μεταξύ δημοσίων και ιδιωτικών clouds γίνεται μέσω VPN.

4.7 Εμπορικά Προϊόντα

Τρία από τα σημαντικότερα και πιο ευρέως διαδεδομένα εμπορικά προϊόντα του Cloud Computing είναι το EC2 της Amazon, η πλατφόρμα Windows Azure της Microsoft και το App Engine της Google.

4.7.1 Amazon EC2

Το Amazon Web Services[28] είναι ένα σύνολο από υπηρεσίες cloud που παρέχουν υπολογισμό βασισμένο στο cloud, αποθηκευτικά μέσα και άλλες λειτουργιές που επιτρέπουν σε εταιρίες/οργανισμούς αλλά και σε μεμονωμένα άτομα να εγκαταστήσουν εφαρμογές και υπηρεσίες σε μια κατ'απαίτηση βάση αλλά και σε πολύ χαμηλές τιμές. Οι υπηρεσίες του Amazon Web Services είναι προσβάσιμες πάνω από HTTP και κάνοντας χρήση των πρωτοκόλλων REST και SOAP.

Το Amazon Elastic Compute Cloud (EC2)[29] επιτρέπει τους χρήστες του cloud να τρέξουν και να διαχειριστούν στιγμιότυπα εξυπηρετητών στα data centers χρησιμοποιώντας APIs η κάποια αλλά διαθέσιμα εργαλεία. Τα στιγμιότυπα του EC2 είναι εικονικές μηχανές που τρέχουν πάνω από την μηχανή εικονοποίησης Xen[30]. Αφού ένα στιγμιότυπο εξυπηρετητή δημιουργηθεί και ξεκινήσει η εκτέλεση του, ένας χρήστης μπορεί να «ανεβάσει» κάποιο λογισμικό και να κάνει αλλαγές σε αυτό. Μόλις οι αλλαγές ολοκληρωθούν μπορούν να συγκεντρωθούν (bundle) σχηματίζοντας ένα νέο στιγμιότυπο μηχανής, το οποίο στην ουσία αποτελεί ένα πανομοιότυπο αντίγραφο που μπορεί να εκτελεστεί ανά πασά στιγμή. Οι χρήστες έχουν σχεδόν εξολοκλήρου έλεγχο της στοίβας λογισμικού στα στιγμιότυπα του EC2 τα οποία «φαίνονται» σε αυτούς ως ένα στρώμα υλικού. Από την άλλη μεριά αυτό το χαρακτηριστικό προκαλεί δυσκολίες στην Amazon, σχετικές με την προσφορά πόρων που κλιμακώνονται αυτόματα.

Το EC2 παρέχει την ικανότητα τοποθέτησης στιγμιότυπων σε πολλαπλές τοποθεσίες. Οι τοποθεσίες του EC2 διαχωρίζονται σε Περιφέρειες (Regions) και σε Ζώνες Διαθεσιμότητας (Availability Zones). Οι περιφέρειες αποτελούνται από μια η περισσότερες Ζώνες Διαθεσιμότητας και είναι γεωγραφικά διάσπαρτες. Οι Ζώνες Διαθεσιμότητας είναι διακριτές τοποθεσίες οι οποίες έχουν σχεδιαστεί έτσι ώστε να παραμένουν απομονωμένες από βλάβες σε άλλες Ζώνες Διαθεσιμότητας, και να παρέχουν φθηνή, χαμηλής καθυστέρησης συνδεσιμότητα σε άλλες Ζώνες Διαθεσιμότητας που βρίσκονται στην ιδία Περιφέρεια.

Τα στιγμιότυπα μηχανής του EC2 αποθηκεύονται και ανακτώνται από το Amazon Simple Storage Service (S3).Το S3 αποθηκεύει τα δεδομένα με τη μορφή αντικειμένων τα οποία είναι οργανωμένα σε «κουβάδες» (buckets). Κάθε αντικείμενο μπορεί να περιέχει από 1 byte

μέχρι και 5 Gbytes δεδομένων. Τα ονόματα των αντικειμένων είναι στην ουσία ομοιόμορφα αναγνωριστικά πόρου (Universal Resource Identifier-URI[31]) Οι «κουβάδες» πρέπει να δημιουργηθούν ρητά προτού μπορέσουν αν χρησιμοποιηθούν ενώ μπορούν να αποθηκευτούν σε κάποια από τις πολλές Περιφέρειες. Από τη μεριά τους οι χρήστες επιλέγουν μια περιφέρεια με σκοπό να ελαχιστοποιήσουν την καθυστέρηση (latency) και οποία αλλά κόστη συνεπάγονται της επιλογής.

Το Virtual Private Cloud της Amazon (VPC) είναι μια ασφαλής γέφυρα ανάμεσα στην υπάρχουσα υποδομή μιας εταιρίας και του Amazon Web Services (AWS) Cloud. Το VPC επιτρέπει στις επιχειρήσεις να συνδέουν την υπάρχουσα υποδομή τους με ένα σύνολο απομονωμένων υπολογιστικών πόρων AWS μέσω ενός Virtual Private Network (VPN), επεκτείνοντας με αυτόν τον τρόπο τις υπάρχουσες διαχωριστικές δυνατότητες όπως υπηρεσίες ασφάλειας, firewalls και συστήματα ανίχνευσης εισβολών εξασφαλίζοντας έτσι τους πόρους AWS που κατέχουν.

Για τους χρήστες του Cloud, το CloudWatch της Amazon είναι ένα χρήσιμο εργαλείο διαχείρισης που συλλέγει ακατέργαστα δεδομένα από συνεργαζόμενες υπηρεσίες AWS, όπως το Amazon EC2, και στη συνεχεία επεξεργάζεται τις πληροφορίες μετατρέποντας τες σε αναγνώσιμα, σχεδόν πραγματικού χρόνου δεδομένα μετρήσεων, τα οποία για παράδειγμα μπορεί να περιέχουν ποσοστό χρησιμοποίησης της CPU, αριθμό bytes που εισέρχονται/εξέρχονται από το δίκτυο, πράξεις εγγραφής/ανάγνωσης από το δίσκο και αλλά.

4.7.2 Microsoft Windows Azure platform

Η πλατφόρμα Windows Azure της Microsoft[32] αποτελείται από τρία μέρη, κάθε ένα από τα οποία παρέχει ένα συγκεκριμένο σύνολο υπηρεσιών στους χρήστες του Cloud. Το Windows Azure παρέχει ένα περιβάλλον παραθύρων για εκτέλεση εφαρμογών και αποθήκευση δεδομένων στους servers που βρίσκονται στα data centers, το SQL Azure παρέχει υπηρεσίες δεδομένων στο cloud που βασίζονται σε SQL server, ενώ οι υπηρεσίες .NET παρέχουν υπηρεσίες κατανεμημένης υποδομής σε cloud-based και τοπικές εφαρμογές. Η πλατφόρμα Windows Azure μπορεί να χρησιμοποιηθεί από εφαρμογές που τρέχουν στο cloud αλλά και από εφαρμογές που τρέχουν σε τοπικά συστήματα.

Το Windows Azure υποστηρίζει επίσης εφαρμογές που έχουν αναπτυχτεί στο .NET framework καθώς και σε άλλες συνηθισμένες γλώσσες προγραμματισμού που υποστηρίζονται από τα συστήματα Windows, όπως C#, Visual Basic, C++ και άλλες. Ακόμη το Windows Azure υποστηρίζει γενικού σκοπού προγράμματα αντί για μια μοναδική κλάση υπολογισμού. Οι προγραμματιστές μπορούν να δημιουργήσουν εφαρμογές web χρησιμοποιώντας τεχνολογίες όπως το ASP.NET και το Windows Communication Foundation (WFC),εφαρμογές οι οποίες εκτελούνται ως ανεξάρτητες, παρασκηνιακές (background) διεργασίες αλλά και εφαρμογές που συνδυάζουν και τα δυο. Επιπρόσθετα το Windows Azure επιτρέπει την αποθήκευση δεδομένων σε φυσαλίδες (blobs), πίνακες και ουρές, όλες προσβάσιμες με το πρωτόκολλο REST

μέσω HTTP ή HTTPS.

Τα τμήματα SQL του Azure είναι μια βάση δεδομένων SQL Azure και το "Huron" Data Sync. Η βάση δεδομένων SQL Azure είναι ενσωματωμένη στον Microsoft SQL Server, παρέχοντας ένα σύστημα διαχείρισης βάσεων δεδομένων (DBMS) στο Cloud. Τα δεδομένα μπορούν αν προσπελαστούν χρησιμοποιώντας το ADO.NET καθώς και άλλες διεπαφές προσπέλασης δεδομένων των Windows, ενώ το "Huron" Data Sync συγχρονίζει τα σχεσιακά δεδομένα σε διαφορά εγκατεστημένα DBMSs.

Τέλος, όλοι οι φυσικοί πόροι, οι εικονικές μηχανές και οι εφαρμογές στο data center παρακολουθούνται από ένα λογισμικό που ονομάζεται Fabric Controller. Με κάθε εφαρμογή οι χρήστες ανεβάζουν ένα αρχείο ρύθμισης παραμέτρων (configuration file) το οποίο παρέχει μια βασισμένη σε XML περιγραφή του τι χρειάζεται η εφαρμογή, στη συνεχεία βασισμένος σε αυτήν την περιγραφή, ο Fabric Controller αποφασίζει για το που θα πρέπει να εκτελεστούν οι νέες εφαρμογές , επιλέγοντας φυσικούς servers με σκοπό την βελτιστοποίηση του ποσοστού χρησιμοποίησης του υλικού.

4.7.3 Google App Engine

Το Google App Engine[33] είναι μια πλατφόρμα για παραδοσιακές εφαρμογές web σε data centers διαχειριζόμενα από την Google. Οι υποστηριζόμενες γλώσσες αυτήν τη στιγμή είναι οι Python και Java, ενώ τα web frameworks που εκτελούνται στο Google App Engine περιλαμβάνουν τα Django, CherryPy, Pylons και web2py, καθώς και frameworks φτιαγμένα από την Google παρόμοια με το JSP ή το ASP.NET. Τα τωρινά APIs υποστηρίζουν χαρακτηριστικά όπως η αποθήκευση και ανάκτηση δεδομένων από μια BigTable[34] μη-σχεσιακή βάση δεδομένων, η δημιουργία αιτημάτων HTTP και το caching, ενώ οι προγραμματιστές έχουν πρόσβαση μόνο για ανάγνωση στο σύστημα αρχείων του App Engine.

Cloud Provider	Amazon EC2	Windows Azure	Google App Engine
Classes of Utility Computing	Infrastructure service	Platform service	Platform service
Target Applications	General-purpose applications	General-purpose Windows applications	Traditional web applications with supported framework
Computation	OS Level on a Xen Virtual Machine	Microsoft Common Language Runtime (CLR) VM; Predefined roles of app. instances	Predefined web application frameworks
Storage	Elastic Block Store; Amazon Simple Storage Service (S3); Amazon SimpleDB	Azure storage service and SQL Data Services	BigTable and MegaStore
Auto Scaling	Automatically changing the number of instances based on parameters that users specify	Automatic scaling based on application roles and a configuration file specified by users	Automatic Scaling which is transparent to users

Πίνακας 4.4: Σύγκριση των τριών επικρατέστερων εμπορικών προϊόντων Cloud Computing. [37]

4.7 Βιβλιογραφία Κεφαλαίου

[1] C.N. Höfer · G. Karagiannis : Cloud computing services: taxonomy and comparison

[2] Mell P, Grance T (2009) The NIST definition of cloud computing (v15). Tech Rep, National Institute of Standards and Technology

[3]Sun Microsystems: *"Introduction to cloud computing Architecture"*, White paper 1st edition, June 2009

[4] Amazon Web Services LLC. Amazon EC2 SLA. http://aws.amazon.com/ec2-sla.

[5] Citrix Systems, Inc. Xen hypervisor. http://www.xen.org

[6] DMTF Cloud Computing Incubator. http://www.dmtf.org/about/cloud-incubator

[7] Google Apps. http://www.google.com/apps

[8]Microsoft Azure. http://www.microsoft.com/windowsazure.

[9] XenSource Inc, Xen, www.xensource.com

[10] Berners-Lee T, Fielding R, Masinter L (2005) RFC 3986: uniform resource identifier (URI): generic syntax, January 2005

[11] Google App Engine, URL http://code.google.com/appengine

[12] Chang F, Dean J et al (2006) Bigtable: a distributed storage system for structured data. In: Proc of OSDI

[13] www.wikipedia.org

Κεφάλαιο 5

Χαρακτηριστικά Cloud Computing

Περιεχόμενα

5.1 Εισαγωγή

Τα cloud computing, grid computing, High Performance computing (HPC), και το data center computing ανήκουν όλα στην κατηγορία του παράλληλου υπολογισμού. Το HPC επικεντρώνεται στον επιστημονικό υπολογισμό ο όποιος μπορεί να είναι πολύ εντατικός και ευαίσθητος σε καθυστερήσεις , όποτε τα σημαντικότερα κριτήρια για το HPC είναι η υψηλή απόδοση του υπολογισμού και οι χαμηλές καθυστερήσεις. Το Grid computing είναι βασισμένο σε ένα HPC κέντρο, πολλά συνδεδεμένα HPC κέντρα σχηματίζουν ένα μεγάλο grid. Το cloud computing, το οποίο είναι βασισμένο στα data centers , έχει μεγαλύτερη απήχηση από ότι το grid computing και αυτό διότι τα data centers δεν επιδιώκουν μόνο την υψηλή απόδοση και την ανοχή σε καθυστερήσεις καθιστώντας τα έτσι πιο ισορροπημένα σε σχέση με τα HPC centers. Στον παρακάτω πινάκα συγκρίνονται μερικά από τα χαρακτηριστικά[35] του cloud computing με αυτά του grid computing.

Characteristic	Cloud computing	Grid computing
Service oriented	Yes	Yes
Loose coupling	Yes	Half
Strong fault tolerant	Yes	Half
Business model	Yes	No
Ease use	Yes	Half
TCP/IP based	Yes	Half
High security	Half	Half
Virtualization	Yes	Half

Πίνακας 5.1 : Σύγκριση χαρακτηριστικών ανάμεσα στο Cloud computing και Grid Computing. [35]

5.2 Τεχνολογικά χαρακτηριστικά

5.2.1 Loose coupling.

Η χαλαρή σύζευξη (loose coupling) είναι το τεχνολογικό θεμέλιο του cloud computing και υπερβαίνει τη μέθοδο loose coupling για την αλληλεπίδραση των εφαρμογών. μέσω της εικονοποίησης η άλλων τεχνολογιών οι τεχνικές υποδομές χωρίζονται σε λογικές η φυσικές. Η συμπεριφορά του ενός μέρους δεν επηρεάζει τα άλλα μέρη, για παράδειγμα, η πλατφόρμα είναι ένα αφηρημένο στρώμα το οποίο μπορεί να απομονώσει διαφορετικές εφαρμογές που εκτελούνται πάνω της. Το σημαντικότερο από όλα είναι ότι το cloud computing εκτελείται με

βάση το μοντέλο client-server. Οι clients, η αλλιώς οι χρήστες του cloud συνδέονται χαλαρά (loosely) με τους servers , η αλλιώς τους παρόχους cloud. Όλοι οι χρήστες έχουν σχεδόν μηδενική εξάρτηση από δεδομένα η ρυθμίσεις.

Συμφώνα λοιπόν με το Loose coupling :Οι χρήστες συνθέτονται από σύνολα χρηστών *Uset1* , *Uset2* , …, *Usetm* (*m* >=1).Οι πάροχοι συνθέτονται από σύνολα παρόχων *Pset1* , *Pset2* ,…, *Psetn* (*n* >=1). Το Loose Coupling μεταξύ του συνόλου χρηστών Useti και του συνόλου παρόχων Psetj αναφέρεται ως Set(Useti,Psetj).

Υπάρχουν οι 3 εξής ιδιότητες:

- Τα σύνολα χρηστών είναι ανεξάρτητα μεταξύ τους: Useti ∩ Usetj=ϕ (0<=i, j<=m ,i!=j)
- Τα σύνολα των παρόχων είναι ανεξάρτητα μεταξύ τους : Pseti ∩ Psetj= ϕ (0<=i, j<=m ,i!=j)
- Τα σύνολα loose coupling (ο χρήστης cloud συνδέεται με τον πάροχο cloud) είναι ανεξάρτητα: Set (Useti1,Psetj1) ∩ Set(Useti2,Psetj2)=ϕ

Παίρνοντας την αναζήτηση στο internet ως ένα απλό παράδειγμα: οι πάροχοι είναι τα Google, Yahoo! και Bing. Οι χρήστες των υπηρεσιών αναζήτησης δεν μπορούν να χρησιμοποιήσουν και τις 3 μηχανές αναζήτησης ταυτόχρονα (σε απολυτό χρόνο) και μπορούν να διαχωριστούν σε ανεξάρτητα σύνολα χρηστών: UsetGoogle ∩ UsetYahoo! ∩ UsetBing=ϕ . Τα data centers που βρίσκονται πίσω από μια απλή αναζήτηση στο διαδίκτυο είναι ανεξάρτητα για τις 3 εταιρείες : PsetGoogle ∩ PsetYahoo! ∩ PsetBing=ϕ. Τα σύνολα loose coupling είναι ανεξάρτητα επίσης: : Set (UsetGoogle,PsetGoogle) ∩ Set(UsetYahoo!,PsetYahoo!) ∩ Set(UsetBing,PsetBing)=ϕ.

Ένα αντίθετο παράδειγμα είναι η ισχυρή σύζευξη (tight coupling) που χρησιμοποιούν τα συστήματα HPC τα όποια επικεντρώνονται στη λύση επιστημονικών προβλημάτων. Συνήθως υπάρχουν πάρα πολλές εξαρτήσεις από δεδομένα ή καθολικούς συγχρονισμούς σε διαφορετικές επαναλήψεις ώστε να ανέχονται τις υψηλές καθυστερήσεις ανάμεσα στους διαφόρους κόμβους που εκτελούν τους υπολογισμούς. Αυτού του είδους τα συστήματα χρησιμοποιούν υψηλής ταχύτητας δίκτυα όπως για παράδειγμα το InfiniBand[36] αντί για το συνηθισμένο Ethernet το οποίο είναι αρκετά φθηνότερο και ευρέως διαδεδομένο. Ένας καθολικός συγχρονισμός σε ένα σύστημα HPC μπορεί να διαρκέσει κάποιες δεκάδες λεπτά, αντίθετα όμως ένας καθολικός συγχρονισμός στο cloud computing μπορεί να διαρκέσει αρκετές ώρες η ακόμη και μέρες.

5.2.2 Υψηλή Ανοχή σε βλάβες

Υπάρχουν πολλές μέθοδοι για ανοχή σε βλάβες στον παράλληλο υπολογισμό. Σε χαμηλότερη επίπεδο υπάρχουν κάποιοι μηχανισμοί επιδιόρθωσης βλαβών που χρησιμοποιούν συγκεκριμένο υλικό. Σε υψηλό επίπεδο, πολλές επιστημονικές εφαρμογές έχουν μελετηθεί, με μεθόδους που χρησιμοποιούν αλγορίθμους. Το check pointing είναι μια από τις πιο αποτελεσματικές μεθόδους στο μεσαίο επίπεδο. Σε παράλληλο υπολογισμού μεγάλης κλίμακας το διάστημα μεταξύ 2 βλαβών μπορεί να είναι μικρότερο από τον χρόνο εκτέλεσης της εφαρμογής. Για παράδειγμα κάποιες επιστημονικές εφαρμογές εκτελούνται για εβδομάδες η ακόμα και περισσότερο και σε αυτό το διάστημα μπορεί να συμβούν περισσότερες από 1 σημαντικές ή όχι βλάβες. Η τεχνολογία ανοχής βλαβών γίνεται πολύ σημαντική σε αυτές τις συνθήκες. Για το λόγο ότι ένα μικρό σε σημασία λάθος είναι ανεκτό, και η επανεκτίμηση όλου του υπολογισμού έχει μεγάλο κόστος σε χρόνο και όχι μόνο, ολόκληρες οι καταστάσεις του υπολογισμού αποθηκεύονται περιοδικά σε σταθερή μνήμη και σε περίπτωση λάθους/βλάβης ο υπολογισμός μπορεί να γυρίσει πίσω (roll back) σε κάποια κατάσταση πριν συμβεί το λάθος και να συνεχίσει τον υπολογισμό από εκεί.

Δεν είναι απαραίτητο να κρατούνται ολόκληρες οι καταστάσεις των συστημάτων cloud computing στη μνήμη, και αυτό διότι υπάρχει σχεδόν μηδενική εξάρτηση ανάμεσα σε 2 συναλλαγές. Η αποτυχία μιας συναλλαγής δεν επηρεάζει την άλλη και η μερική αποτυχία του συστήματος δεν θα προκαλέσει αλυσιδωτή αντίδραση.

Υπάρχουν κυρίως 4 μέρη στα όποια μπορούν να συμβούν βλάβες στο cloud computing: provider-inner, provider across, provider-user, user-across.

Εάν η βλάβη συμβεί στον πάροχο, το backup ή ο πλεονασμός των δεδομένων στον πάροχο μπορούν να αντικαταστήσουν το σημείο που συνέβη το λάθος. Το σταμάτημα των υπηρεσιών και η επανεκκίνηση τους είναι ένας άλλος συνήθης τρόπος αντιμετώπισης εάν οι υπηρεσίες δεν είναι επείγουσες. Η loose coupling φύση του παρόχου κάνει αυτού του είδους τις βλάβες εύκολες να αντιμετωπιστούν.

Εάν η βλάβη σημειωθεί ανάμεσα σε παρόχους, η provider-across συναλλαγή θα αποτύχει και θα επιστρέψει ένα μήνυμα λάθους. Η ανακατεύθυνση σε άλλους παρόχους είναι μια καθολική μέθοδος η όποια περιλαμβάνει την εξισορρόπηση του φόρτου σε όλο το σύστημα cloud.

Υπάρχουν πολλοί λόγοι όπως η συμφόρηση του δικτύου, η βλάβη του browser, το time out της αίτησης και επιθέσεις hacker που μπορεί να προκαλέσουν βλάβες ανάμεσα σε χρήστη και πάροχο. Εάν αυτές οι βλάβες δεν εμπεριέχουν κάποια χαρακτηριστικά-κλειδιά μπορούν να παραλειφθούν και ο χρήστης να προσπαθήσει ξανά αργότερα. Οι αλγόριθμοι που είναι ανεκτικοί σε Βυζαντινές βλάβες είναι πολύ σημαντικοί λόγω τις αύξησης των κακόβουλων βλαβών μεταξύ χρήστη και παρόχου οι όποιες μπορεί να προκαλέσουν ελαττωματικούς κόμβους να παρουσιάζουν αυθαίρετη συμπεριφορά η όποια είναι δύσκολο να αντιμετωπιστεί. Εάν οι βλάβες εμπεριέχουν κάποια χαρακτηριστικά τα όποια προκαλούν πραγματική απώλεια στους χρήστες, όπως η απώλεια χρημάτων στον προσωπικό λογαριασμό, πρέπει να ληφθούν επιπρόσθετα μετρά ώστε να διασφαλιστεί η συναλλαγή,

Ο χρήστης δεν συνδέεται μόνο με τον πάροχο αλλά και με άλλους χρήστες. Πολλοί χρήστες παρακολουθούν δραστηριότητες και μοιράζονται πολλούς κρίσιμους, για το σύστημα, πόρους. Σε αυτήν την περίπτωση η μη ασφαλής πρόσβαση σε κρίσιμους πόρους του συστήματος μπορεί να προκαλέσει χάος στα συστήματα cloud computing. Υπάρχουν μέθοδοι σε επίπεδο υλικού, επίπεδο λειτουργικού και επίπεδο λογισμικού για την προστασία αυτών

των κρίσιμων πόρων και αν και αυτοί οι μέθοδοι δεν αποδεδειχθούν αρκετοί, υπάρχει και η λύση της προσφυγής στο νόμο.

5.3 Τεχνολογίες Cloud Computing[37]

5.3.1 Αρχιτεκτονικός σχεδιασμός των Data Centers

Το data center είναι το κεντρικό σημείο ενός συστήματος cloud computing και περιέχει χιλιάδες συσκευές όπως servers, switches και routers. Ο προσεκτικός σχεδιασμός αυτής της αρχιτεκτονικής δικτύου είναι υψηλής σημασίας καθώς θα επηρεάσει σημαντικά την απόδοση των εφαρμογών και την ρυθμαπόδοση σε ένα τέτοιο κατανεμημένο περιβάλλον. Επιπρόσθετα θέματα κλιμάκωσης και ανθεκτικότητας πρέπει να ληφθούν σοβαρά υπόψιν.

Προς το παρόν μια προσέγγιση στρωμάτων είναι το βασικό θεμέλιο στον σχεδιασμό της αρχιτεκτονικής του δικτύου, η όποια έχει ελεγχθεί σε μερικά από τα μεγαλύτερα data centers που έχουν εγκατασταθεί. Τα βασικά στρώματα ενός data center αποτελούνται από στρώματα πυρήνα , στρώματα συνάθροισης και στρώματα πρόσβασης. Το στρώμα πρόσβασης είναι το μέρος οπού οι servers συνδέονται φυσικά στο δίκτυο. Συνήθως σε κάθε rack υπάρχουν 20 με 40 servers, ο καθένας εκ των όποιων συνδέεται σε ένα διακόπτη πρόσβασης με μια γραμμή 1 Gbps. Οι διακόπτες πρόσβασης συνήθως συνδέονται σε 2 διακόπτες συνάθροισης για πλεονασμό με γραμμές 10 Gbps.Το στρώμα συνάθροισης συνήθως παρέχει σημαντικές λειτουργιές όπως υπηρεσίας ονόματος, υπηρεσίες τοποθεσίας, υπηρεσίες εξισορρόπησης φόρτου και αλλά. Το στρώμα πυρήνα παρέχει συνδεσιμότητα σε πολλαπλούς διακόπτες συνάθροισης και παρέχει ένα ανθεκτικό δρομολογούμενο οικοδόμημα με μηδενικά σημεία βλάβης. Οι δρομολογητές του πυρήνα διαχειρίζονται την κίνηση από και προς το data center.

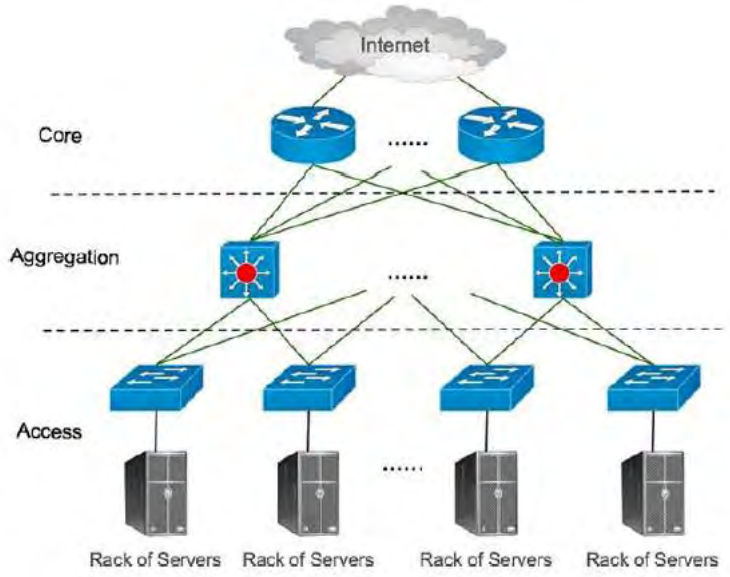
Ο σχεδιασμός μιας αρχιτεκτονικής data center πρέπει να ικανοποιεί τις παρακάτω προϋποθέσεις:

- ***Ενιαία υψηλή χωρητικότητα (Uniform High Capacity)***: Ο μέγιστος ρυθμός ροής πληροφορίας από server σε server πρέπει να περιορίζεται μόνο από την διαθέσιμη χωρητικότητα στις κάρτες δικτύου των server που αποστέλλουν, και των server που δέχονται δεδομένα, και η ανάθεση ενός server σε μια υπηρεσία πρέπει να είναι ανεξάρτητη από την τοπολογία του δικτύου. Θα πρέπει να είναι δυνατό για έναν αυθαίρετο host να μπορεί να επικοινωνεί με οποιονδήποτε άλλο μέσα στο δίκτυο στο μέγιστο δυνατό bandwidth της τοπικής διεπαφής δικτύου.
- ***Ελεύθερη μετακίνηση εικονικών μηχανών:*** Η εικονοποίηση επιτρέπει την μετάδοση ολόκληρης της κατάστασης μιας εικονικής μηχανής από ένα φυσικό μηχάνημα σε ένα άλλο. Μια υπηρεσίας φιλοξενίας cloud computing μπορεί να μεταφέρει τις εικονικές μηχανές με σκοπό την στατιστική πολυπλεξία η την δυναμική τροποποίηση των προτύπων επικοινωνίας έτσι ώστε να επιτύχει υψηλό bandwidth για ισχυρά συζευγμένους (tightly coupled) hosts ή για να επιτύχει μεταβλητή κατανομή θερμοκρασίας και ενεργειακής διαθεσιμότητας

στο data center. Η τοπολογία επικοινωνίας πρέπει να σχεδιαστεί ώστε να υποστηρίζει τη γρήγορη μετανάστευση των εικονικών μηχανών.

- ***Ανθεκτικότητα (Resiliency):*** Η υποδομή δικτύου θα πρέπει να είναι ανεκτική σε ποικίλου είδους βλάβες, όπως αποτυχίες server, διακοπές συνδέσμων και αλλά. Οι υπάρχουσες unicast και multicast επικοινωνίες δεν θα πρέπει να επηρεάζονται στο σημείο που το επιτρέπει η υποκείμενη φυσική συνδεσιμότητα.
- ***Κλιμάκωση (Scalability):*** Η υποδομή του δικτύου θα πρέπει να κλιμακώνεται για υποστήριξη μεγαλυτέρου αριθμού servers και να επιτρέπει την αυξητική επέκταση.
- ***Συμβατότητα με το υπάρχον υλικό (Backward compatibility):*** Η υποδομή δικτύου θα πρέπει να είναι συμβατή με το υπόβαθρο, τους διακόπτες και τους δρομολογητές που λειτουργούν με βάση το Ethernet και το IP λόγω της κατά κόρου χρήσης αυτών των 2 τεχνολογιών στα υπάρχοντα data centers.

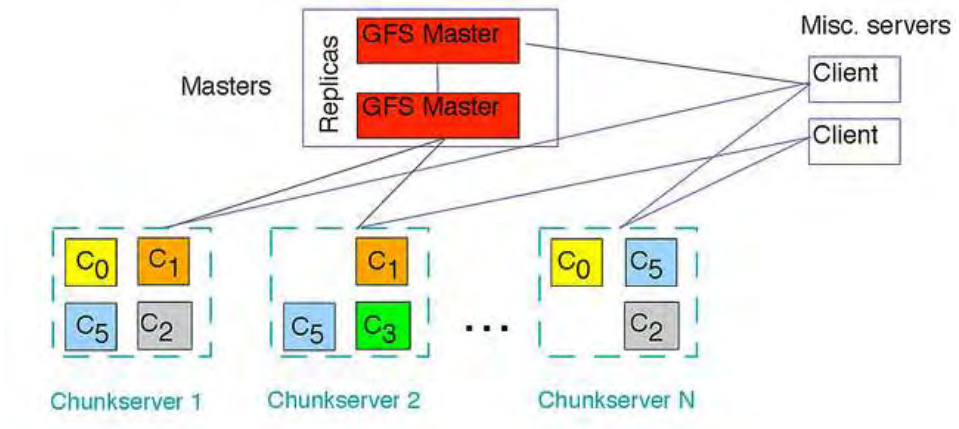
Μια ακόμη καινοτομία γα τη βιομηχανία είναι ο σχεδιασμός και η ανάπτυξη αρθρωτών data centers (Modular Data Center- MDC), μια μέθοδος φορητής ανάπτυξης της χωρητικότητας ενός data center. Σε αντίθεση με τα παραδοσιακά data centers ένα MDC μπορεί να τοποθετηθεί οπουδήποτε χρειάζεται επιπλέον χωρητικότητα δεδομένων[38]. Σε ένα MDC μερικές χιλιάδες servers συνδέονται μεταξύ τους μέσω διακόπτων για να σχηματίσουν τη υποδομή δικτύου. Είναι, επίσης, σχεδιασμένα για πολύ γρήγορη εγκατάσταση, ενεργειακή απόδοση και μπορούν να παραδώσουν χωρητικότητα στα data centers με κόστος μικρότερο από τις παραδοσιακές μεθόδους κατασκευής, μειώνοντας επίσης σημαντικά το χρόνο κατασκευής από αρκετά χρονιά σε μόλις μερικούς μήνες.



Εικόνα 5.1: Ο βασικός σχεδιασμός σε στρώματα μιας υποδομής δικτύου ενός data center. [37]

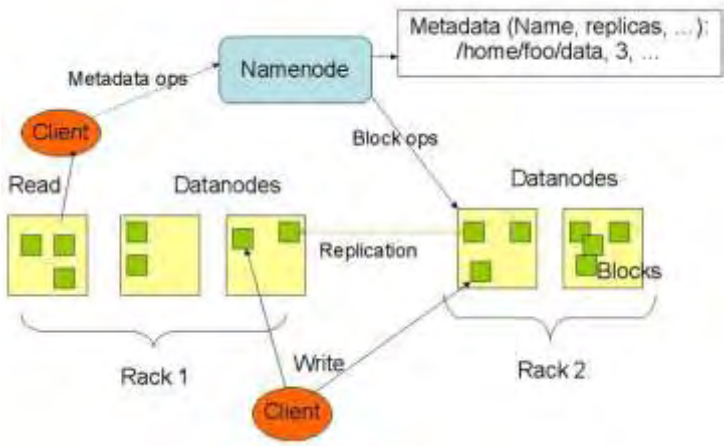
5.3.2 Κατανεμημένα συστήματα Αρχείων

Το Google File System (GFS)[39] είναι ένα ιδιόκτητο κατανεμημένο σύστημα αρχείων που έχει αναπτυχτεί από τη Google και έχει σχεδιαστεί για να παρέχει αποδοτική, αξιόπιστη πρόσβαση στα δεδομένα χρησιμοποιώντας μεγάλες συστάδες από servers. Τα αρχεία διαχωρίζονται σε τμήματα των 64 MB και στο καθένα αποδίδεται μια μοναδική 64-bit ετικέτα. Κάθε τμήμα αναπαράγεται το λιγότερο 3 φόρες μέσα σε όλο το δίκτυο, και πολλές περισσότερες για αρχεία που έχουν μεγάλη ζήτηση ή χρειάζονται περισσότερο πλεονασμό. Σε σύγκριση με τα παραδοσιακά συστήματα αρχείων , το GFS είναι σχεδιασμένο και βελτιστοποιημένο να εκτελείται πάνω σε data centers για να παρέχει πολύ υψηλή ρυθμαπόδοση δεδομένων, χαμηλή καθυστέρηση και ανοχή σε ατομικές αποτυχίες server.



Εικόνα 5.2: Η αρχιτεκτονική του Google GFS. [39]

Εμπνευσμένο από το GFS το open-source Hadoop Distributed File System (HDFS)[40] αποθηκεύει ένα μεγάλο αρχείο ανάμεσα σε πολλαπλές μηχανές. Επιτυγχάνει αξιοπιστία αναπαράγοντας τα δεδομένα ανάμεσα σε πολλούς servers. Παρόμοια με το GFS τα δεδομένα αποθηκεύονται σε πολλαπλούς γέω-ποικίλους κόμβους, Το σύστημα αρχείων είναι δομημένο από μια συστάδα κόμβων δεδομένων , κάθε ένας εκ των όποιων εξυπηρετεί μπλοκ δεδομένων πάνω στο δίκτυο χρησιμοποιώντας κάποιο συγκεκριμένο πρωτόκολλο για το HDFS. Τα δεδομένα παρέχονται επίσης πάνω από HTTP, επιτρέποντας πρόσβαση σε όλο το περιεχόμενο από έναν web browser η κάποιο άλλο είδος client. Οι κόμβοι δεδομένων μπορούν να επικοινωνούν μεταξύ τους ώστε να εξισορροπήσουν την κατανομή δεδομένων, να μετακινούν αντίγραφα και να κρατούν σε υψηλό επίπεδο την αναπαραγωγή δεδομένων.

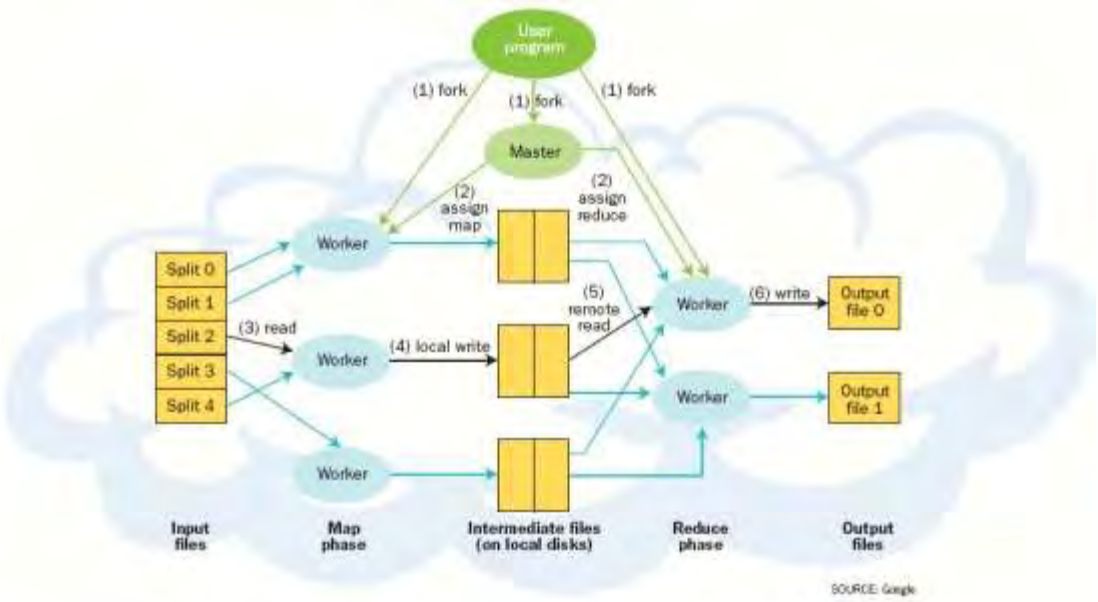


Εικόνα 5.3: Η Αρχιτεκτονική του HDFS. [40]

5.3.3 Κατανεμημένα Frameworks Εφαρμογών

Οι εφαρμογές βασισμένες στο HTTP συνήθως προσαρμόζονται σε κάποιο πλαίσιο web εφαρμογών όπως το Java EE. Στα σύγχρονα περιβάλλοντα των data centers συστάδες από servers χρησιμοποιούνται για υπολογισμούς και απαιτητικές σε δεδομένα εργασίες όπως η ανάλυση οικονομικών τάσεων και το animation ταινιών.

Το MapReduce[41] είναι ένα πλαίσιο λογισμικού που εισήγαγε η Google για να υποστηρίξει τον κατανεμημένο υπολογισμό για μεγάλα σύνολα δεδομένων σε συστάδες υπολογιστών. Το MapReduce αποτελείται από έναν Master στον οποίο οι εφαρμογές-πελάτες στέλνουν της MapReduce εργασίες τους. Ο Master στέλνει τις εργασίες σε διαθέσιμους κόμβους διεργασιών μέσα στο data center προσπαθώντας να κρατήσει τις διεργασίες όσο πιο κοντά στα δεδομένα γίνεται. Ο Master γνωρίζει ποιος κόμβος περιέχει τα δεδομένα και ποιοι άλλοι hosts βρίσκονται κοντά. Εάν η διεργασία δεν μπορεί να πραγματοποιηθεί στον κόμβο οπού τα δεδομένα είναι αποθηκευμένα, δίνεται προτεραιότητα στους κόμβους που βρίσκονται στο ίδιο server-rack. Με αυτόν τον τρόπο η κυκλοφορία στο κεντρικό σημείο του δικτύου μειώνεται, κάτι που βοηθά στη βελτίωση της ρυθμαπόδοσης, καθώς ο κεντρικός άξονας του δικτύου συνήθως αποτελεί και το σημείο συμφόρησης του (bottleneck).



Εικόνα 5.4: Ο τρόπος λειτουργιάς του MapReduce. [41]

5.4 Βιβλιογραφία Κεφαλαίου

[1] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong : *The Characteristics of Cloud Computing*

[2] D. Malcolm, “The five defining characteristics of cloud computing, ”http://news.zdnet.com/2100-9595_22-287001.html”.

[3] Qi Zhang · Lu Cheng · Raouf Boutaba**:** *Cloud computing: state-of-the-art and research challenges*

[4] Ghemawat S, Gobioff H, Leung S-T (2003): The Google file system.
In: Proc of SOSP, October 2003

[5] Hadoop Distributed File System, hadoop.apache.org/hdfs

[6] Al-Fares M et al (2008) A scalable, commodity data center network architecture. In: Proc SIGCOMM
[7] Guo C, Lu G, Li D et al (2009) BCube: a high performance, server-centric network architecture for modular data centers. In: Proc SIGCOMM

[8] Dean J, Ghemawat S (2004) MapReduce: simplified data processing
on large clusters. In: Proc of OSDI

[9] www.wikipedia.org

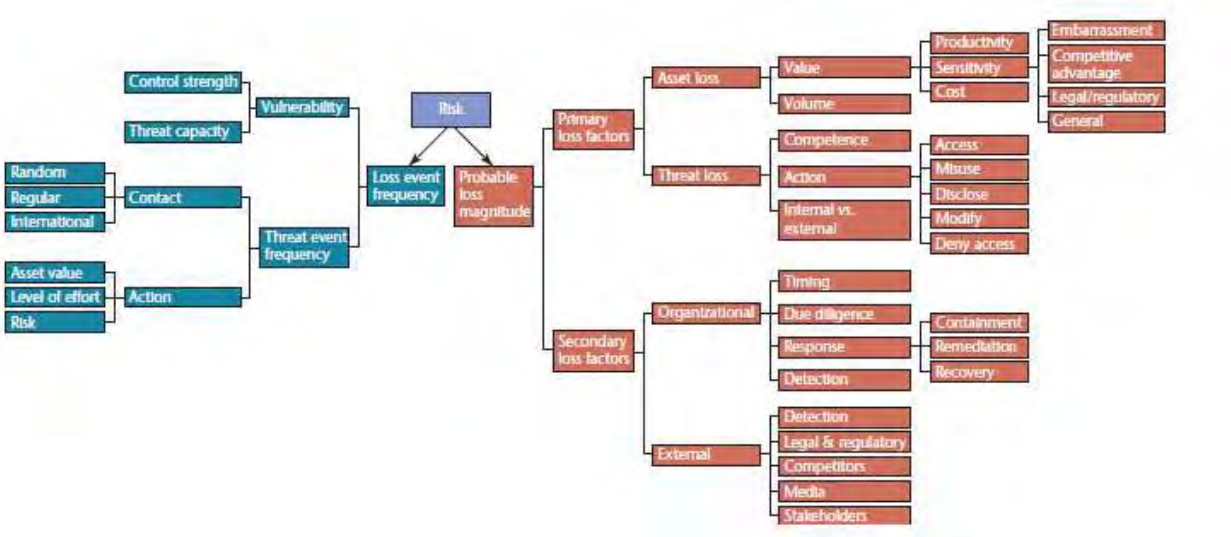
Κεφάλαιο 6

Αδυναμίες του Cloud Computing

Περιεχόμενα

6.1 Εισαγωγή

Ένα «τρωτό σημείο» (vulnerability) είναι ένας σημαντικός παράγοντας ρίσκου. Σύμφωνα με το ISO[42] 27005 το ρίσκο είναι «η πιθανότητα ότι μια δεδομένη απειλή θα εκμεταλλευτεί τυχόν τρωτά σημεία κάποιου περιουσιακού στοιχείου ή μιας ομάδας περιουσιακών στοιχειών προκαλώντας έτσι κακό στον οργανισμό».



Εικόνα 6.1: Παράγοντες που συμβάλλουν στο ρίσκο, το οποίο αντιστοιχεί στο προϊόν της απώλειας συχνότητας του γεγονότος (αριστερά) και της πιθανότητας απώλειας μεγέθους (δεξιά). [44]

Σύμφωνα με την ταξινομία του Open Group[43] ένα τρωτό σημείο είναι η πιθανότητα ότι ένα περιουσιακό στοιχείο δεν θα είναι σε θέση να αντισταθεί στις δράσεις ενός πράκτορα απειλής. Τρωτό σημείο υπάρχει όταν υπάρχει διαφορά ανάμεσα στην προσπάθεια που καταβάλλει ο πράκτορας απειλής και στην ικανότητα ενός αντικειμένου να αποκρούσει αυτή την ικανότητα. Το τρωτό σημείο στο χώρο των Υπολογιστικών Συστημάτων μπορεί να περιγραφεί ως η αποδυνάμωση η αφαίρεση μιας συγκεκριμένης ικανότητας του συστήματος για άμυνα. Ένα λάθος υπερχείλισης (buffer-overflow) για παράδειγμα αποδυναμώνει την ανθεκτικότητα του συστήματος σχετικά με την αυθαίρετη εκτέλεση κώδικα.

Σύμφωνα με το US National Institute of Standards and Technology (NIST) ένα σύστημα cloud πρέπει να ικανοποιεί τα εξής 5 χαρακτηριστικά:

- ***Υπηρεσία κατ'απαίτηση (On demand Service):*** Οι χρήστες μπορούν να προσαρμόσουν και να διαχειριστούν τις υπηρεσίες χωρίς αλληλεπίδραση με τον πάροχο της υπηρεσίας.
- ***Πρόσβαση από παντού(Ubiquitous network access):*** Οι υπηρεσίες cloud, προσπελαύνονται πάνω από το δίκτυο χρησιμοποιώντας προτυποποιημένους μηχανισμούς και πρωτοκόλλα.
- ***Διάθεση των πόρων(Resource Pooling):*** Οι υπολογιστικοί πόροι που χρησιμοποιούνται για την παροχή της cloud υπηρεσίας γίνονται αντιληπτοί μέσο μιας ομογενοποιημένης υποδομής που είναι κοινή για όλους τους χρήστες της υπηρεσίας.
- ***Ταχεία Ελαστικότητα(Rapid Elasticity) :*** Οι πόροι μπορούν να καμακώνονται προς τα πάνω και προς τα κάτω με μεγάλη ταχύτητα και ελαστικότητα.
- ***Μετρήσιμη Υπηρεσία(Measured Service):*** Η χρήση πόρων/υπηρεσιών μετριέται συνεχώς, με σκοπό την υποστήριξη της βελτιστοποίησης της χρήσης των πόρων, τις αναφορές χρήσης στους πελάτες και τα pay-as-you-go μοντέλα.

6.2 Τρωτά σημεία σχετικά με το Cloud

Μια αδυναμία ενός συστήματος cloud computing μπορεί να χαρακτηριστεί ως τρωτό σημείο[44] εάν :

- Είναι εγγενής η επικρατούσα στον πυρήνα της τεχνολογίας του cloud computing.
- Έχει τα κύρια αίτια της σε ένα από χαρακτηριστικά του cloud σύμφωνα με το NIST.
- Προκαλείται όταν οι καινοτομίες του cloud computing καθιστούν τα δοκιμασμένα συστήματα ασφάλειας πολύ δύσκολο η αδύνατο να υλοποιηθούν.
- Είναι επικρατούσα σε καθιερωμένες προσφορές υπηρεσιών του cloud.

6.2.1 Αδυναμίες των τεχνολογιών πυρήνα του Cloud

Οι τεχνολογίες που βρίσκονται στον πυρήνα του cloud όπως οι web εφαρμογές και υπηρεσίες, η εικονοποίηση και η κρυπτογραφία έχουν τρωτά σημεία τα οποία είναι εγγενή στην τεχνολογία ή επικρατούν στις σύγχρονες (state-of-the-art) υλοποιήσεις. Μερικά παραδείγματα τέτοιων τρωτών σημείων είναι η διαφυγή της εικονικής μηχανής, το session-

riding και high jacking και η απαρχαιωμένη κρυπτογραφία.

Πρώτον, η πιθανότητα ενός εισβολέα να διαφύγει από το εικονοποιημένο περιβάλλον έγκειται στην αυτή κάθε αυτή φύση της εικονοποίησης. Έτσι αυτή η αδυναμία πρέπει να θεωρηθεί ως εγγενής ως προς την εικονοποίηση και απόλυτα σχετική με το cloud computing.

Δεύτερον, η τεχνολογία των web εφαρμογών πρέπει να ξεπεράσει το πρόβλημα ότι εξ'αρχής από τον σχεδιασμό, το πρωτόκολλο HTTP είναι ένα ακαταστατικό (stateless) πρωτόκολλο ενώ οι web εφαρμογές χρειάζονται την αντίληψη μιας κατάστασης σε μια σύνοδο (session). Πολλές τεχνολογίες υλοποιούν των χειρισμό των sessions και πολλές υλοποιήσεις είναι ευάλωτες στο session riding και session highjacking.

Τρίτον, η πρόοδος της κρυπτοανάλυσης μπορεί να καταστήσει οποιονδήποτε μηχανισμό ή αλγόριθμο κρυπτογραφίας ανασφαλή, καθώς νέες μέθοδοι διάσπασης τους ανακαλύπτονται συνεχώς. Είναι ακόμα πιο συνηθισμένη η ύπαρξη σημαντικών ελαττωμάτων σε ένα αλγόριθμο κρυπτογραφίας που μπορεί να μετατρέψει μια ισχυρή κρυπτογραφία σε μια αδύναμη, η μερικές φορές να την καταστήσει τελείως ανύπαρκτη. Επειδή λοιπόν η μη ύπαρξη κρυπτογραφίας στο cloud θα σήμαινε ελλιπή ή ακόμη και ανύπαρκτη προστασία και ακεραιότητα των ευαίσθητων δεδομένων , οι απαρχαιωμένες και ανασφαλείς μέθοδοι κρυπτογραφίας θεωρούνται απόλυτα σχετικές με το cloud computing.

6.2.2 Αδυναμίες των βασικών χαρακτηριστικών του Cloud

Όπως αναλύθηκε παραπάνω , σύμφωνα με το NIST ένα σύστηνα cloud computing πρέπει να έχει τα εξής χαρακτηριστικά: Υπηρεσία κατ'απαίτηση, Πρόσβαση από παντού, Διάθεση των πόρων, Ταχεία Ελαστικότητα, Μετρήσιμη Υπηρεσία. Παρακρατώ ακολουθούν μερικά παραδείγματα τρωτών σημείων που έχουν τις κύριες αιτίες τους σε ένα η και περισσότερα από αυτά τα χαρακτηριστικά.

- ***Μη εξουσιοδοτημένη πρόσβαση στη διεπαφή διαχείρισης:*** Το χαρακτηριστικό "Υπηρεσία κατ'απαίτηση" απαιτεί μια διεπαφή διαχείρισης η οποία πρέπει να είναι προσπελάσιμη από τους χρήστες του cloud. Η εξουσιοδοτημένη πρόσβαση σε αυτήν τη διεπαφή αποτελεί ένα αδύναμο σημείο για το cloud. Επιπλέον η πιθανότητα μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα cloud είναι πολύ μεγαλύτερη από ότι στα παραδοσιακά συστήματα όπου την πρόσβαση στη διαχείριση του συστήματος είχαν μόνο λίγοι διαχειριστές του.
- ***Αδυναμίες των πρωτοκόλλων του Internet*** : Το χαρακτηριστικό "Πρόσβαση από παντού" αναφέρεται στην πρόσβαση στις υπηρεσίες cloud πάνω από ένα δίκτυο χρησιμοποιώντας καθιερωμένα πρωτόκολλα. Σε αυτήν την περίπτωση το δίκτυο είναι το Internet, το οποίο δεν μπορεί να θεωρηθεί έμπιστο, οπότε οι αδυναμίες των πρωτοκόλλων του internet, όπως αδυναμίες που επιτρέπουν τις

επιθέσεις man-in-the-middle, είναι επιπλέον και αδυναμίες όλου του συστήματος cloud computing.

- ***Αδυναμίες ανάκτησης δεδομένων:*** Τα χαρακτηριστικά "Διάθεση των πόρων " και "Ταχεία Ελαστικότητα" συνεπάγονται την μετακίνηση πόρων που είχαν παραχωρηθεί σε έναν χρήστη, σε κάποιον άλλο χρήστη. Για συγκεκριμένη μορφή πόρων όπως μνήμη η αποθηκευτικός χώρος , είναι πιθανή η ανάκτηση δεδομένων τα οποία είχαν δημιουργηθεί η τροποποιηθεί από κάποιον προηγούμενο χρήστη.
- ***Αποφυγή μετρήσεων και χρεώσεων:*** Τα δεδομένα των μετρήσεων χρησιμοποιούνται για την βελτίωση της απόδοσης των υπηρεσιών καθώς και για τη χρέωση τους, αυτά τα δεδομένα μπορεί να χρησιμοποιηθούν ή τροποποιηθούν από κακόβουλους χρήστες ώστε να αποφύγουν τη χρέωση τους για την παροχή των υπηρεσιών.

6.2.3 Ελαττώματα σε γνωστούς ελέγχους ασφαλείας

Τα τρωτά σημεία σε καθιερωμένα συστήματα ασφαλείας θα πρέπει να θεωρηθούν απόλυτα σχετικά με το cloud computing εάν οι καινοτομίες του cloud προκαλούν άμεσα δυσκολίες στην υλοποίηση αυτών των ελέγχων ασφαλείας. Τέτοιου είδους αδυναμίες είναι γνώστες ως control challenges. Παρακάτω ακολουθούν τρία παραδείγματα τέτοιων αδυναμιών.

Πρώτον, τα εικονοποιημένα δίκτυα παρέχουν ανεπαρκή έλεγχο δικτύου. Με δεδομένη τη φύση των υπηρεσιών cloud η διαχειριστική πρόσβαση σε μια IaaS υποδομή δικτύου και η ικανότητα προσαρμογής της υποδομής δικτύου είναι τυπικά περιορισμένη, οπότε καθιερωμένοι έλεγχοι ασφάλειας όπως το IP-based network zoning δεν μπορούν να εφαρμοστούν. Επίσης καθιερωμένες τεχνικές όπως η σάρωση του δικτύου για εύρεση αδυναμιών συνήθως δεν επιτρέπονται από τους παρόχους IaaS καθώς οι σαρώσεις που γίνονται με πραγματικό σκοπό την ανίχνευση μιας βλάβης δεν μπορούν να διακριθούν από κάποια σάρωση ενός εισβολέα. Τέλος, τεχνολογίες όπως η εικονοποίηση υπονοούν ότι η κυκλοφορία του δικτύου γίνεται και στο πραγματικό δίκτυο αλλά και στο εικονικό, όπως για παράδειγμα συμβαίνει στην επικοινωνία δυο εικονικών μηχανών που φιλοξενούνται στον ίδιο server. Αυτά τα θέματα αποτελούν μια πρόκληση γιατί οι υπάρχουσες και δοκιμασμένες λύσεις για την ασφάλεια του δικτύου μπορεί να μη λειτουργούν σωστά σε ένα περιβάλλον cloud computing.

Δεύτερον, όπως επισημάνθηκε στο European Network and Information Security Agency study[45] , οι υποδομές cloud computing απαιτούν διαχείριση και αποθήκευση πολλών διαφορετικών ειδών κλειδιών. Επειδή οι εικονικές μηχανές δεν έχουν μια σταθερή υποδομή υλικού και το περιεχόμενο του cloud είναι γεωγραφικά κατανεμημένο, είναι πολύ δυσκολότερη η επιβολή καθιερωμένων μεθόδων ελέγχου

όπως το Hardware Security Module (HSM) στα κλειδιά που βρίσκονται σε υποδομές cloud.

Τέλος, οι μετρικές ασφάλειας δεν έχουν υιοθετηθεί στα συστήματα cloud. Προς το παρόν δεν υπάρχουν τυποποιημένες μέθοδοι μετρικών ασφάλειας τις οποίες οι πελάτες του cloud να μπορούν να χρησιμοποιούν για να παρατηρούν τη κατάσταση ασφάλειας των πόρων cloud που διαθέτουν.

6.2.4 Διαδεδομένες αδυναμίες στις προσφερόμενες υπηρεσίες Cloud

Παρόλο που το cloud computing είναι μια σχετικά νέα τεχνολογία , υπάρχουν ήδη πάρα πολλές υπηρεσίες cloud στην αγορά. Αρκετές από αυτές τις προσφερόμενες υπηρεσίες/εφαρμογές cloud έχουν αδύναμα σημεία, προσθέτοντας με αυτόν τον τρόπο πολλά τρωτά σημεία σε ένα σύστημα cloud computing. Παραδείγματα τέτοιων αδυναμιών περιλαμβάνουν αδυναμίες έγχυσης (injection vulnerabilities) και ανεπαρκή σχεδιασμό αυθεντικοποίησης.

Οι αδυναμίες έγχυσης αξιοποιούνται από κακόβουλες υπηρεσίες η εισαγωγές (inputs)εφαρμογών με σκοπό την διερμηνεία και την εκτέλεση τμημάτων του κώδικα τους, ενάντια στους σκοπούς του προγραμματιστή τους. Μερικά παραδείγματα αδυναμιών έγχυσης είναι :

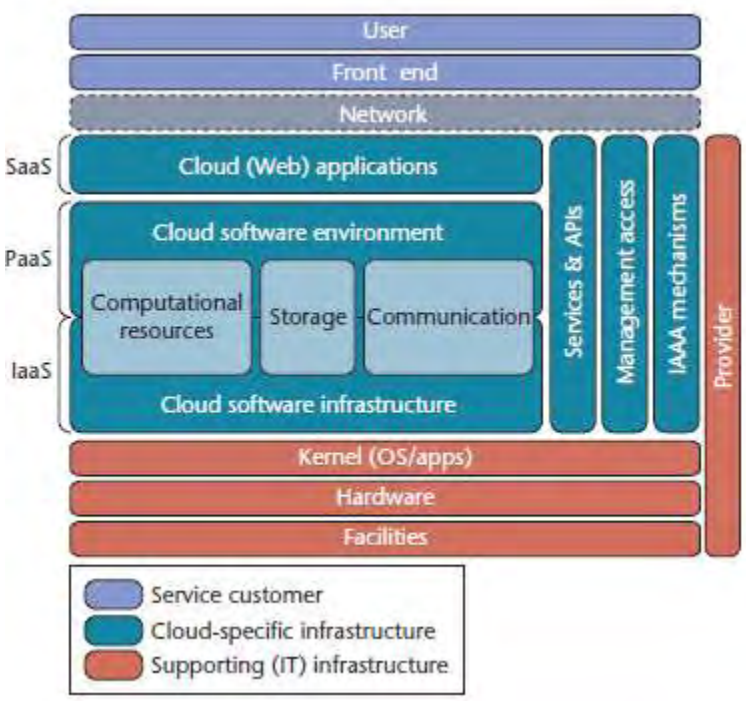
- ***SQL έγχυση***, στην οποία η είσοδος περιέχει κώδικα SQL ο όποιος εκτελείται λανθασμένα στη βάση δεδομένων.
- ***Έγχυση εντολών***, στην οποία η είσοδος περιέχει εντολές οι οποίες εκτελούνται λανθασμένα στο λειτουργικό σύστημα.
- ***Cross-site scripting***, στο οποίο η είσοδος περιέχει κώδικα JavaScript που εκτελείται λανθασμένα από τον browser του θύματος.

Επιπρόσθετα πολλοί ευρέως χρησιμοποιούμενοι μηχανισμοί αυθεντικοποίησης είναι ανεπαρκείς. Για παράδειγμα η χρήση username και password για την αυθεντικοποίηση ενός χρήστη είναι μια αδύναμη μέθοδος:

- Ο χρήστης μπορεί να χρησιμοποιεί αδύναμους κωδικούς, η να χρησιμοποιεί πολλές φορές τους ίδιους κωδικούς.
- Έμφυτοι περιορισμοί των μηχανισμών αυθεντικοποίησης που χρησιμοποιούν μόνο έναν παράγοντα αυθεντικοποίησης.

6.3 Αδυναμίες αρχιτεκτονικών συνιστωσών

Τα μοντέλα των cloud υπηρεσιών συνήθως χωρίζονται σε SaaS, PaaS και IaaS και κάθε μοντέλο επηρεάζει τα συγκεκριμένα αδύναμα σημεία μιας υποδομής cloud computing. Στην εικόνα παρατίθεται μια αναφορική αρχιτεκτονική που κάνει σαφείς τις πιο σημαντικές αδυναμίες των τμημάτων ενός συστήματος cloud.



Εικόνα 6.2: Αρχιτεκτονική του Cloud και τρωτά σημεία που αντιστοιχούν σε κάθε τμήμα της. [44]

Αυτή η αρχιτεκτονική βασίζεται στη δουλεία των University of California , Los Angeles και IBM, κληρονομεί χαρακτηριστικά από την αρχιτεκτονική με στρώματα, στα οποία μπορούν να στεγαστούν μια η παραπάνω υπηρεσίες. Η συγκεκριμένη αρχιτεκτονική έχει τρία κυρίως τμήματα :

- ***Supporting (IT) infrastructure:*** Αυτές είναι εγκαταστάσεις και υπηρεσίες γνωστές σε κάθε υπηρεσία της τεχνολογίας πληροφοριών. Συμπεριλαμβάνονται στην αρχιτεκτονική καθώς η ασφάλεια θα πρέπει να διατηρείται και για τα τμήματα των cloud υπηρεσιών τα οποία δεν είναι σχετικά με το cloud αυτό κάθε αυτό.

- ***Cloud-specific Infrastructure:*** Τα τμήματα αυτά αποτελούν τον πυρήνα μιας cloud υπηρεσίας και οποιαδήποτε αδυναμία η έλεγχος ασφάλειας θα πρέπει να σχεδιαστεί πάνω σε αυτά τα τμήματα.
- ***Cloud Service Consumer:*** Συμπεριλαμβάνεται στην αρχιτεκτονική καθώς αποτελεί μέρος της ασφάλειας στην γενικότερη μορφή της.

6.3.1 Υποδομή και περιβάλλον Cloud Λογισμικού

Το στρώμα της υποδομής λογισμικού του cloud παρέχει μια αφαίρεση των βασικών πόρων IT οι οποίες προσφέρονται ως υπηρεσία σε υψηλοτέρα στρώματα : υπολογιστικοί πόροι (συνήθως VMs), αποθηκευτικά μέσα, επικοινωνίες.

Το περιβάλλον λογισμικού cloud παρέχει υπηρεσίες στο επίπεδο της εφαρμογής πλατφόρμας:

- Ένα περιβάλλον ανάπτυξης και εκτέλεσης για υπηρεσίες και εφαρμογές που έχουν δημιουργηθεί με μια η περισσότερες υποστηριζόμενες γλώσσες προγραμματισμού
- Υπηρεσίες αποθήκευσης
- Υποδομή επικοινωνίας

Οι αδυναμίες στην υποδομή και στο περιβάλλον συνήθως αναφέρονται σε έναν από τους τρεις τύπους πόρων που παρέχονται από αυτά τα 2 στρώματα.

6.3.2 Υπολογιστικοί Πόροι

Ένα μεγάλο σύνολο αδυναμιών αφορά τον τρόπο με τον οποίο γίνεται ο χειρισμός των εικονικών μηχανών. Ο μόνος εφικτός τρόπος για την παροχή σχεδόν πανομοιότυπων στιγμιότυπων ενός server , παρέχοντας έτσι υπηρεσία κατ' απαίτηση για εικονικούς servers, είναι κοινοποιώντας στιγμιότυπα προτύπων.

Τα ευάλωτα στιγμιότυπα προτύπων μιας εικονικής μηχανής προκαλούν την εξάπλωση των αδυναμιών του λειτουργικού συστήματος η μιας εφαρμογής σε πολλά συστήματα. Ένας εισβολέας ίσως μπορέσει να αναλύσει τις ρυθμίσεις του συστήματος, το επίπεδο patch και τον κώδικα χρησιμοποιώντας διαχειριστικά δικαιώματα νοικιάζοντας έναν εικονικό server ως ένας πελάτης υπηρεσίας, κερδίζοντας έτσι γνώση που θα τον βοηθήσει σε επιθέσεις ενάντια σε στιγμιότυπα άλλων πελατών.

Η απώλεια δεδομένων από την αναπαραγωγή μιας εικονικής μηχανής είναι ένα αδύναμο σημείο που οφείλεται επίσης στη χρήση της κλωνοποίησης για την παροχή κατ' απαίτησης υπηρεσιών. Η κλωνοποίηση οδηγεί στο πρόβλημα της διαρροής δεδομένων αναφορικά με κάποια μυστικά στοιχειά της μηχανής, συγκεκριμένα στοιχειά του λειτουργικού θα πρέπει να είναι ιδιωτικά για ένα και μοναδικό host. Η κλωνοποίηση μπορεί να παραβιάσει αυτήν την υπόθεση ιδιοτικότητας.

Μπορεί να υπάρχουν επίσης αδυναμίες σχετικές με την κρυπτογραφία εξαιτίας της μη επαρκούς παραγωγής τυχαίων αριθμών εάν το επίπεδο αφαίρεσης ανάμεσα στο υλικό και τον kernel του λειτουργικού συστήματος είναι προβληματικό για την παράγωγη τυχαίων αριθμών σε ένα περιβάλλον εικονικής μηχανής.

6.3.3 Αποθήκευση

Πολλές πολιτικές ασφάλειας σχετικά με την αποθήκευση των δεδομένων είναι πολύ δύσκολο ή μερικές φορές ανέφικτο να υλοποιηθούν σε περιεχόμενο cloud. Για παράδειγμα οι πολιτικές καταστροφής δεδομένων που εφαρμόζονται στο τέλος του κύκλου ζωής ενός τόμου, απαιτούν την καταστροφή του δίσκου κάτι το οποίο δεν είναι επιτρεπτό εάν ο δίσκος χρησιμοποιείται από κάποιον άλλο χρήστη.

Η κρυπτογραφία χρησιμοποιείται τακτικά για να ξεπεραστούν αδυναμίες που έχουν άμεση σχέση με την αποθήκευση δεδομένων, για αυτό το λόγο αδυναμίες αυτής της τεχνολογίας, όπως η ανεπαρκής ή απαρχαιωμένη κρυπτογραφία, έχουν έναν κυρίαρχο ρόλο στην αποθήκευση δεδομένων στο cloud.

6.3.4 Επικοινωνίες

Το πιο αντιπροσωπευτικό παράδειγμα μιας υπηρεσίας επικοινωνίας cloud είναι η δικτύωση που παρέχεται για τα περιβάλλοντα εικονικών μηχανών σε ένα περιβάλλον IaaS. Εξαιτίας του Resource Pooling αρκετοί πελάτες είναι πιθανόν να μοιραστούν συγκεκριμένα τμήματα του δικτύου. Οι αδυναμίες κάποιων τμημάτων της υποδομής ενός διαμοιραζομένου δικτύου, όπως αδυναμίες σε έναν DNS server, Dynamic Host Configuration Protocol (DHCP), και αδυναμίες του πρωτοκόλλου IP μπορεί να καταστίσουν δυνατές τις επιθέσεις δικτύου ανάμεσα

σε χρήστες μιας IaaS υπηρεσίας. Όπως ειπώθηκε και παραπάνω, η εικονική δικτύωση αποτελεί επίσης μια πρόκληση ασφάλειας, γιατί κυκλοφορία υπάρχει όχι μόνο στο πραγματικό δίκτυο αλλά και στα εικονικά δίκτυα, όπως αυτά που δημιουργούνται όταν δυο εικονικές μηχανές που φιλοξενούνται στον ίδιο server επικοινωνούν μεταξύ τους. Κάτι τέτοιο καταλήγει στο ίδιο συμπέρασμα με παραπάνω, τα υπάρχοντα επίπεδα ασφάλειας ίσως να μη λειτουργήσουν σωστά σε ένα περιβάλλον cloud.

6.3.5 Εφαρμογές web

Μια εφαρμογή web χρησιμοποιεί την τεχνολογία ενός browser για την παροχή μιας διεπαφής με τον τελικό χρήστη. Ακολουθώντας την ανάπτυξη στις τεχνολογίες των browsers όπως η JavaScript, Java , Flash και Silverlight, μια web cloud εφαρμογή εντάσσεται σε μια από τις 2 κατηγορίες:

- Ένα τμήμα μιας εφαρμογής που εκτελείται κάπου μέσα στο cloud.
- Ένα τμήμα κάποιου browser που εκτελείται μέσα στον browser του χρήστη.

Στο μέλλον, οι προγραμματιστές θα χρησιμοποιούν όλο και περισσότερο τεχνολογίες, όπως το Google Gears[46], που επιτρέπουν την Offline χρήση του τμήματος του browser μιας εφαρμογής web για περιπτώσεις χρήσης που δεν απαιτούν διαρκή πρόσβαση σε απομακρυσμένα δεδομένα.

Κάποια αλλά τρωτά σημεία μιας web εφαρμογής εκτός του session riding και highjacking και τις απειλές μέσω injection που αναλύθηκαν παραπάνω, αφορούν το front-end μέρος ενός browser. Ανάμεσα τους είναι η κακόβουλη χρήση δεδομένων από την πλευρά του πελάτη, στις οποίες οι χρήστες επιτίθενται σε εφαρμογές Web τροποποιώντας τα δεδομένα που στέλνονται από τη δική τους εφαρμογή στο μέρος της εφαρμογής στην πλευρά του server, δηλαδή τα δεδομένα που λαμβάνονται από το τμήμα server δεν είναι αυτά που αναμένονται από τον πελάτη αλλά κάποια τροποποιημένα δεδομένα ή ακόμα και εντελώς νέα τα οποία δημιουργήθηκαν από τον χρήστη. Τέλος οι εφαρμογές Web βασίζονται στους μηχανισμούς ενός browser ώστε να απομονώσουν τυχόν περιεχόμενο που προέρχεται από τρίτους και έχει ενσωματωθεί στη εφαρμογή, όπως διαφημίσεις, banners κλπ.

6.3.6 Ταυτοποίηση, Αυθεντικοποίηση, Εξουσιοδότηση, Μηχανισμοί Ελέγχου

Όλες οι cloud υπηρεσίες απαιτούν μηχανισμούς για τη διαχείριση της ταυτοποίησης, αυθεντικοποίησης, εξουσιοδότησης και έλεγχου (IAAA). Μέχρι ενός βαθμού, τμήματα αυτών των υπηρεσιών μπορούν να χρησιμοποιηθούν ως μια αυτόνομη IAAA υπηρεσία που θα μπορεί να χρησιμοποιηθεί από άλλες υπηρεσίες. Δυο IAAA στοιχειά τα οποία πρέπει να είναι μέρος κάθε υλοποίησης μιας υπηρεσίας είναι η εκτέλεση επαρκούς αριθμού ελέγχων εξουσιοδότησης, και έλεγχο (auditing) της υποδομής του cloud.

Οι περισσότερες αδυναμίες που σχετίζονται με το τμήμα IAAA μιας υπηρεσίας πρέπει να θεωρηθούν και αδυναμίες ενός συστήματος cloud computing . Κάποια παραδείγματα ελλιπούς αυθεντικοποίησης ή εξουσιοδότησης είναι τα έξης:

- ***Denial of service λόγω κλειδώματος λογαριασμού (account lockout).*** Ένα μετρό ασφάλειας που χρησιμοποιείται συχνά είναι το κλείδωμα των λογαριασμών για τους οποίους έχουν ληφθεί πολλές αποτυχημένες προσπάθειες αυθεντικοποίησης σε μικρό χρονικό διάστημα. Ένας εισβολές μπορεί να χρησιμοποιήσει τέτοιου είδους αποτυχημένες προσπάθειες ώστε να πραγματοποιήσει DOS επιθέσεις εις βάρος κάποιου χρήστη.
- ***Ανεπαρκείς μηχανισμοί επαναφοράς πιστοποιητικών.*** Οι πάροχοι cloud computing υπηρεσιών διαχειρίζονται οι ίδιοι πιστοποιητικά χρηστών , οπότε θα πρέπει να παρέχουν κάποιους μηχανισμούς για την επαναφορά αυτών των πιστοποιητικών σε περιπτώσεις πιστοποιητικών που έχουν ξεχαστεί η χαθεί. Μηχανισμοί τέτοιου είδους έχουν αποδεδειχθεί αρκετά επισφαλείς στο παρελθόν.
- ***Ανεπαρκείς η λανθασμένοι έλεγχοι εξουσιοδότησης.*** Οι σύγχρονες web εφαρμογές και οι προσφερόμενες υπηρεσίες cloud είναι πολύ συχνά ευάλωτες στον ανεπαρκή ή λανθασμένο έλεγχο εξουσιοδότησης κάτι που μπορεί να οδηγήσει στη γνωστοποίηση απόρρητων πληροφοριών ή εκτέλεση πράξεων που απαιτούν εξουσιοδότηση σε μη εξουσιοδοτημένους χρηστές. Για παράδειγμα η έλλειψη ελέγχων εξουσιοδότησης είναι η βασική αιτία τον URL-guessing επιθέσεων, στις οποίες οι χρήστες τροποποιούν URLs για να εμφανίσουν πληροφορίες λογαριασμού άλλων χρηστών.
- ***Πρόχειρος έλεγχος εξουσιοδότησης .*** Οι διεπαφές διαχείρισης των cloud υπηρεσιών είναι συχνά επιρρεπείς στην προσφορά μοντέλων αυθεντικοποίησης τα οποία είναι πολύ πρόχειρα. Έτσι κάποια τυπικά μέτρα ασφαλείας όπως ο διαχωρισμός καθηκόντων δεν είναι δυνατόν να επιβληθούν γιατί είναι αδύνατη η επιβολή στους χρήστες μόνο εκείνων των προνομίων που αυστηρά απαιτούνται για την ολοκλήρωση μιας εργασίας.

- ***Ανεπαρκείς δυνατότητες παρακολούθησης και logging .*** Προς το παρόν δεν υπάρχουν πρότυπα η μηχανισμοί οι οποίοι να δίνουν στους χρήστες των υπηρεσιών cloud δυνατότητες logging και παρατήρησης των πόρων μέσα στις εγκαταστάσεις του cloud. Κάτι τέτοιο προκαλεί ένα σημαντικό πρόβλημα, τα αρχεία log καταγράφουν τα γεγονότα για όλους τους ενοίκους και δεν μπορούν εύκολα να απομονωθούν τα γεγονότα ενός συγκεκριμένου ενοίκου/χρήστη.

6.4 Βιβλιογραφία Κεφαλαίου

[1] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker: *Understanding Cloud Computing Vulnerabilities*

[2] Open Group's risk taxonomy : www. opengroup.org/onlinepubs/9699919899/toc.pdf

[3] *ISO/IEC 27005:2007 Information Technology—Security Techniques—Information Security Risk Management*, Int'l Org. Standardization, 2007.

[4] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Nov. 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

Κεφάλαιο 7

Ασφάλεια και Ιδιοτικότητα στο Cloud Computing

Περιεχόμενα

7.1 Εισαγωγή

Το Cloud Computing παρέχει πολλά πλεονεκτήματα τόσο στους χρήστες του όσο και στους παρόχους των υπηρεσιών του, για αυτό το λόγο εξελίσσεται με εκπληκτικό ρυθμό και αναμένεται να υιοθετηθεί από μεγάλο αριθμό χρηστών στο πρόσεχες μέλλον. Παρόλα αυτά όμως το θέμα της ασφάλειας και της διατήρησης της ιδιοτικότητας στέκονται εμπόδιο στην ευρεία υιοθέτηση του Cloud και στην χρήση των υπηρεσιών που αυτό προσφέρει. Οι χρήστες του Cloud Computing ανησυχούν για την ασφάλεια των επιχειρηματικών τους πληροφοριών και των κρίσιμης σημασίας πόρων τεχνολογίας στο σύστημα του Cloud Computing τα όποια μπορεί να είναι ευάλωτα σε επιθέσεις από τρίτους[47].

Επιπρόσθετα, πολλά περιστατικά σχετικά με την ασφάλεια και την διατήρηση της ιδιοτικότητας σε σημερινά εμπορικά προϊόντα Cloud Computing έχουν παρατηρηθεί επιδεινώνοντας αυτήν την ανησυχία των υποψήφιων πελατών. Οι ασφάλεια και η ιδιοτικότητα που παρέχουν οι σημερινές εταιρίες δεν είναι επαρκής, δημιουργώντας έτσι ένα μεγάλο εμπόδιο για την υιοθέτηση του cloud computing από μεγαλύτερο αριθμό πελατών.[48]

7.2 Ασφάλεια κατ'απαίτηση

Οι υπηρεσίες cloud είναι εφαρμογές που εκτελούνται σε κάποιο μέρος της υποδομής ενός cloud computing συστήματος μέσω ενός εσωτερικού δικτύου ή του internet. Οι χρήστες δεν χρειάζεται να γνωρίζουν σε ποιο ακριβώς μέρος αποθηκεύονται τα δεδομένα ή σε ποιο μέρος παρέχονται οι υπηρεσίες. Οι πάροχοι μπορούν να αναπτύξουν, να εγκαταστήσουν και να εκτελέσουν εφαρμογές οι οποίες με πολύ εύκολο τρόπο μπορούν να μεγαλώσουν σε χωρητικότητα/ικανότητα (scalability), να έχουν αυξημένη απόδοση (performance), και σπάνια να αντιμετωπίζουν βλάβες/λάθη (reliability). Το μειονέκτημα του cloud computing στην προσπάθεια του να εξασφαλίσει αυτές τις ιδιότητες είναι η αποθήκευση των προσωπικών δεδομένων κάθε πελάτη στην άλλη πλευρά του internet και η ανάμιξη τρίτων πρόσωπων που παρέχουν υπηρεσίες, κάτι το όποιο έχει ως αποτέλεσμα την ύπαρξη προβλημάτων ασφάλειας και ιδιοτικότητας.

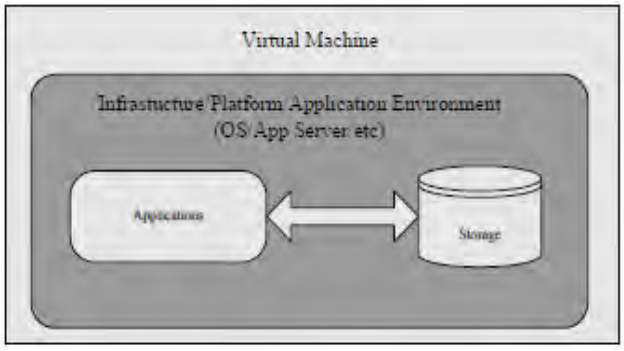
Ένα σύστημα cloud computing θεωρείται ασφαλές όταν οι πελάτες μπορούν αν βασιστούν στο γεγονός ότι αυτό θα λειτουργεί με τον τρόπο που αναμένουν οι χρηστές. Παραδοσιακά υπάρχουν πέντε στόχοι που χαρακτηρίζουν την ασφάλεια σε ένα υπολογιστικό σύστημα: διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα δεδομένων, ρύθμιση και έλεγχος.

7.2.1 Διαθεσιμότητα

Η διαθεσιμότητα σε ένα σύστημα Cloud Computing απαιτεί την διατήρηση της λειτουργιάς της υπηρεσίας έτσι ώστε οι χρήστες να μπορούν να την χρησιμοποιήσουν οποιαδήποτε ώρα, από οποιοδήποτε μέρος. Δυο στρατηγικές χρησιμοποιούνται κυρίως για την ενίσχυση της διαθεσιμότητας των συστημάτων cloud ή των εφαρμογών που φιλοξενούνται σε αυτά, η σκλήρυνση (hardening), και ο πλεονασμός.

Πολλές εταιρίες παραγωγής υπηρεσιών cloud computing παρέχουν υποδομές και πλατφόρμες cloud που βασίζονται σε εικονικές μηχανές. Οι εικονικές αυτές μηχανές μπορούν να ικανοποιήσουν ξεχωριστές απαιτήσεις μνήμης, δίσκου, CPU τα όποια αποτελούν μέρη ενός μεγάλου αριθμού υπολογιστών του εμπορίου , παρέχοντας έτσι τη δυνατότητα στους παρόχους cloud υπηρεσιών να δανείζονται υπολογιστικούς πόρους κατ' απαίτηση . Έτσι η εικονική μηχανή είναι το βασικό μέρος για τη φιλοξενία αυτών των υπηρεσιών. Οι εικονικές μηχανές έχουν τη δυνατότητα λοιπόν να παρέχουν υπηρεσίες κατ' απαίτηση, ανάλογα με την επιθυμία του χρήστη για μια συγκεκριμένη ποσότητα πόρων, για μεγάλο αριθμό χρηστών. Από την άλλη μεριά οι πωλητές cloud συστημάτων βασίζονται στην εικονική μηχανή για το συνδυασμό πολλών υπολογιστών του εμπορίου ή servers ώστε να παρέχουν ένα κλιμακούμενο, ισχυρό σύστημα.

Οι σημερινοί πωλητές συστημάτων Cloud που παρέχουν υποδομές και πλατφόρμες βασιζόμενες στη χρήση εικονικών μηχανών, όπως η Amazon, προσφέρουν τη δυνατότητα μπλοκαρίσματος και φιλτραρίσματος της κυκλοφορίας βασιζόμενοι στην διεύθυνση IP του αποστολέα με σκοπό να εξασφαλίσουν τα συστήματα τους, παρόλα αυτά όμως αυτές οι υπηρεσίες δεν είναι ανάλογες με τις υπηρεσίες ασφάλειας των δικτύων στις περισσότερες μεγάλες επιχειρήσεις. Αυτές οι στρατηγικές ασφάλειας αναπτύσσονται μέσα στην εικονική μηχανή που χρησιμοποιούν, η όποια με τη σειρά της βελτιώνει τη διαθεσιμότητα.



Εικόνα 7.1: Η εικονική μηχανή ως Υποδομή/Πλατφόρμα. [48]

Όσων άφορα τον πλεονασμό, οι μεγάλοι πωλητές συστημάτων cloud παρέχουν γεωγραφικό πλεονασμό στα συστήματα τους, επιτρέποντας έτσι μεγάλη διαθεσιμότητα στους παρόδους των cloud υπηρεσιών. Για παράδειγμα η Amazon οικοδομεί data centers σε πολλαπλές περιοχές και πολλαπλές ζώνες διαθεσιμότητας μέσα σε αυτές τις περιοχές. Οι ζώνες διαθεσιμότητας είναι διακριτές θέσεις σχεδιασμένες έτσι ώστε να προστατεύονται από βλάβες/αποτυχίες σε άλλες ζώνες διαθεσιμότητας και να παρέχουν φθηνή, χαμηλής καθυστέρησης (low latency) συνδεσιμότητα σε άλλες ζώνες διαθεσιμότητας στην ιδία περιοχή. Με αυτόν τον τρόπο οι εφαρμογές μπορούν να προστατευτούν από βλάβες που συμβαίνουν σε μια συγκεκριμένη τοποθεσία.

7.2.2 Εμπιστευτικότητα

Η εμπιστευτικότητα σε ένα σύστημα cloud computing έχει να κάνει με τη διατήρηση των δεδομένων του χρήστη κρυφή. Η εμπιστευτικότητα αποτελεί ένα μεγάλο εμπόδιο για τους χρήστες του cloud computing, καθώς δεν εμπιστεύονται το cloud για την διατήρηση των δεδομένων τους. Υπάρχουν δυο κυρίες προσεγγίσεις για την επίτευξη της εμπιστευτικότητας που έχουν υιοθετηθεί σε μεγάλο βαθμό από τους πωλητές cloud συστημάτων, η φυσική απομόνωση και η κρυπτογραφία.

Οι υπηρεσίες του cloud computing μεταδίδονται πάνω από δημόσιας χρήσης δίκτυα. Έτσι δεν μπορεί να επιτευχτεί φυσική απομόνωση, για αυτό το λόγο θα πρέπει να αναπτυχτούν και να χρησιμοποιηθούν Virtual Local Area Networks και ενδιάμεσα σταδία ασφάλειας στο δίκτυο όπως firewalls και φίλτρα πακέτων για να επιτευχτεί αυτή η φυσική απομόνωση.

Η κρυπτογράφηση των δεδομένων του χρήστη είναι ένας άλλος τρόπος για την διασφάλιση της εμπιστευτικότητας. Για παράδειγμα η κρυπτογράφηση των δεδομένων πριν την τοποθέτηση τους στο cloud μπορεί να είναι πολύ πιο ασφαλής από την τοποθέτηση τους χωρίς κρυπτογράφηση σε ένα τοπικό data center.

7.2.3 Ακεραιότητα Δεδομένων

Η ακεραιότητα των δεδομένων σε ένα σύστημα cloud σημαίνει τη διατήρηση της ακεραιότητας της πληροφορίας, για παράδειγμα τη μη τροποποίηση ή διαγράφη της από μη εξουσιοδοτημένους χρηστές. Η διατήρηση της ακεραιότητας των δεδομένων είναι μια θεμελιώδης εργασία καθώς τα δεδομένα αποτελούν τη βάση των cloud computing υπηρεσιών, όπως της SaaS, PaaS και DaaS.

Ένα σύστημα cloud computing συνήθως παρέχει τεράστιες δυνατότητες επεξεργασίας δεδομένων, ο χειρισμός τόσο μεγάλου όγκου δεδομένων σημαίνει Tera Bytes η ακόμη και

Peta Bytes δεδομένων σε κάθε τόμο. Οι προκλήσεις για τη διατήρηση της ακεραιότητας των δεδομένων σε ένα σύστημα cloud είναι οι ακόλουθες. Αρχικά, η εξέλιξη των σκληρών δίσκων δεν συμβαδίζει με αυτήν της πληροφορίας, δηλαδή η χωρητικότητα τους δεν μπορεί να συγκριθεί με το μέγεθος των πληροφοριών που χρειάζονται αποθήκευση. Έτσι για να διατηρήσουν την κλιμάκωση στην αποθήκευση της πληροφορίας, οι πωλητές cloud συστημάτων πρέπει να αυξήσουν τον αριθμό σκληρών δίσκων στις εγκαταστάσεις τους. Αυτό με τη σειρά του μπορεί να προκαλέσει αυξημένη πιθανότητα είτε αποτυχίας κόμβου είτε αποτυχίας ενός δίσκου, αλλά ακόμα και φθορά και απώλεια δεδομένων. Δεύτερον, οι σκληροί δίσκοι γίνονται όλο και μεγαλύτεροι αναφορικά με την χωρητικότητα τους ενώ παραμένουν σχεδόν στάσιμοι στην προσφερόμενη ταχύτητα πρόσβασης στα δεδομένα.

Η ψηφιακή υπογραφή είναι μια συνήθης τεχνική για έλεγχο της ακεραιότητας των δεδομένων. Τα ευρέως διαδεδομένα κατανεμημένα συστήματα αρχείων όπως το GFS και HDFS συνήθως διαχωρίζουν τα δεδομένα που βρίσκονται σε μεγάλους τόμους, σε μπλοκ πληροφορίας το καθένα από τα όποια έχει προκαθορισμένο μέγεθος, για παράδειγμα 64MB ή 128MB. Όταν ένα μπλοκ δεδομένων αποθηκεύεται, μια ψηφιακή υπογραφή επισυνάπτεται σε αυτό. Αυτή τη υπογραφή είναι χρήσιμη για την πραγματοποίηση μελλοντικών ελέγχων ακεραιότητας των δεδομένων, και σε περίπτωση προβλήματος ανάνηψης τους από φθορές.

7.2.4 Έλεγχος

Ο έλεγχος σε ένα σύστημα cloud σημαίνει τη ρύθμιση της χρήσης του συστήματος, συμπεριλαμβανόμενου των εφαρμογών, της υποδομής και των δεδομένων.

Ένα σύστημα cloud computing πάντοτε περιλαμβάνει κατανεμημένους υπολογισμούς σε μεγάλης κλίμακας σύνολα δεδομένων ανάμεσα σε μεγάλο αριθμό από κόμβους υπολογιστών . Ακόμη, κάθε χρήστης του internet μπορεί να ανεβάσει τα δικά του ατομικά δεδομένα στο σύστημα cloud computing το όποιο βρίσκεται στην άλλη άκρη του internet και να τα χρησιμοποιήσει σε κάποια άλλη χρονική στιγμή. Για παράδειγμα το κάθε κλικ που κάνει κάποιος χρήστης κατά την περιήγηση του σε διαφόρους δικτυακούς χώρους μπορεί να χρησιμοποιηθεί για στοχευόμενες διαφημίσεις. Όταν προσωπικά δεδομένα όπως αυτά αποθηκεύονται σε ένα cloud σύστημα οι χρήστες του μπορεί να πέσουν θύματα υποκλοπής .

Για αυτό το λόγο χρειάζεται αποδοτικός και αποτελεσματικός έλεγχος στην πρόσβαση στα δεδομένα που βρίσκονται αποθηκευμένα σε ένα σύστημα cloud computing και καθορισμός της συμπεριφοράς των εφαρμογών και υπηρεσιών που στεγάζονται σε αυτό .

7.2.5 Audit

Το Audit αναφέρεται στην παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα Cloud Computing . Το χαρακτηριστικό αυτό θα μπορούσε να προστεθεί ως ένα επιπλέον στρώμα πάνω από το εικονοποιημένο λειτουργικό σύστημα, ή το εικονοποιημένο περιβάλλον εφαρμογών που φιλοξενείται στην εικονική μηχανή, με σκοπό να παρέχει δυνατότητες παρακολούθησης του συστήματος. Υπάρχουν τρία κυρίως πράγματα που θα έπρεπε να παρακολουθηθούν:

- ***Γεγονότα:*** Οι αλλαγές κατάστασης και άλλοι παράγοντες που επηρεάζουν την διαθεσιμότητα του συστήματος.
- ***Logs:*** Πληροφορίες σχετικά με τις εφαρμογές του κάθε χρήστη και το περιβάλλον εκτέλεσης του.
- ***Παρακολούθηση(Monitoring):*** Δεν θα πρέπει να παρεμβαίνει στις δραστηριότητες των χρηστών, και θα πρέπει να περιορίζεται μονό στα στοιχειά που χρειάζεται ο πάροχος για να επιτελέσει το έργο του.

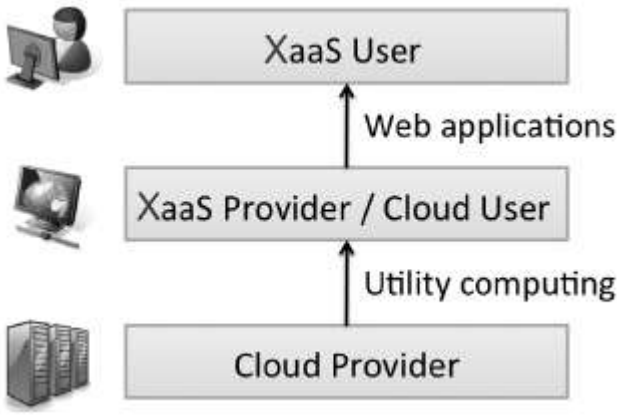
7.3 Ιδιοτικότητα κατ'απαίτηση

Ένα σύστημα Cloud Computing συνήθως προσφέρει υπηρεσίες στην άλλη άκρη του διαδικτύου και χρειάζεται κάποιες προσωπικές πληροφορίες του χρήστη για να το κάνει. Αυτές οι πληροφορίες αποθηκεύονται και διαχειρίζονται από τους παρόχους των υπηρεσιών, κάτι που έχει ως αποτέλεσμα την ανησυχία των πελατών τους σχετικά με την διατήρηση της ιδιοτικότητας. Θέματα ιδιοτικότητας υπάρχουν εδώ και πολύ καιρό στην επιστήμη των υπολογιστών, και πολλοί νόμοι έχουν θεσπιστεί με σκοπό να προστατευόσουν την ατομική ιδιοτικότητα ενός ανθρώπου αλλά και τα επιχειρηματικά μυστικά. Παρόλα αυτά οι περισσότεροι από αυτούς τους νόμους είναι απαρχαιωμένοι και μη εφαρμόσιμοι στα σημερινά δεδομένα όπου αναπτύσσεται μια σχέση μεταξύ χρηστών και παρόχων.

7.3.1 Νομικά ζητήματα

Τα συστήματα Cloud Computing έχουν σημαντικές επιπτώσεις στην ιδιοτικότητα των προσωπικών πληροφοριών αλλά και των επιχειρηματικών και κυβερνητικών πληροφοριών και αυτό γιατί οποιουδήποτε είδους πληροφορία μεταφέρεται από τοπικούς υπολογιστές στο cloud, συμπεριλαμβανόμενου e-mails, φωτογραφίες, παρουσιάσεις και οποιοδήποτε άλλο είδος πληροφορίας μπορεί να αποθηκευτεί σε έναν ηλεκτρονικό υπολογιστή. Ακόμη, ολόκληρο το περιεχόμενο της πληροφορίας που ο χρήστης είχε αποθηκευμένο σε μια τοπική συσκευή, τώρα μπορεί να μεταφερθεί σε όχι μόνον ένα πάροχο υπηρεσίας cloud, αλλά στις περισσότερες των περιπτώσεων, σε πολλούς διαφορετικούς παρόχους. Όποτε λοιπόν ένα άτομο, μια επιχείρηση ή κάποια άλλη οντότητα μοιραστεί πληροφορίες στο cloud μπορεί να προκύψουν θέματα εμπιστευτικότητας η ιδιοτικότητας.

Η σχέση μεταξύ χρηστών και παρόχων σε ένα σύστημα cloud computing είναι ποιο πολύπλοκη από αυτές στις συνηθισμένες υπηρεσίες web. Εμπεριέχει 3 ρόλους: Τον πάροχο Cloud , τον πάροχο XaaS/ χρήστη Cloud και τον XaaS χρήστη. Ο XaaS χρήστης είναι ένας πελάτης, ή πιθανός πελάτης μιας υπηρεσίας cloud computing, ο οποίος μπορεί να είναι ένα άτομο μια επιχείρηση, μια κυβερνητική υπηρεσία ή κάποια άλλη οντότητα. Ο πάροχος XaaS είναι ο οργανισμός που προσφέρει την υπηρεσία Cloud Computing ο όποιος είναι επίσης χρήστης του συστήματος cloud computing . Ο πάροχος cloud είναι ένας οργανισμός που προσφέρει το σύστημα cloud computing. Αυτό που πρέπει να σημειωθεί είναι ότι ο πάροχος της υπηρεσίας είναι ένα τρίτο πρόσωπο που κρατά πληροφορίες που αφορούν μια άλλη οντότητα, ή εκ μέρους μιας άλλης οντότητας.



Εικόνα 7.2: Χρήστες και πάροχοι του Cloud Computing. [48]

Οι περισσότεροι νόμοι δεν μπορούν να εφαρμοστούν σε αυτό το νέο περιβάλλον κυρίως εξαιτίας της ύπαρξης αυτού του τρίτου πρόσωπου καθώς αυτοί οι νόμοι έχουν εκδοθεί αρκετό καιρό πριν και προστατεύουν μονό τις σχέσεις ανάμεσα σε δυο μέρη.

7.3.2 Ζητήματα πολλαπλής τοποθεσίας

Ο σκοπός ενός συστήματος cloud computing είναι να προσφέρει τεράστιες ποσότητες υπολογιστικών πόρων στους χρήστες, περιλαμβάνοντας υποδομές, πλατφόρμες και υπηρεσίες. Έτσι οι επιχειρήσεις οφείλουν να εμπιστευτούν τους πωλητές συστημάτων cloud ώστε να αποθηκεύσουν στα συστήματα αυτές τις τυχόν ευαίσθητες πληροφορίες τους και αυτό γιατί στην ουσία τα προσωπικά τους δεδομένα είναι αποθηκευμένα στον υπολογιστή κάποιου αλλού. Κάτι τέτοιο συνεπάγεται κίνδυνο για τους χρήστες των cloud υπηρεσιών. Για παράδειγμα ο πάροχος μιας cloud υπηρεσίας μπορεί να αποφασίσει να σταματήσει τις εργασίες του, ή να κρατήσει τα δεδομένα «όμηρο» εάν προκύψει μια διαφωνία. Επιπλέον οι μεγάλοι πωλητές cloud συστημάτων έχουν τα cloud mirror sites τους σε πολλές διαφορετικές χώρες. Για παράδειγμα το EC2 της Amazon στεγάζεται πολλές διαφορετικές τοποθεσίες, ένα μέρος του βρίσκεται στις ΗΠΑ και το υπόλοιπο στην Ευρώπη. Το AppEngine της Google στεγάζεται σε πολλές τοποθεσίες επίσης, όπως οι ΗΠΑ, η Κίνα και άλλες. Τα προβλήματα που μπορεί να προκύψουν εάν τα ευαίσθητα δεδομένα αποθηκευτούν σε πολλαπλές τοποθεσίες είναι τα παρακάτω :

- ***Τοποθέτηση σε πολλαπλές τοποθεσίες (Multi-location) των ιδιωτικών δεδομένων:*** Θεωρείται αρκετά επικίνδυνο για μια επιχείρηση να αποθηκεύσει τα ευαίσθητα δεδομένα της σε συσκευές κάποιου τρίτου. Κάτι τέτοιο μπορεί να προκαλέσει πολλά προβλήματα. Πρώτον ο πάροχος της υπηρεσίας cloud μπορεί να σταματήσει τις εργασίες του. Δεύτερον μπορεί να αποφασίσει να κρατήσει τα δεδομένα «όμηρο» εάν προκύψει κάποια διαμάχη. Τρίτον θα ήταν αρκετά σημαντικό για μια εταιρία να γνωρίζει σε ποια χωρά θα φιλοξενηθούν τα δεδομένα της και αυτό διότι η τοποθεσία των δεδομένων επηρεάζει άμεσα τους νόμους που θα επιβληθούν σε αυτά τα ευαίσθητα δεδομένα. Για παράδειγμα εάν τα δεδομένα αποθηκευτούν στην Κίνα, ο Κινέζικος νομός μπορεί να επιτρέψει στην Κινεζική κυβέρνηση την απεριόριστη πρόσβαση σε αυτά τα δεδομένα και ότι αυτό συνεπάγεται.
- ***Τοποθέτηση σε πολλαπλές τοποθεσίες (Multi-location) του παρόχου της υπηρεσίας:*** Ο πελάτης της υπηρεσίας cloud χρειάζεται επίσης να γνωρίζει τον τρόπο με τον όποιο ο πάροχος της υπηρεσίας cloud εκτελεί τις εργασίες για τις

οποίες έχει δεσμευτεί. Έτσι ο πελάτης θα πρέπει να διατηρεί άμεση σχέση με τον πάροχο της υπηρεσίας και να έχει τον έλεγχο πάνω στα δικά του προσωπικά δεδομένα.

- ***Συνδυασμός και επικάλυψη δεδομένων (combination and commingling):*** Ο πελάτης θα πρέπει αν διαβεβαιωθεί για το εάν τα προσωπικά του δεδομένα είναι αποθηκευμένα ξεχωριστά από αυτά άλλων πελατών η όχι. Εάν είναι συνενωμένα η διαπλεγμένα με δεδομένα άλλων πελατών τότε ο κίνδυνος είναι μεγαλύτερος. Για παράδειγμα κάποιοι ιοί μπορεί να μεταδοθούν από τον ένα πελάτη στον άλλο, εάν κάποιος πελάτης πέσει θύμα μιας επίθεσης hacker τότε είναι πολύ πιθανό να επηρεαστεί η διαθεσιμότητα και η ακεραιότητα των δεδομένων και των υπόλοιπων πελατών που βρίσκονται στο ίδιο περιβάλλον.
- ***Περιορισμοί σε τεχνικές και λογιστικές:*** Είναι πολύ δύσκολο, αν όχι αδύνατο για έναν πάροχο cloud υπηρεσιών να διαβεβαιώσει έναν πελάτη για την τοποθεσία στην όποια βρίσκονται τα δεδομένα του, για παράδειγμα η Amazon έχει data centers σε όλο τον κόσμο, τα δεδομένα του πελάτη αποθηκεύονται αυτόματα ανάμεσα τους, εκτός εάν η Amazon χρησιμοποιήσει συγκεκριμένους servers για τον συγκεκριμένο πελάτη.
- ***Μεταφορά δεδομένων σε άλλες χώρες:*** Εάν κάποια παγκόσμια εταιρία αποφασίσει να χρησιμοποιήσει τις υπηρεσίες cloud computing πρέπει να γνωρίζει επακριβώς ποιες χώρες θα στεγάζουν τα δεδομένα της και θα παρέχουν τις υπηρεσίες cloud, καθώς και τους νόμους που θα ισχύουν για αυτά τα δεδομένα. Για παράδειγμα μια Γερμανική εταιρία μπορεί να μην έχει αντίθεση να χρησιμοποιήσει υπηρεσίες cloud που παρέχονται στην Αργεντινή, αλλά να μη συμφωνήσει με τη μεταφορά της στην Τουρκιά ή στο Μέξικο. Η εκ των προτέρων γνώση για την τοποθεσία στην οποία θα αποθηκευτούν τα δεδομένα είναι προαπαιτούμενη για την γνώση του τρόπου με τον οποίο τα δεδομένα ή οι υπηρεσίες που παρέχονται θα μεταφερθούν τυχόν από χωρά σε χωρά.

7.4 Βιβλιογραφία Κεφαλαίου

[1] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou*: "Security and Privacy in Cloud Computing: A Survey"*

[2] C. Wang, Forrester: A close look at cloud computing security issues *http://www.forrester.com/securityforum2009*, 2009.

[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, *"Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley, Tech. Rep*, 2009.

[4] IDC, "*It cloud services user survey, pt.2: Top benefits & challenges," http://blogs.idc.com/ie/?p=210*, 2008.

Συνολική Βιβλιογραφία

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, *"Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley,Tech. Rep*, 2009.

[2] White Paper: Introduction to cloud computing, ThinkGrid Business IT On Demand

[3] Cloud Computing For Dummies, HP Special Edition, Wiley Publishing Inc.

[4] Emmanuel Marilly, Olivier Martinot, Htlkne Papini, Danny Goderis: *Service level Agreements: A Main Challenge For Next Generation Networks*

[5] Pankesh Patel, Ajith Ranabahu1, Amit Sheth: *Service Level Agreement in Cloud Computing*

[6] Organization for the advancement of structured information standards. [Online]. Available: http://www.oasis-open.org

[7] Mohammad Hadi Valipour, Bavar Amirzafari, Khashayar Niki Maleki and Negin Daneshpour: *A Brief Survey of Software Architecture Concepts and Service Oriented Architecture*

[8] Systems Engineering at MITRE : Service-Oriented Architecture (SOA) Series

[9] Brian Carpenter : "*Grid Computing, ISOC Member Briefing #11"*

[10] Lamia Youseff, Maria Butrico Dilma Da Silva : *Toward a Unified Ontology of Cloud Computing*

[11] Salesforce.com. http://salesforce.com

[12] "Apex: Salesforce on-demand programming language and framework," http://developer.force.com/.

[13] Marc Seeger: "*Key-Value stores: A Practical Overview"*

[14] "EMC Managed Storage Service," http://www.emc.com/

[15] "Microsoft Connected Service Framework, http://www.microsoft.com/serviceproviders/solutions/connectedservicesframework.mspx

[16] I. Foster and C. Kesselman, "Globus: A metacomputing infrastructure toolkit," *International Journal of Supercomputer Applications*, 1997.

[17] T. Tannenbaum and M. Litzkow, "The condor distributed processing system," *Dr. Dobbs Journal*, February 1995

[18] C.N. Höfer · G. Karagiannis : Cloud computing services: taxonomy and comparison

[19] Mell P, Grance T (2009) The NIST definition of cloud computing (v15). Tech Rep, National Institute of Standards and Technology

[20] Thin Client: http://en.wikipedia.org/wiki/Thin_client

[21] Google Apps. http://www.google.com/apps

[22] Citrix Systems, Inc. Xen hypervisor. http://www.xen.org

[23] Youseff L, Butrico M, Da Silva D (2008) Toward a unified ontology of cloud computing. In: Grid computing environments workshop,GCE'08, pp 1–10

[24] Pay-as you-go :http://en.wikipedia.org/wiki/Compensation_methods

[25] Hilley D (2009) Cloud computing: a taxonomy of platform and infrastructure-level offerings. Tech Rep GIT-CERCS-09-13,CERCS, Georgia Institute of Technology

[26] DMTF Cloud Computing Incubator. http://www.dmtf.org/about/cloud-incubator

[27] Sun Microsystems: *"Introduction to cloud computing Architecture"*, White paper 1st edition,June 2009

[28] Amazon Web Services, aws.amazon.com

[29] Amazon Elastic Computing Cloud, aws.amazon.com/ec2

[30] XenSource Inc, Xen, www.xensource.com

[31] Berners-Lee T, Fielding R, Masinter L (2005) RFC 3986: uniform resource identifier (URI): generic syntax, January 2005

[32] Windows Azure, www.microsoft.com/azure

[33] Google App Engine, URL http://code.google.com/appengine

[34] Chang F, Dean J et al (2006) Bigtable: a distributed storage system for structured data. In: Proc of OSDI

[35] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong : *The Characteristics of Cloud Computing*

[36]InfinityBand: http://en.wikipedia.org/wiki/InfiniBand

[37] Qi Zhang · Lu Cheng · Raouf Boutaba**:** *Cloud computing: state-of-the-art and research challenges*

[38] Guo C, Lu G, Li D et al (2009) BCube: a high performance, server-centric network architecture for modular data centers. In: Proc SIGCOMM

[39] Ghemawat S, Gobioff H, Leung S-T (2003): The Google file system.In: Proc of SOSP, October 2003

[40] Hadoop Distributed File System, hadoop.apache.org/hdfs

[41] Dean J, Ghemawat S (2004) MapReduce: simplified data processing on large clusters. In: Proc of OSDI

[42] *ISO/IEC 27005:2007 Information Technology—Security Techniques—Information Security Risk Management*, Int'l Org. Standardization, 2007.

[43] Open Group's risk taxonomy : www. opengroup.org/onlinepubs/9699919899/toc.pdf

[44] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker: *Understanding Cloud Computing Vulnerabilities*

[45] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Nov. 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[46] Google Gears: http://gears.google.com/

[47] C. Wang, "Forrester: A close look at cloud computing security issues," *http://www.forrester.com/securityforum2009*, 2009.

[48] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou*:* "*Security and Privacy in Cloud Computing: A Survey"*