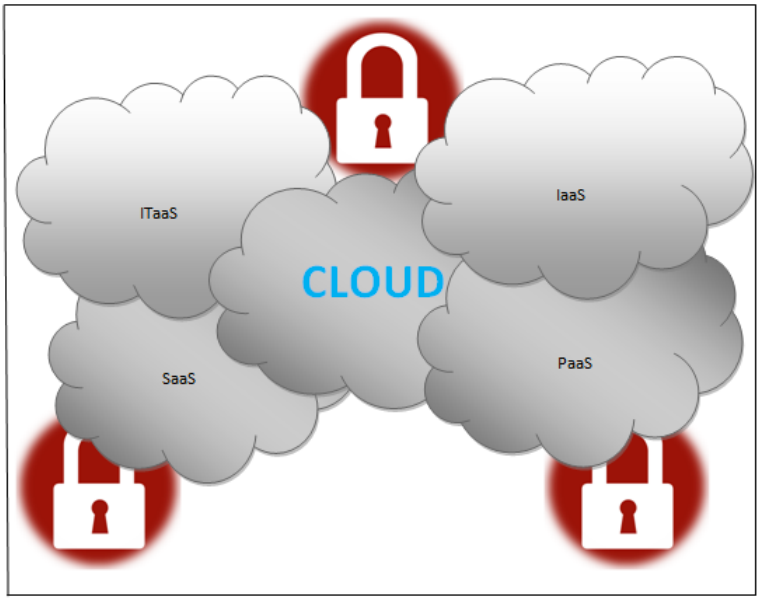
ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια στο Cloud Computing



Του φοιτητή

Πέτρου Γιαννούλη

Αρ. Μητρώου: 052785

Επιβλέπων καθηγητής

Χρήστος Ηλιούδης

Θεσσαλονίκη 2012

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία ασχολείται με το ζήτημα της ασφάλειας στο Cloud Computing. Αρχικά αναλύεται η έννοια του Cloud Computing καθώς αποτελεί ένα νέο τεχνολογικό πεδίο, έπειτα γίνεται μια προσπάθεια να εντοπιστούν τα βασικότερα ζητήματα ασφάλειας καθώς και λύσεις στα ζητήματα αυτά. Τέλος δημιουργείται ένα Cloud με τις υποδομές του τμήματος Πληροφορικής προκειμένου να κατανοήσουμε στην πράξη το Cloud Computing και να αποτελέσει την βάση για περαιτέρω έρευνα πάνω στο αντικείμενο αυτό.

Εκπονήθηκε στη Θεσσαλονίκη το 2012 ως προαπαιτούμενο της αποφοίτησής μου από το τμήμα πληροφορικής του Αλεξάνδρειου Τεχνολογικού Εκπαιδευτικού Ιδρύματος της Θεσσαλονίκης (ΑΤΕΙΘ).

ΠΕΡΙΛΗΨΗ

Το cloud computing είναι ένα ταχέως αναπτυσσόμενο μοντέλο που εισάγει καινοτόμες έννοιες και πτυχές σε σχέση με το παραδοσιακό μοντέλο διανομής. Μέσα στην βιασύνη των εταιριών να υιοθετήσουν το cloud προκύπτουν ζητήματα ασφάλειας που πρέπει να αναλυθούν και να επιλυθούν.

Στο πρώτο κεφάλαιο δίνεται ο ορισμός του cloud computing και αναλύεται η αρχιτεκτονική της υποδομής του. Στο δεύτερο κεφάλαιο αναλύονται τα ζητήματα ασφάλειας που προκύπτουν σε αυτό το νέο μοντέλο και προτείνονται λύσεις για την αντιμετώπιση τους. Στο τρίτο κεφάλαιο περιγράφονται οι μεγαλύτεροι πάροχοι υπηρεσιών cloud και υλοποιείται ένα ιδιωτικό cloud εντός του δικτύου του ΑΤΕΙΘ.

ABSTRACT

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities in compare of traditional delivery model. As companies are increasingly claiming to be “cloudy” new aspects of security are coming up, those aspects are necessary to be analyzed and solved.

At first chapter cloud computing defined and analyzed the architecture of infrastructure, at second chapter analyzed the security aspects and propose solutions. At third chapter analyzed the most important cloud services providers and implement a private cloud into the network of ATEI of Thessaloniki.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή αυτής της εργασίας Ηλιούδη Χρήστο για την αμέριστη συμπαράσταση του σε όλα τα επίπεδα ακαδημαϊκά και μη, καθώς και τον Χαρχαλάκη Στέφανο και Ψαρρά Νίκο για την τεχνική βοήθεια που μου προσέφεραν.

Ως ελάχιστη ευγνωμοσύνη για το Τμήμα Πληροφορικής που εκτός από την ακαδημαϊκή γνώση που μου προσέφερε, συνέβαλε τα μέγιστα ώστε να διαμορφωθεί ο χαρακτήρας μου από χρόνο σε χρόνο, θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου και ιδιαιτέρως τους κυρίους : Σταμάτη Δημοσθένη, Κότσιαλο Ευθύμιο, Μάργαρη Αθανάσιο, Γουλιάνα Κωνσταντίνο, Βαφειάδη Αντώνιο και Κατωπόδη Κωνσταντίνο για τις αξίες και το μεράκι που μου μετέδωσαν.

Τέλος θα ήθελα να ευχαριστήσω τους συμφοιτητές μου, με τους οποίους μοιραστήκαμε το όνειρο για έναν καλύτερο κόσμο και με την ορμή της νιότης ζήσαμε όμορφες στιγμές. Εύχομαι να συνεχίσουμε να τα λέμε στους δρόμους..

Αφιερώνω την εργασία αυτή στην οικογένεια μου και ιδιαίτερα στους γονείς μου Ιωάννη και Ευγενία Γιαννούλη που με προσωπικές θυσίες φρόντισαν να μην μου λείψει τίποτα όλα αυτά τα χρόνια, στάθηκαν και στέκονται δίπλα μου σε κάθε μου βήμα.

Στον άνθρωπο που μοιράζομαι την ζωή μου για την ενθάρρυνση και την συμπαράσταση του..

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Στόχος της πτυχιακής εργασίας είναι αρχικά να δοθεί ένας ορισμός σχετικά με το τι είναι cloud computing, έπειτα να προσδιοριστούν τα ζητήματα ασφάλειας που σχετίζονται με αυτή την νέα αρχιτεκτονική και να προταθούν λύσεις αντιμετώπισης τους. Τέλος στόχος είναι να υλοποιηθεί εντός του δικτύου του ΑΤΕΙΘ και με υποδομές του Τμήματος Πληροφορικής ένα cloud που θα αποτελέσει την βάση για περαιτέρω μελέτη.

Στο πρώτο κεφάλαιο δίνεται ο ορισμός του cloud computing και αναλύεται η αρχιτεκτονική του δομή. Στο δεύτερο κεφάλαιο περιγράφονται τα ζητήματα ασφάλειας και ορισμένες λύσεις. Στο τρίτο κεφάλαιο παρουσιάζονται οι βασικότεροι πάροχοι υπηρεσιών cloud, πλατφόρμες υλοποίησης cloud ανοιχτού κώδικά και υλοποιείται ένα cloud με την πλατφόρμα Eucalyptus.

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

ΕΙΣΑΓΩΓΗ

Η άνοδος του cloud computing είναι κάτι παραπάνω από μία ακόμα πλατφόρμα που θα κάνει τους λάτρεις του χώρου να ενθουσιαστούν. Είναι βέβαιο ότι θα μεταλλάξει την βιομηχανία IT, αλλά και τον τρόπο που οι άνθρωποι δουλεύουν και τον τρόπο που οι εταιρείες λειτουργούν.

-The Economist, “Let it Rise,” 10/23/08

1.1 Το πρόβλημα που μελετάει η πτυχιακή

Cloud: πολλά περισσότερα από φτηνή υπολογιστική

Το cloud computing φέρνει ένα νέο επίπεδο αποδοτικότητας και οικονομίας στην παροχή πόρων IT κατά απαίτηση και στις διαδικασίες νέων επιχειρηματικών μοντέλων και στις επιχειρηματικές ευκαιρίες.

Ενώ πολλοί άνθρωποι σκέφτονται το τρέχον cloud computing ως μια πλατφόρμα παροχής “πληρωμής σύμφωνα με την χρήση ” στην πραγματικότητα είναι μια σύγκλιση δύο μεγάλων και αλληλοεξαρτώμενων τάσεων :

Αποδοτικότητα IT – Ελαχιστοποίηση του κόστους όπου οι εταιρείες έχουν μειώσει τις κεφαλαιουχικές δαπάνες για λειτουργικά έξοδα μέσω τις τεχνολογίας της εικονικοποίησης . Το cloud computing ξεκινά ως ένας τρόπος για τη βελτίωση των υποδομών, ανάπτυξη και αξιοποίηση των πόρων, αλλά και την πλήρη αξιοποίηση αυτής της υποδομής και τελικά οδηγεί σε ένα νέο μοντέλο ανάπτυξης εφαρμογών.

Ευελιξία Επιχειρήσεων - Μεγιστοποίηση της απόδοσης χρησιμοποιώντας την ως ανταγωνιστικό όπλο μέσω της ταχείας διείσδυσης στην αγορά, ολοκληρωμένη στοίβα εφαρμογών , ανάπτυξη εικονικών μηχανών και παράλληλο προγραμματισμό. Το cloud computing έχει καταφέρει να φέρει την επανάσταση του χρόνου στην υπηρεσία αλλά αναπόφευκτα αυτές οι υπηρεσίες θα πρέπει να βασίζονται σε εξίσου ταχέα αναπτυσσόμενα μοντέλα υποδομής.

Οι τάσεις αυτές υπήρχαν στην βιομηχανία IT για χρόνια ωστόσο οι πρόσφατη μαζική ανάδυση της ταχύτητας των δικτύων και των τεχνολογιών εικονικότητας έστρεψε αυτή την τάση σε μια νέα προσανατολισμένη στις υπηρεσίες υποδομή.

Το cloud computing επιτρέπει στους οργανισμούς να αυξήσουν τα ποσοστά χρήσης του υλικού δραματικά, και να κλιμακωθούν μέχρι και σε τεράστιες χωρητικότητες σε μια στιγμή - χωρίς συνεχώς να χρειάζεται να επενδύουν σε νέες υποδομές, την εκπαίδευση νέου προσωπικού, ή να αγοράσουν άδειες για νέο

λογισμικό. Δημιουργεί, επίσης νέες ευκαιρίες για καλύτερες υπηρεσίες δικτύου, σε λιγότερο χρόνο, με λιγότερα χρήματα.

Μέχρι το 2011, θα μειωθούν οι κεφαλαιουχικές δαπάνες
για εφαρμογές τεχνολογίας και το 40% αυτών των δαπανών για υποδομή θα μεταφερθεί στο cloud.
-Δελτίο Τύπου της Gartner, «Η Gartner επισημαίνει τις βασικές προβλέψεις για Οργανισμούς IT και χρήστες απο το 2008 και πέρα, "1/31/08

Το cloud computing έχει να κάνει με την αποτελεσματικότητα. Παρέχει έναν τρόπο για την ανάπτυξη και την πρόσβαση σε όλα, από απλά συστήματα μέχρι τεράστιες ποσότητες πόρων IT – κατά απαίτηση , σε πραγματικό χρόνο και σε προσιτή τιμή. Καθιστά διαθέσιμη υψηλής απόδοσης υπολογιστική ισχύ και υψηλής χωρητικότητας αποθήκευσης σε οποιονδήποτε με μια πιστωτική κάρτα. Και δεδομένου ότι το cloud βασίζεται σε εργαλεία που οι προγραμματιστές γνωρίζουν ήδη, επαναπροσδιορίζεται η σχέση μεταξύ της τεχνολογίας πληροφοριών και των προγραμματιστών καθώς και των επιχειρηματικών μονάδων που εξαρτώνται από αυτήν.

Μείωση των κεφαλαιουχικών δαπανών - Το cloud computing καθιστά δυνατό για τις επιχειρήσεις να μειώσουν το κόστος των λειτουργικών δαπανών μέσω τεχνολογιών όπως το virtualization.

Μείωση του κόστος λειτουργίας ενός κέντρου δεδομένων - Το cloud computing βελτιώνει τις υποδομές,τα ποσοστά χρησιμοποίησης και απλοποιεί τη διαχείριση των πόρων. Για παράδειγμα, το cloud επιτρέπει αυτοπροσδιορισμό των πόρων μέσω APIs, φέρνοντας ένα υψηλότερο επίπεδο αυτοματοποίησης στο κέντρο δεδομένων και τη μείωση του κόστους διαχείρισης.

Μείωση των υπερβολικών προβλέψεων – Το cloud παρέχει κλιμάκωση κατά απαίτηση έτσι οι εταιρείες μπορούν στιγμιαία να απαιτήσουν πόρους για να ανταπεξέλθουν στις ανάγκες τους χωρίς την ανάγκη προηγούμενης πρόβλεψης.

Ένα παράδειγμα που εξηγεί γιατί είναι σημαντικό το cloud και πώς επηρεάζει τους οργανισμούς είναι η New York Times που χρειάστηκε να μετατρέψει 11 εκατομμύρια άρθρα και εικόνες από το αρχείο της (από το 1851 εώς το 1980) σε pdf. Το τμήμα IT της εταιρείας προέβλεψε πως θα χρειαστεί εφτά εβδομάδες για αυτήν την διαδικασία. Αντίθετα ένας προγραμματιστής που χρησιμοποίησε 100 στιγμιότυπα που έτρεχαν το Hadoop μέσω το Amazon EC2 ολοκλήρωσε την εργασία αυτή σε μόλις 24 ώρες κα με κόστος λιγότερο από 300 δολάρια.

—open.blogs.nytimes.com, “Self-service, Prorated Super Computing Fun!” 11/1/07, open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/

Το cloud computing μαζί με τις καινοτομίες που φέρνει κουβαλάει μέσα του και τις παθογένειες των υπαρχόντων συστημάτων που το αποτελούν καθώς και νέες που προκύπτουν από την καινούργια αυτή πλατφόρμα. Έτσι τα ζητήματα ασφάλειας είναι ένας από τους βασικότερους φραγμούς για να υιοθετήσει κάποιος την νέα αυτή πλατφόρμα.

1.2 Οι στόχοι της πτυχιακής

Στόχος της πτυχιακής εργασίας είναι να μελετήσει και να ορίσει τι είναι το cloud computing καθώς και αναπτύξει λεπτομερώς την αρχιτεκτονική δομή αυτού. Αναλύεται το μοντέλο διανομής του cloud (SaaS, IaaS , PaaS) και το μοντέλο εφαρμογής του cloud (Public, Private, Hydrid) . Επίσης θα μελετηθούν οι κυριότεροι λόγοι για την υιοθέτηση του cloud και της επίδρασης του στους οργανισμούς και τις επιχειρήσεις. Επίσης θα μελετηθεί το ζήτημα της ασφάλειας στο cloud computing όπως αυτό παρουσιάζεται με βάση την αρχιτεκτονική δομή του cloud από την υποδομή μέχρι τον τελικό χρήστη και θα προταθούν τεχνολογικές λύσεις για την εξάλειψη των προβλημάτων ασφάλειας που προκύπτουν. Και τέλος στόχος είναι να υλοποιηθεί μια πειραματική εφαρμογή λειτουργίας ενός cloud computing με υλική υποδομή του τμήματος Πληροφορικής προκειμένου να μελετήσουμε στην πράξη τον τρόπο εγκατάστασης και λειτουργίας του.

1.3 Η μεθοδολογία

Αρχικά θα μελετήσουμε την αρχιτεκτονική δομή του cloud, (framework, data centers, μοντέλο διανομής και εφαρμογής). Έπειτα θα αναλύσουμε τα ζητήματα ασφάλειας που προκύπτουν από αυτή την αρχιτεκτονική και θα εξηγήσουμε γιατί προτείνουμε τις συγκεκριμένες τεχνολογίες ως λύση στα ζητήματα ασφάλειας. Τέλος θα παρουσιάσουμε τους σημαντικότερους παρόχους cloud και το τι αυτοί προσφέρουν και θα παρουσιάσουμε ορισμένα ανοιχτά περιβάλλοντα υλοποίησης cloud και θα επιλεγεί ένα από αυτά για την δική μας πειραματική υλοποίηση.

1.4 Η Διάρθρωση της πτυχιακής

Στο δεύτερο κεφάλαιο δίνεται ο ορισμός του cloud computing και αναλύεται το πλαίσιο εργασίας (framework). Έπειτα γίνεται μια αναλυτική παρουσίαση του μοντέλου διανομής και εφαρμογής του cloud. Και τέλος προσεγγίζεται το cloud

από την οικονομική του διάσταση τι αλλαγές επιφέρει στους οργανισμούς και γιατί αξίζει να προτιμηθεί έναντι άλλων υπολογιστικών μοντέλων.

Στο τρίτο κεφάλαιο εξετάζονται τα ζητήματα ασφάλειας που προκύπτουν στο cloud σύμφωνα με την αρχιτεκτονική του δομή, δίνονται παραδείγματα επιθέσεων και αναλύεται το ποιος έχει την ευθύνη της ασφάλειας ανάλογα το επίπεδο του cloud στο οποίο βρισκόμαστε. Τέλος αναλύεται το Σύνορο Εμπιστοσύνης και Διαχείριση Ταυτοποίησης και Πρόσβασης (IAM- Identity and Access Management).

Στο τέταρτο κεφάλαιο προσπαθώντας να υλοποιήσουμε ένα cloud computing παρουσιάζονται οι βασικότεροι πάροχοι του χώρου και οι υπηρεσίες που αυτοί προσφέρουν. Έπειτα παρουσιάζονται ορισμένες πλατφόρμες υλοποίησης cloud computing ανοιχτού κώδικα προκειμένου να επιλέξουμε μια από αυτές για την πειραματική μας υλοποίηση.

Και τέλος στο πέμπτο κεφάλαιο υλοποιείται πειραματικά ένα cloud computing με υποδομές του τμήματος πληροφορικής. Περιγράφεται ο τρόπος λειτουργίας του και τα εργαλεία διαχείρισης Euca2ools και Hydrifox.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό παρουσιάστηκε το πρόβλημα που μελετά η πτυχιακή εργασία, τους στόχους που έχουν τεθεί, η μεθοδολογία που θα ακολουθηθεί και τέλος η δομή των επόμενων κεφαλαίων. Στο επόμενο κεφάλαιο θα γίνει η πρώτη επαφή με το cloud computing.

ΚΕΦΑΛΑΙΟ 2 Cloud Computing

ΕΙΣΑΓΩΓΗ

Το cloud computing μπορεί να φαντάζει ως τεχνολογία του μέλλοντος, ωστόσο γυρνώντας πίσω στο χρόνο βλέπουμε πώς ο ανθρώπινος πολιτισμός πέρασε τρείς κυρίως φάσεις εξέλιξης. Στην πρώτη φάση έχουμε την εποχή της γεωργίας, στην δεύτερη φάση την εποχή της βιομηχανικής επανάστασης και τέλος στην τρίτη φάση την εποχή της πληροφορίας. Το πέρασμα όμως από την μία εποχή στην άλλη δεν έγινε ακαριαία, έτσι μέσα σε κάθε εποχή έχουμε πολλές και σημαντικές υπό-φάσεις Σε αυτή λοιπόν την μετά-βιομηχανική εποχή της πληροφορίας είναι η αρχή αυτού που πολλοί αποκαλούν εποχή του cloud computing

2.1 Ορισμός του Cloud Computing

Ο όρος cloud έχει τις ρίζες στου στην αρχή του internet όπου συνήθιζαν να το αναπαριστούν ως ένα σύννεφο λόγω της αφαιρετικότητας που προσέδιδε στον χρήστη ως προς τις υποδομές που βρισκόντουσαν πίσω από αυτό. Το cloud computing όμως βασίζεται σε πέντε βασικά χαρακτηριστικά(Mather κ.α., 2009): πολλαπλή μίσθωση , ευρεία κλιμάκωση ,ελαστικότητα, πληρωμή ανάλογα με την χρήση, και αυτοκαθορισμός των πόρων

Πολλαπλή Μίσθωση (Shared resources)

Σε αντίθεση με τα προηγούμενα υπολογιστικά μοντέλα(mainframe, minicomputer, προσωπικοί υπολογιστές, Client/Server, IP δίκτυα, φορητές συσκευές) τα οποία παρείχαν τους υπολογιστικούς πόρους αποκλειστικά σε έναν χρήστη ή ιδιοκτήτη, το cloud computing βασίζεται σε ένα επιχειρησιακό πλάνο στο οποίο οι πόροι μοιράζονται (πολλοί χρήστες χρησιμοποιούν τους ίδιους πόρους) σε επίπεδο δικτύου, σε επίπεδο φιλοξενίας(host level), και σε επίπεδο εφαρμογής.

Ευρεία Κλιμάκωση

Αν και οι οργανισμοί θα μπορούσαν να διαθέτουν εκατοντάδες ή χιλιάδες υπολογιστικά συστήματα, το cloud παρέχει την δυνατότητα να ανέρθουν σε δεκάδες χιλιάδες καθώς και την δυνατότητα να αυξηθεί μαζικά το εύρος ζώνης(bandwith) και ο αποθηκευτικός χώρος.

Ελαστικότητα

Οι χρήστες μπορούν γρήγορα να αυξήσουν ή να μειώσουν τους υπολογιστικούς πόρους σύμφωνα με τις ανάγκες τους, καθώς και να αποδεσμεύσουν πόρους για να χρησιμοποιηθούν από άλλους χρήστες, όταν αυτοί δεν τους χρειάζονται πλέον.

Πληρωμή ανάλογα με την χρήση

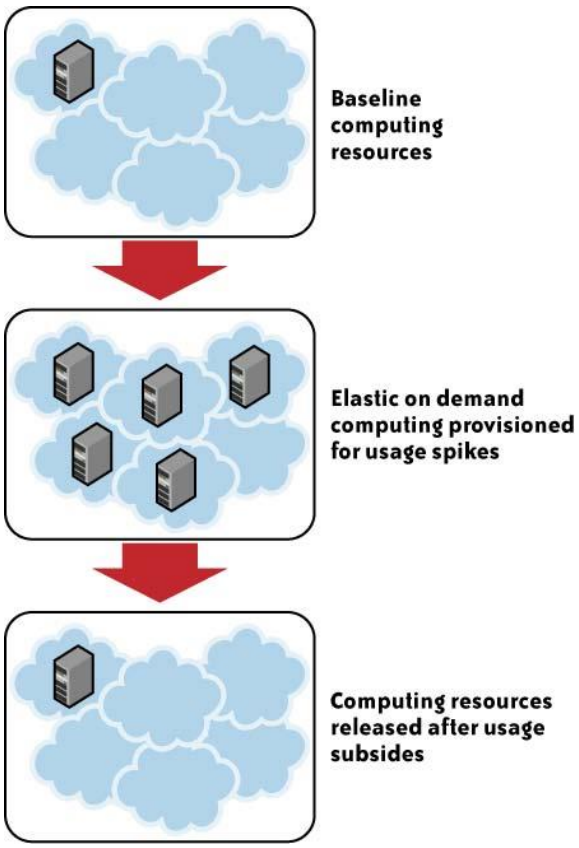
Οι χρήστες πληρώνουν μόνο για τους πόρους που χρησιμοποιούν και μόνο για όσο χρόνο τους χρειάζονται.

Αυτοκαθορισμός των πόρων

Οι χρήστες προβλέπουν μόνοι τους τις ανάγκες σε πόρους, όπως επιπλέον συστήματα(επεξεργαστική ικανότητα, λογισμικό, αποθήκευση) και πόρους δικτύου.

Ένα από τα χαρακτηριστικά του cloud computing είναι η ελαστικότητα(elasticity) στην χρήση των πόρων. Αυτή η δυνατότητα του cloud επιτρέπει στους χρήστες να αυξάνουν ή να μειώνουν τους υπολογιστικούς πόρους σύμφωνα με τις ανάγκες τους, Εικόνα 2-1. Συνήθως υπάρχει επίγνωση των βασικών αναγκών σε πόρους αλλά το να προβλεφθούν μελλοντικές ανάγκες είναι αρκετά δύσκολο ειδικά όταν οι απαιτήσεις αλλάζουν συχνά. Το cloud παρέχει τα μέσα αυτά ώστε να παρέχει πόρους τεχνολογίας πληροφορικής κατά απαίτηση και να ανταπεξέρχεται στις μέγιστες απαιτήσεις.

Εικόνα 2.1.Χαρακτηριστικό της Ελαστικότητας

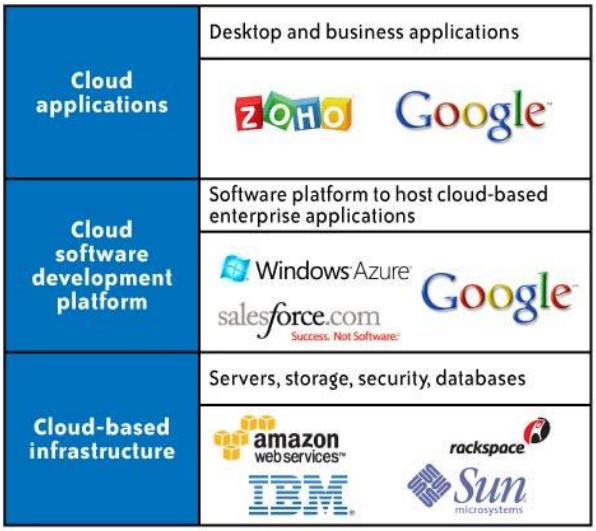


Το ενδιαφέρον γύρω από το cloud αυξάνεται καθώς παρέχει πρόσβαση στους χρήστες σε πόρους που μέχρι σήμερα βλέπαμε σε υπέρ-υπολογιστές. Η πρόσβαση αυτή, σε συνάρτηση του κόστους/χρήσης καθίσταται πιο εφικτή από ποτέ. Επιπλέον οι λύσεις που παρέχει μπορούν να αποκτιούνται κατά απαίτηση του χρήστη, το δίκτυο γίνεται ο υπερ-υπολογιστής στο cloud όπου οι χρήστες μπορούν να αγοράζουν ότι χρειάζονται όταν το χρειάζονται. Το cloud παρέχει υπό μορφή υπηρεσίας προς τους χρήστες υποστήριξη σε τεχνολογίες πληροφορικής οι οποίες γίνονται προσβάσιμες μέσω της τεχνολογίας του διαδικτύου.

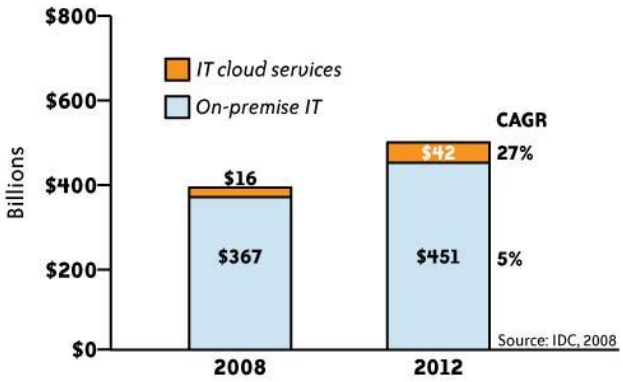
Το cloud computing έχει δημιουργήσει ιδιαίτερο ενδιαφέρον στην αγορά και αναμένεται να έχει μεγάλη ανάπτυξη όπως φαίνεται στην εικόνα 1.2 η οποία επισημαίνει τις πρόσφατες αξιοσημείωτες εξελίξεις του, καθώς και τα τωρινά αλλά και μελλοντικά αναμενόμενα έσοδα του.

Εικόνα 2.2 Πρόσφατες αξιοσημείωτες υπηρεσίες και επενδύσεις σε cloud υπηρεσίες

Recent notable cloud launches



Worldwide IT spending by consumption 2008, 2012

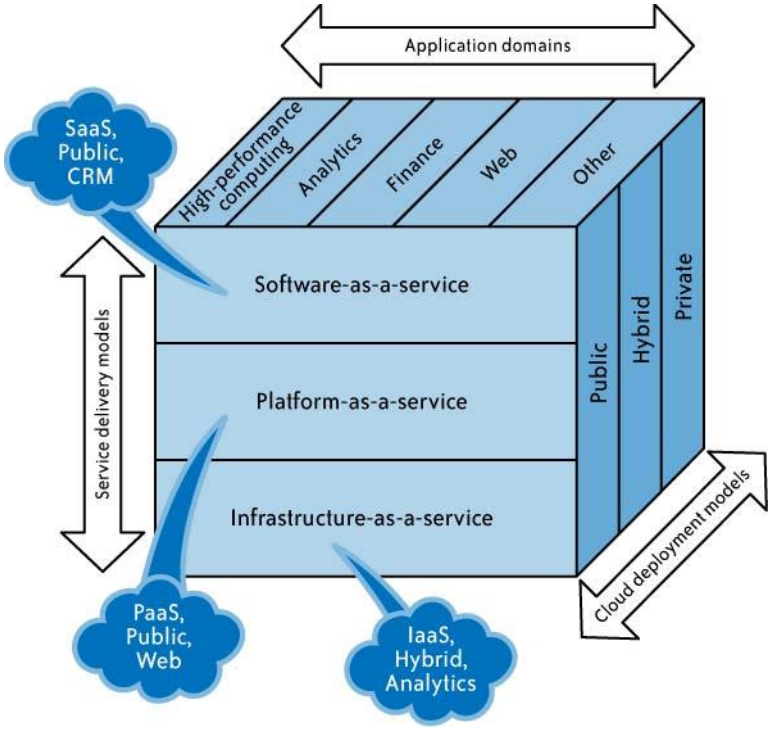


Το cloud computing αναμένεται να έχει μια σημαντική αύξηση επενδύσεων σε τεχνολογίες πληροφορικής σε παγκόσμιο επίπεδο. Είναι γεγονός ότι οι υπηρεσίες του cloud αναμένεται να έχουν έναν αυξανόμενο ενιαίο ετήσιο ρυθμό ανάπτυξης της τάξης του 27% και να φτάσουν τα 42 δισεκατομμύρια δολάρια μέχρι το 2012.Ενώ οι επενδύσεις σε υπηρεσίες που δεν ανήκουν στο cloud αναμένεται να έχουν ανάπτυξη κατά 5% σύμφωνα με το IDC(International Data Corporation, http://www.idc.com/getdoc.jsp?sessionId=&containerId=prMY21726709&sessionId=JC4TVLQ0F4XZICQJAFICFFAKBEAUMIWD , 17/1/2010).

2.2 Το SPI πλαίσιο εργασίας(framework) για το Cloud Computing

Μια κοινά αποδεκτή προσέγγιση που περιγράφει τις υπηρεσίες του cloud computing ακολουθεί το ακρωνύμιο “SPI”.Το ακρωνύμιο αυτό βασίζεται στις τρείς κύριες υπηρεσίες που παρέχονται μέσα από το cloud: λογισμικό ως υπηρεσία(software-as-a-service-SaaS), πλατφόρμα ως υπηρεσία (platform-as-a-service-PaaS), και υποδομή ως υπηρεσία (Infrastracture-as-a-Service-IaaS). Η εικόνα 1.3 απεικονίζει την σχέση μεταξύ των υπηρεσιών, της χρήσης, και τα είδη του cloud.

Εικόνα 1.3 Μοντέλο υπηρεσιών SPI

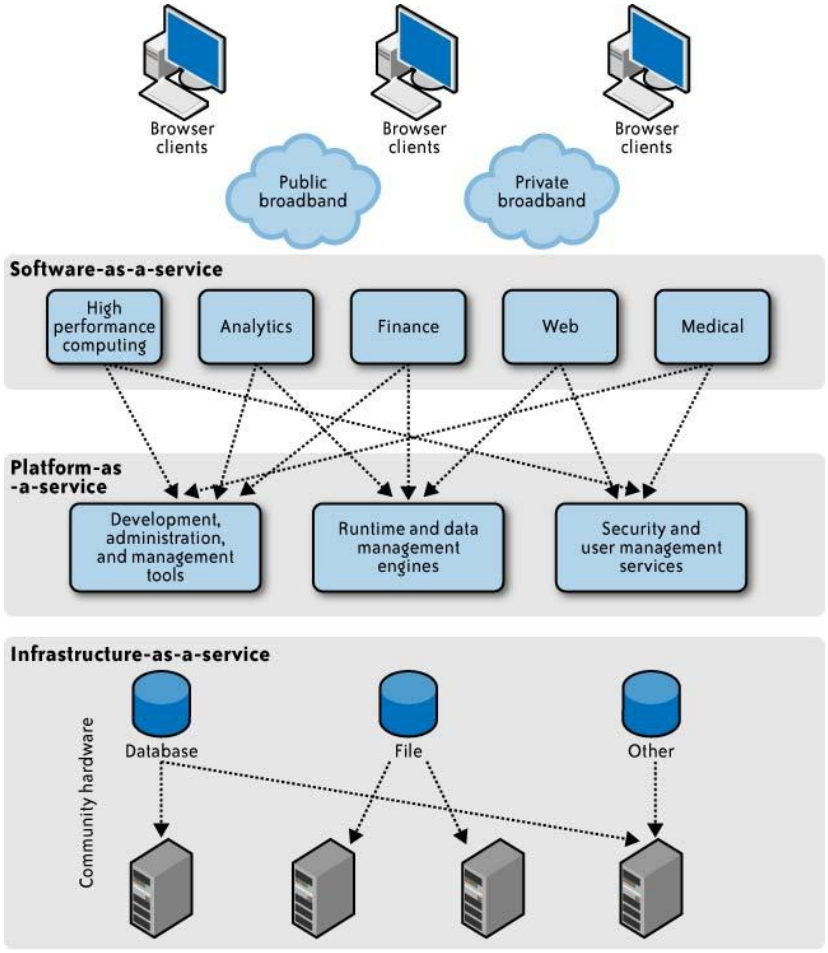


2.2.1 Σχετικές Τεχνολογίες στο Cloud Computing

Το cloud computing δεν χαρακτηρίζεται από μόνο του ως μια τεχνολογία αλλά ως συνδυασμός από πολλές προϋπάρχουσες τεχνολογίες. Οι τεχνολογίες αυτές ωρίμασαν σε διαφορετικό βαθμό και με διαφορετικό περιεχόμενο, και δεν σχεδιάστηκαν με μία λογική συνέπια. Ωστόσο συνδυάστηκαν ώστε να

δημιουργήσουν ένα τεχνητό οικοσύστημα για το cloud computing. Σύγχρονες καινοτομίες σε επεξεργαστές, τεχνολογίες εικονικότητας (virtualization technologies), αποθηκευτικά μέσα, ευρυζωνικές συνδέσεις Internet και γρήγοροι, φτηνοί εξυπηρετητές (servers) συνδυάστηκαν για να κάνουν το cloud μια πιο ελκυστική λύση. Η εικόνα 2.4 απεικονίζει τις σχετικές τεχνολογίες.

Εικόνα 2.4 Αρχιτεκτονική των σχετικών τεχνολογιών.



2.2.2 Συσκευές πρόσβασης στο Cloud

Το εύρος των συσκευών πρόσβασης στο cloud έχει εξαπλωθεί τα τελευταία χρόνια. Οικιακοί προσωπικοί υπολογιστές, εταιρικοί προσωπικοί υπολογιστές, δικτυακοί υπολογιστές, φορητές τηλεφωνικές συσκευές, συνήθης συσκευές χειρός, και συνήθης

σταθερές συσκευές(συμπεριλαμβανομένων και των ψυγείων) είναι συνδεδεμένες. Ενδιαφέρον παρουσιάζει η ανάπτυξη του iPhone και η εξάπλωση των διαθέσιμων εφαρμογών από το App Store η οποία δείχνει εμφανώς μια βελτίωση της πρόσβασης στο cloud. Η ευρύτερη πρόσβαση έχει ως αποτέλεσμα την μεγαλύτερη χρήση και την μεγαλύτερη αύξηση των υπηρεσιών στο cloud. Για παράδειγμα κάποιος μπορεί να χρησιμοποιήσει το Skype μέσα από το iPhone, αυτό φέρνει πιο κοντά στους χρήστες ένα peer-to-peer δίκτυο, επίσης η εταιρεία Salesforce.com έχει παρουσιάσει μια εφαρμογή που επιτρέπει τους χρήστες να έχουν πρόσβαση στις υπηρεσίες της από το iPhone όπως και από πολλούς άλλους κατασκευαστές

2.2.3 Φυλλομετρητές (Browsers) και thin clients

Χρήστες διαφορετικού τύπου συσκευών μπορούν να έχουν πρόσβαση σε εφαρμογές και πληροφορίες από οπουδήποτε μπορούν να φορτώσουν έναν browser.Πραγματικά οι browsers γίνονται όλο και περισσότερο πολύπλοκοι και εξεζητημένοι. Επαγγελματικές εφαρμογές όπως το SAP και η Oracle μπορούν να είναι προσβάσιμες μέσα από μια διεπαφή browser χωρίς να χρειάζεται να εγκατασταθεί και να φορτωθεί στην μεριά του χρήστη επιπλέον λογισμικό. Το μεγαλύτερο μέρος των χρηστών είναι εξοικειωμένο με την χρήση του browser και μπορούν να χειριστούν διαισθητικά το περιβάλλον διαφορετικών εφαρμογών χωρίς να απαιτείτε επιπλέον εκπαίδευση ή εγχειρίδια χρήσης

2.2.4 Υψηλών ταχυτήτων ευρυζωνική πρόσβαση

Ένα κρίσιμο χαρακτηριστικό του cloud computing είναι το ευρυζωνικό δίκτυο το οποίο παρέχει τα μέσα ώστε να συνδέονται τα επί μέρους συστατικά του, ορίζοντας έτσι την ουσιαστικότερη διαφορά από την αρχή της γενικής χρήσης υπολογιστή όπως ήταν πριν 30 χρόνια. Η ευρυζωνική πρόσβαση είναι πλέον ευρέως διαθέσιμη , ειδικά σε μητροπολιτικές περιοχές σε παγκόσμιο επίπεδο. Η διείσδυση της ασύρματης πρόσβασης (π.χ Wifi, δίκτυο κινητής τηλεφωνίας, WiMAX) έχει καταστήσει τις φορητές συσκευές ως σημείο εισόδου στους πόρους τεχνολογιών πληροφορικής στις επιχειρήσεις και στο cloud.

2.2.5 Κέντρα Διαχείρισης Δεδομένων(Data Centers) και Servers farms

Οι υπηρεσίες του cloud απαιτούν μεγάλη υπολογιστική ισχύ και για αυτό το λόγο φιλοξενούνται σε data centers και server farms.Αυτά τα κατανεμημένα data centers και server farms εκτείνονται σε πολλές περιοχές και συνδέονται μεταξύ τους μέσω του Internet, παρέχοντας έτσι την υποστήριξη σε κατανεμημένες υπηρεσίες και υπολογιστικούς πόρους.

Πολλά σημερινά παραδείγματα δείχνουν εμφανώς την ευελιξία και την προσαρμοστικότητα της ισχύς του cloud computing.Για παράδειγμα η Google έχει

διασυνδέσει ένα μεγάλο αριθμό φτηνών servers για να παρέχει τεράστια ευελιξία και ισχύ. Επίσης η Amazon με το Elastic Compute Cloud (EC2) παρέχει εικονικά data center δημιουργώντας έναν τεράστιο αριθμό από εικονικά στιγμιότυπα υπηρεσιών. Η Salesforce.com παρέχει λογισμικό ως υπηρεσία(SaaS) στην μεγάλη βάση των πελατών της με το να τους ομαδοποιεί σε clusters,καθιστώντας εφικτή την προσαρμοστικότητα και την ευελιξία.

2.2.6 Συσκευές Αποθήκευσης

Μειώνοντας το κόστος αποθήκευσης και με την ευκολία που αναπτύσσονται τα μέσα αποθήκευσης το τοπίο στον χώρο αυτό έχει αλλάξει. Η απευθείας πρόσβαση στις συσκευές αποθήκευσης(direct access storage device “DASD”), έχει αντικατασταθεί με τις δικτυακές περιοχές αποθήκευσης(storage area networks (SANs)), με αποτέλεσμα να μειώνεται το κόστος και να αυξάνεται η ευελιξία με την οποία οι επιχειρήσεις αποθηκεύουν τα δεδομένα τους. Το λογισμικό του SAN διαχειρίζεται την ενοποίηση των συσκευών αποθήκευσης και μπορεί να κατανέμει ανεξάρτητα χώρο αποθήκευσης κατά απαίτηση ανάμεσα σε ένα σύνολο συσκευών.

2.2.7 Τεχνολογίες εικονικότητας(Virtualization technologies)

Το virtualization είναι η θεμελιώδης τεχνολογία που πλαισιώνει το cloud και μεταμορφώνει την εικόνα ενός σύγχρονου data center. Ο όρος virtualization αναφέρεται στην απόκρυψη των υπολογιστικών πόρων (CPU, αποθήκευση, δίκτυο, μνήμη, στοίβα εφαρμογών, και βάσεις δεδομένων) από τις εφαρμογές και του τελικούς χρήστες που χρησιμοποιούν την υπηρεσία, δίνοντας έτσι μια πιο αφαιρετική προσέγγιση. Η απόκρυψη της υποδομής δημιουργεί την αντίληψη μιας πιο «δημοκρατικής» διαχείρισης των πόρων είτε πρόκειται για υποδομές, είτε για εφαρμογές ή πληροφορίες. Παρέχεται έτσι η δυνατότητα να δημιουργείται μια δεξαμενή πόρων οι οποίοι είναι διαθέσιμοι και προσβάσιμοι από τον καθένα ή από όποιον είναι εξουσιοδοτημένος να τους χρησιμοποιεί, μέσα από τυποποιημένες διαδικασίες.

Το virtualization καθιστά ικανό ένα πολύ-μισθωτικό (multi-tenancy) μοντέλο στο cloud, παρέχοντας μια κλιμακωτή, με διαμοιραζόμενους πόρους πλατφόρμα για όλους τους χρήστες. Το σημαντικότερο είναι ότι παρέχει μια εικόνα στους χρήστες της πλατφόρμας ότι οι πόροι είναι αποκλειστικά αφιερωμένοι σε αυτούς. Από την οπτική τον επιχειρήσεων το virtualization προσφέρει μια συγκέντρωση των data

center βελτιώνοντας έτσι την επιχειρησιακή ικανότητα των τεχνολογιών πληροφορικής. Σήμερα, οι επιχειρήσεις αναπτύσσουν τεχνολογίες virtualization μέσα στα data centers με διάφορες μορφές συμπεριλαμβανομένων των: λειτουργικών συστημάτων (VMware,Xen), αποθηκευτικών μέσων (NAS,SAN), βάσεων δεδομένων, και εφαρμογών ή λογισμικού (Apache Tomcat, JBoss, Oracle App Server, WebSphere).

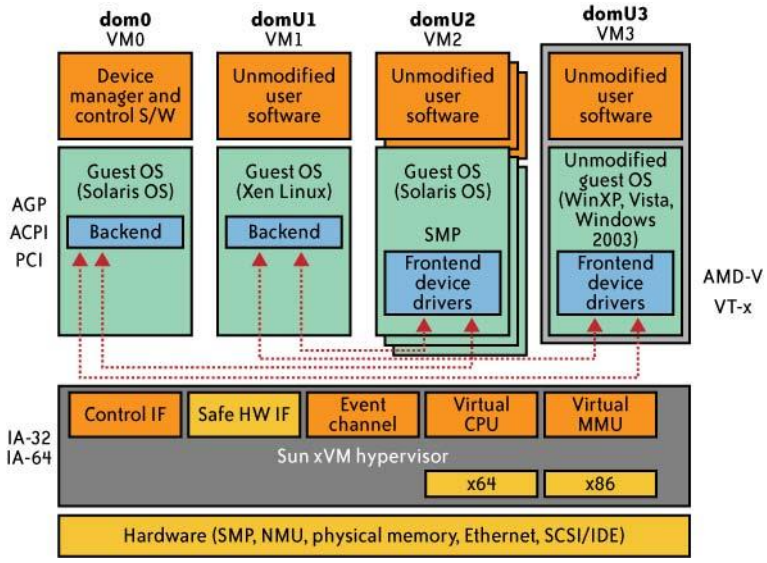
Από την πλευρά του δημόσιου (public) cloud, σύμφωνα με το SPI μοντέλο του cloud το virtualization εμφανίζεται ως διαμοιραζόμενος πόρος σε διάφορα επίπεδα της εικονικής υπηρεσίας (π.χ Λειτουργικό σύστημα, αποθήκευση, βάσεις δεδομένων, εφαρμογές).

Η εικόνα 2.5 παρουσιάζει το virtualization του λειτουργικού συστήματος και τα επίπεδα του περιβάλλοντος του virtualization όπως αυτά ορίζονται από την Sun Microsystems. Οι πάροχοι IaaS (υποδομή ως υπηρεσία) συμπεριλαμβανομένων των: Amazon(EC2), ServePath(GoGrid), και Sun Cloud, ανέπτυξαν αυτό τον τύπο του virtualization το οποίο επιτρέπει στους πελάτες να τρέχουν στιγμιότυπα από διάφορα λειτουργικά συστήματα μέσα στο δημόσιο cloud. Η πλατφόρμα εικονικότητας που παρουσιάζεται στην εικόνα 1.5 είναι το περιβάλλον επόπτης(hypervisor) xVM της Sun που εικονικοποιεί τους κοινόχρηστους πόρους υλικού(hardware) για τα φιλοξενούμενα ή εικονικά λειτουργικά συστήματα εξυπηρετητών(servers) (π.χ Linux, Solaris, και Microsoft Windows) που φιλοξενούνται στον επόπτη. Ο επόπτης είναι μια μικρή εφαρμογή που εκτελείται στην κορυφή του επιπέδου της μηχανής που διαχειρίζεται το υλικό (physical machine hardware layer). Υλοποιεί και διαχειρίζεται τις εικονικές CPU (vCPU), την εικονική μνήμη (vMemory), καταγράφει τα κανάλια και την μνήμη που μοιράζονται οι φιλοξενούμενες εικονικές μηχανές(VMs). Επίσης ελέγχει τα I/O και την πρόσβαση των συσκευών στην μνήμη.

Στο Xen, όπως επίσης στο xVM της Sun (το οποίο είναι βασισμένο στο έργο της κοινότητας του Xen) ,μια εικονική μηχανή (VM) ονομάζεται τομέας(domain) ενώ στο VMware αναφέρεται ως φιλοξενούμενο (guest) λειτουργικό. Στην εικόνα 1.5 οι εικονικές μηχανές(VMs) χαρακτηρίζονται ως dom0 και domU1,domU2,domU3. Το dom0 χρησιμοποιείται για να διαχειρίζεται τα υπόλοιπα domains των χρηστών (domU1 κ.τ.λ). Το VMware επίσης υλοποιεί έναν παρόμοιο μηχανισμό που τον

ονομάζει “service console”. Η διαχείριση μέσω του dom0 ή του service console αποτελείται από την δημιουργία, καταστροφή, μεταφορά, αποθήκευση ή επανάκτηση των domains των χρηστών. Ένα λειτουργικό σύστημα που εκτελείται σε ένα domain ενός χρήστη είναι ρυθμισμένο έτσι ώστε να εκτελεί προνομιούχες λειτουργίες μέσω κλήσεων στον επόπτη.

Εικόνα 2.5 Επόπτης του περιβάλλοντος Sun xVM



Σε αντίθεση με την εικονικοποίηση του λειτουργικού συστήματος και των μέσων αποθήκευσης, οι πάροχοι που παρέχουν υπηρεσίες Saas και PaaS έχουν υλοποιήσει εικονικοποίηση του λογισμικού και των βάσεων δεδομένων δια μέσω της οποίας οι πελάτες μοιράζονται την στοίβα εφαρμογών και την στοίβα βάσεων δεδομένων. Σε αυτό το μοντέλο όλοι οι πελάτες μοιράζονται κάθε επίπεδο της υποδομής.

2.2.8 Application programming interface (APIs)

Μια κατάλληλη διεπιφάνεια προγραμματισμού εφαρμογών(API) κάνει πιο δυνατό το μοντέλο υπηρεσιών του cloud computing (Εικόνα 1.6).Τα APIs ενδυναμώνουν τους χρήστες με το να τους παρέχουν χαρακτηριστικά .όπως να αυτό-προμηθεύονται και να ελέγχουν μέσω προγραμμάτων συσκευές και πόρους. Εξαρτάται από τον τύπο του μοντέλου υπηρεσιών του cloud (SPI), ένα API μπορεί να εκδηλώνεται με διαφορετικές μορφές από απλά URL manipulations μέχρι προγραμματιστικά μοντέλα SOA. Τα APIs βοηθάνε επίσης στο να εκμεταλλεύεται

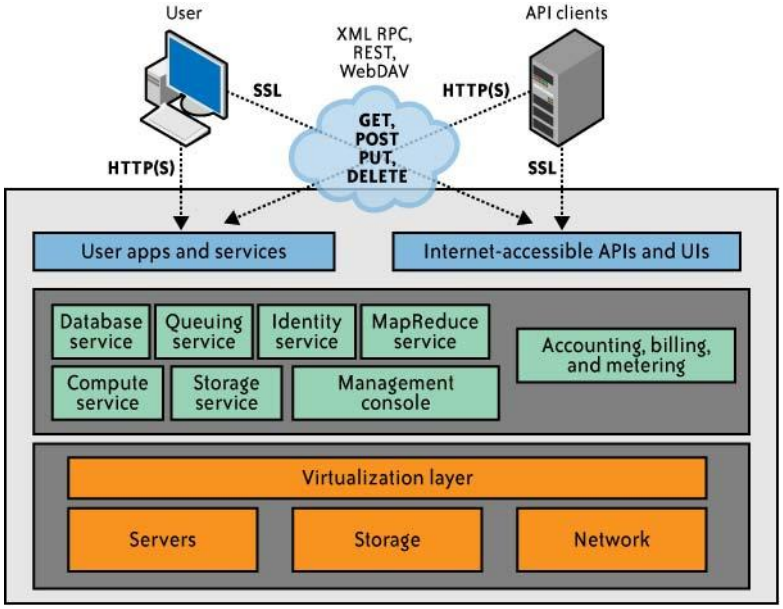
στο έπακρο το δυναμικό του cloud computing και κρύβουν την πολυπλοκότητα που περιέχεται στην υπάρχουσα διαδικασία διαχείρισης τεχνολογιών πληροφορικής και τακτικών στις υπηρεσίες του cloud.

Τα APIs που παρέχονται από τους παρόχους(CSPs) IaaS όπως το Amazon EC2, Sun Cloud, και το GoGrid επιτρέπουν στον χρήστες να δημιουργούν και να διαχειρίζονται πόρους συμπεριλαμβανομένων συστατικών όπως υπολογιστική ισχύ, αποθήκευση και δικτύωση. Σε αυτή την περίπτωση η χρήση του API γίνεται μέσα από το πρωτόκολλο HTTP. Οι αιτήσεις GET, POST, PUT, DELETE χρησιμοποιούνται αν και οι περισσότερες αποστολές μπορούν να ολοκληρωθούν με τις GET και POST. Σε μερικές περιπτώσεις οι αναπαραστάσεις των πόρων γίνονται με την JavaScript Object Notation (JSON). Για παράδειγμα οι προδιαγραφές της SUN για το API του Sun Cloud περιλαμβάνει:

- Κοινές συμπεριφορές που απευθύνονται σε όλα τα αιτήματα και σε όλες τις αποκρίσεις.
- Μοντέλα πόρων που περιγράφουν την δομή των δεδομένων του JSON που χρησιμοποιούνται στα αιτήματα και τις αποκρίσεις.
- Αιτήματα που μπορεί να αποστέλλονται στους πόρους του cloud και ανταποκρίσεις που αναμένονται.

Όλοι οι παραγωγοί οποιασδήποτε (*aaS) υπηρεσίας, θα πρέπει να είναι εξοικειωμένοι με συγκεκριμένα APIs για να αναπτύσσουν και να διαχειρίζονται τμήματα λογισμικού οποιασδήποτε (*aaS) πλατφόρμας.

Εικόνα 2.6 Ενδυνάμωση του cloud με τα APIs



Σήμερα μια από τις προκλήσεις που έχουν να αντιμετωπίσουνε οι χρήστες του cloud είναι ότι ο κάθε πάροχος (CSP) παρέχει το δικό του API. Σαν αποτέλεσμα οι εφαρμογές του cloud δεν έχουν φορητότητα από cloud σε cloud και είναι δύσκολο να επιτευχθεί συνεργασία (interoperability) ανάμεσα σε εφαρμογές που τρέχουν σε διαφορετικά clouds(συμπεριλαμβανομένων και των ιδιωτικών clouds). Εφόσον λοιπόν τα APIs είναι μοναδικά σε κάθε υπηρεσία του cloud, οι αρχιτέκτονες, οι άνθρωποι που αναπτύσσουν υπηρεσίες και το προσωπικό των data centers θα πρέπει να εξοικειωθούν με χαρακτηριστικά επικεντρωμένα σε συγκεκριμένες πλατφόρμες.

Παρόλο που δεν υπάρχει τυποποίηση στα APIs οι προσπάθειες για τυποποίηση έρχονται η μία μετά την άλλη, τόσο από τους πωλητές όσο και από τις κοινότητες των χρηστών. Μια τέτοια προσπάθεια είναι το “Universal Cloud Interface” (UCI), μια προσπάθεια να δημιουργηθεί μια ανοιχτή και τυποποιημένη διεπαφή (interface) για την ενοποίηση των διάφορων APIs. Το UCI φόρουμ υποστηρίζει ότι στόχος είναι να επιτευχθεί ένα μοναδικό προγραμματικό σημείο επαφής το οποίο να περιγράφει ολόκληρη την στοίβα υποδομής, όπως επίσης να φέρει στην επιφάνεια τεχνολογίες επικεντρωμένες στο cloud, όλα μέσα από μια ενιαία διεπαφή. Μέχρι στιγμής δεν υπάρχει μια οργανωμένη προσπάθεια από τους παρόχους (CSPs) να αναπτύξουν μια πανταχού παρόν διεπαφή, επιπλέον το εμπορικό κίνητρο

των παρόχων να κερδίσουν τα προϊόντα τους περισσοτέρους πελάτες κάνει την εύκολη συνεργασία μεταξύ των clouds, δύσκολη να επιτευχθεί.

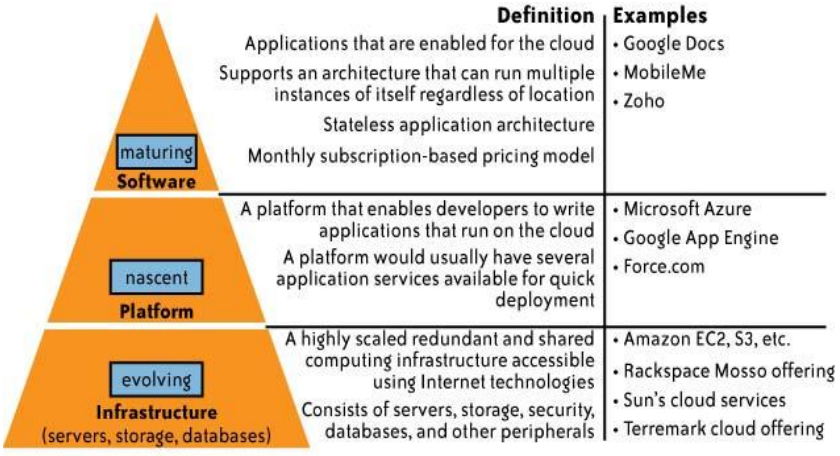
2.3 Το παραδοσιακό μοντέλο λογισμικού

Το παραδοσιακό μοντέλο λογισμικού βασίζεται στο μεγάλο αρχικό κόστος για την απόκτηση της άδειας χρήσης και σε ένα επιπλέον ετήσιο κόστος υποστήριξης του προϊόντος. Αυξάνοντας τον αριθμό των χρηστών αυξάνει και το βασικό κόστος του πακέτου λογισμικού λόγω της ανάγκης ανάπτυξης επιπλέον εξοπλισμού εξυπηρετητών και υποστήριξης. Το κόστος των αδειών χρήσης συχνά βασίζεται σε μετρικές που δεν είναι άμεσα συνδεδεμένες με την χρήση (τύπος εξυπηρετητή, αριθμός CPUs, κ.τ.λ., ή σε μερικά φυσικά χαρακτηριστικά) και οι μετρικές αυτές δεν είναι εικονικές. Ένα τυπικό εταιρικό πακέτο λογισμικού απαιτεί την ανάπτυξη υλικού(hardware), εξυπηρετητών, και παροχή δικτύωσης και λήψης αντιγράφων ασφαλείας(backup), ώστε να εξυπηρετούνται οι χρήστες τόσο μέσα όσο και έξω από τις εγκαταστάσεις της εταιρείας Η αρχιτεκτονική ασφάλειας συμπεριλαμβάνεται στα κόστη, προκειμένου να προστατευθούν, ζωτικής σημασίας πόρους από μη εξουσιοδοτημένη πρόσβαση. Οι εφαρμογές λογισμικού του παραδοσιακού μοντέλου τείνουν να είναι ιδιαίτερα παραμετροποιήσιμες από τον χρήστη, κάτι το οποίο επιφέρει επιπλέον κόστος σε χρήματα και ανθρώπινο δυναμικό.

2.4 Το μοντέλο διανομής του Cloud

Όπως έχει αναφερθεί και νωρίτερα το μοντέλο διανομής υπηρεσιών του cloud αναφέρεται ως SPI και κατηγοριοποιείται σε 3 γενικές κατηγορίες (Εικόνα 2.7).

Εικόνα 2.7 Το μοντέλο διανομής υπηρεσιών του Cloud



While cloud-based software services are maturing, cloud platform and infrastructure offerings are still in their early stages

2.4.1 Το μοντέλο λογισμικού ως υπηρεσία (Software-as-a-Service)

Οι παραδοσιακές μέθοδοι της αγοράς λογισμικού προϋποθέτουν από τον χρήστη να φορτώσει το λογισμικό στον δικό του εξοπλισμό, αφού πρώτα έχει πληρώσει για την άδεια χρήσης. Ο πελάτης επίσης μπορεί να προβεί στην αγορά μιας σύμβασης συντήρησης προκειμένου να λαμβάνει ενημερώσεις ασφαλείας(patches), ή άλλες υπηρεσίες υποστήριξης. Ο πελάτης είναι αυτός που ενδιαφέρεται για την συμβατότητα των λειτουργικών συστημάτων, την εγκατάσταση των patches, και την συμμόρφωση του με τους όρους της άδειας χρήσης.

Στο μοντέλο του SaaS, ο πελάτης δεν αγοράζει το λογισμικό, αντιθέτως το ενοικιάζει για χρήση με συνδρομή ή με το μοντέλο πληρωμής ανάλογα με την χρήση(pay per use). Σε μερικές περιπτώσεις η υπηρεσία διατίθεται δωρεάν για περιορισμένη χρήση. Συνήθως η αγορά της υπηρεσίας είναι ολοκληρωμένη από την πλευρά του υλικού, του λογισμικού και της υποστήριξης. Ο χρήστης έχει πρόσβαση στην υπηρεσία από οποιαδήποτε εξουσιοδοτημένη συσκευή. Σε μερικές περιπτώσεις όμως χρειάζεται προκαταρτική εργασία προκειμένου να δημιουργηθούν εξειδικευμένα δεδομένα της εταιρείας και να χρησιμοποιηθούν πλήρως, και ενδεχομένως να ολοκληρώνονται με άλλες εφαρμογές που δεν είναι κομμάτι της πλατφόρμας του Saas.

Τα κύρια χαρακτηριστικά του μοντέλου Saas περιλαμβάνουν:

- Το SaaS δίνει την δυνατότητα στον οργανισμό να αναθέτει σε τρίτους (κατασκευαστής και πάροχος λογισμικού) την φιλοξενία και την διαχείριση των εφαρμογών, μειώνοντας έτσι το κόστος των αδειών χρήσης λογισμικού, εξυπηρετητών, και άλλων υποδομών και προσωπικού που χρειάζεται για να φιλοξενεί τις εφαρμογές εσωτερικά.
- Το SaaS δίνει την δυνατότητα στον κατασκευαστή να ελέγχει και να περιορίζει την χρήση, εμποδίζοντας την αντιγραφή και την διανομή , με αποτέλεσμα να διευκολύνεται ο έλεγχος όλων των παραγόμενων εκδόσεων λογισμικού. Ο κεντρικός έλεγχος του SaaS επιτρέπει στον κατασκευαστή ή στον προμηθευτή να αυξήσει τα έσοδα του από πολλές επιχειρήσεις ή

χρήστες, χωρίς να χρειαστεί να εγκαταστήσει το λογισμικό σε κάθε μία συσκευή των πελατών του.

- Οι εφαρμογές που διανέμονται με το μοντέλο διανομής SaaS συχνά χρησιμοποιούν την προσέγγιση του “ένα προς πολλούς” (one to many), με το Web να αποτελεί την υποδομή διανομής. Ο τελικός χρήστης μπορεί να έχει πρόσβαση στην εφαρμογή μέσω ενός φυλλομετρητή, επίσης μερικοί κατασκευαστές παρέχουν την δική τους διεπαφή (interface) η οποία είναι σχεδιασμένη να υποστηρίζει χαρακτηριστικά που είναι μοναδικά στις εφαρμογές τους.
- Μια τυπική εφαρμογή SaaS δεν χρειάζεται επιπλέον εξοπλισμό και μπορεί να τρέξει πάνω στην υπάρχουσα υποδομή πρόσβασης στο Internet. Ορισμένες φορές είναι αναγκαία κάποια αλλαγή στους κανόνες του φίλτρου προστασίας (firewall) και ορισμένες ρυθμίσεις προκειμένου η εφαρμογή να λειτουργεί απροβλημάτιστα.
- Η διαχείριση μιας εφαρμογής SaaS υποστηρίζεται από τον κατασκευαστή, από την πλευρά του ο χρήστης μπορεί να παραμετροποιήσει μερικώς την εφαρμόγη χρησιμοποιώντας ένα API, αλλά οι εφαρμογές SaaS δεν είναι πλήρως παραμετροποιήσιμες.

Ένας συνηθισμένος τρόπος να παρέχεται SaaS είναι μέσω της υποδομής δημοσίου δικτύου (public network), με αυτόν τον τρόπο η εφαρμογή φτάνει μέσω του Internet στο firewall του οργανισμού.

Η πιο σημαντική διαφορά στην αρχιτεκτονική του μοντέλου SaaSκαι του παραδοσιακού μοντέλου λογισμικού είναι ο αριθμός των εκμισθωτών (tenants) που υποστηρίζει μια εφαρμογή. Το παραδοσιακό μοντέλο λογισμικού είναι ένα απομονωμένο, ενός εκμισθωτή μοντέλο, πράγμα που σημαίνει ότι ο πελάτης αγοράζει μια εφαρμογή λογισμικού και την εγκαθιστά σε έναν εξυπηρετητή. Ο εξυπηρετητής τρέχει μόνο αυτή την εφαρμογή και μόνο για τους τελικούς χρήστες αυτού του πελάτη. Το μοντέλο SaaS όμως είναι ένα πολύ-εκμισθωτικό (multitenant), μοντέλο, που σημαίνει ότι η φυσική υποδομή πίσω από το SaaS διαμοιράζεται μεταξύ πολλών και διαφορετικών πελατών, αλλά σε λογικό επίπεδο η υποδομή παραμένει μοναδική για κάθε πελάτη.

Η αρχιτεκτονική πολλαπλών εκμισθωτών (multitenant) , βελτιστοποιεί τον διαμοιρασμό των πόρων ανάμεσα στους εκμισθωτές, αλλά παράλληλα είναι σε θέση να διακρίνει με ασφάλεια τα δεδομένα διαφορετικών εκμισθωτών. Για παράδειγμα όταν ένας χρήστης μιας εταιρείας προσπελαύνει πληροφορίες για έναν πελάτη χρησιμοποιώντας λογισμικό “διαχείρισης πελατειακών σχέσεων” (Customer Relathionship Management –CRM) το στιγμιότυπο (instance) της εφαρμογής που συνδέεται ο χρήστης μπορεί την ίδια στιγμή να εξυπηρετεί χρήστες από δεκάδες ή ακόμα και εκατοντάδες άλλες εταιρείες, όλες εντελώς άγνωστες στους υπόλοιπους χρήστες.

Οι λύσεις που προσφέρει το SaaS είναι πολύ διαφορετικές από τις λύσεις που προσφέρει ένας ASP. Υπάρχουν δύο βασικές εξηγήσεις για αυτό:

- Οι εφαρμογές των ASPs είναι οι παραδοσιακές, ενός εκμισθωτή εφαρμογές, αλλά φιλοξενούνται (hosted) από έναν τρίτο. Είναι εφαρμογές πελάτη/εξυπηρετητή (client/server) με μια html διεπαφή που επιτρέπει την απομακρυσμένη πρόσβαση στην εφαρμογή.
- Οι εφαρμογές των ASPs δεν είναι γραμμένες ως αμιγώς δικτυακές εφαρμογές. Ως αποτέλεσμα η απόδοση τους μπορεί να μην είναι επαρκής, επιπλέον οι αναβαθμίσεις των εφαρμογών αυτών δεν είναι καλύτερες από τις αυτό-διαχειριζόμενες στεγασμένες εφαρμογές.

Συγκριτικά οι εφαρμογές SaaS είναι πολύ-εκμισθωτικές εφαρμογές που φιλοξενούνται από ένας κατασκευαστή με εξειδίκευση σε αυτές τις εφαρμογές και έχουν σχεδιαστεί ως αμιγώς δικτυακές εφαρμογές που αναβαθμίζονται σε συχνή βάση.

2.4.2 Το μοντέλο Πλατφόρμας Ανάπτυξης ως Υπηρεσίας (Platform-as-a-Service)

Στο μοντέλο πλατφόρμας ως υπηρεσία, ο κατασκευαστής προσφέρει ένα περιβάλλον ανάπτυξης στους προγραμματιστές εφαρμογών, οι οποίοι αναπτύσσουν εφαρμογές και τις προσφέρουν μέσα από την πλατφόρμα του παρόχου. Ο πάροχος συνήθως αναπτύσσει εργαλεία (toolkits), πρότυπα ανάπτυξης και κανάλια διανομής και πληρωμής. Ο πάροχος διαθέτει την πλατφόρμα ανάπτυξης καθώς και τις υπηρεσίες πωλήσεων και διανομής, αφού πρώτα ο χρήστης καταβάλει το ανάλογο αντίτιμο. Οι εφαρμογές λογισμικού γνωρίζουν έτσι μεγάλη άνθιση και σε συνδυασμό με το χαμηλό κόστος εισαγωγής τους στην αγορά αυξάνονται και οι αγοραστικές επιλογές των πελατών.

Το μοντέλο PaaS είναι μια παραλλαγή του μοντέλου SaaS μέσω του οποίου το περιβάλλον ανάπτυξης παρέχεται ως υπηρεσία. Οι προγραμματιστές εφαρμογών χρησιμοποιούν δομικά κομμάτια (για παράδειγμα προκατασκευασμένα κομμάτια κώδικα) του περιβάλλοντος ανάπτυξης του κατασκευαστή, για να δημιουργήσουν τις δικές τους εφαρμογές.

Η λύσεις που προσφέρει το PaaS είναι πλατφόρμες ανάπτυξης για οποίες τα εργαλεία ανάπτυξης φιλοξενούνται στο cloud και είναι προσβάσιμα μέσα από έναν φυλλομετρητή. Με το PaaS οι προγραμματιστές μπορούν να δημιουργούν web εφαρμογές χωρίς να εγκαταστήσουν κανένα εργαλείο στον υπολογιστή τους, και μπορούν να τις αναπτύξουν χωρίς να χρειάζονται ειδικές ικανότητες διαχείρισης.

Τα συστήματα PaaS είναι χρήσιμα επειδή βοηθάνε προγραμματιστές (developers) που δουλεύουν μόνοι τους ή νέες επιχειρήσεις στο ξεκίνημα τους, να αναπτύσσουν web εφαρμογές χωρίς το κόστος και την πολυπλοκότητα της αγοράς και εγκατάστασης εξυπηρετητών. Τα προνόμια του PaaS εμπεριέχονται στο ότι όλο και περισσότεροι άνθρωποι μπορούν πλέον να αναπτύσσουν και να συντηρήσουν web εφαρμογές. Εν ολίγοις, το PaaS προσέφερε τον εκδημοκρατισμό στην ανάπτυξη web εφαρμογών, με τον ίδιο τρόπο που η Microsoft Access εκδημοκράτισε την ανάπτυξη των client/server εφαρμογών.

Σήμερα η ανάπτυξη web εφαρμογών απαιτεί εξειδικευμένους προγραμματιστές με τρείς κυρίως ικανότητες:

- Backend server development (π.χ Java/J2EE)
- Frontend client development (π.χ JavaScript/Dojo)
- Διαχείριση Ιστοσελίδων

Το μοντέλο PaaS προσφέρει την δυνατότητα σε προγραμματιστές με γενικές γνώσεις να αναπτύσσουν Web εφαρμογές χωρίς να χρειάζονται εξειδικευμένες γνώσεις. Πράγμα που επιτρέπει σε μια ολόκληρη γενιά προγραμματιστών εξοικειωμένων με την MS Access, το Lotus Notes και το PowerBuilder να αναπτύσσουν Web εφαρμογές χωρίς να χρειάζεται να ακολουθήσουν την καμπύλη μάθησης.

Η εναλλακτική επιλογή του PaaS είναι να αναπτύσσονται web εφαρμογές χρησιμοποιώντας εργαλεία ανάπτυξης που εγκαθίστανται στον υπολογιστή όπως

το Eclipse ή η MS Access, και μετά χειροκίνητα να φιλοξενούνται αυτές οι εφαρμογές σε έναν πάροχο Cloud όπως το Amazon Web Services.

Μια PaaS προσέγγιση θα πρέπει το λιγότερο να περιέχει τα εξής στοιχεία:

- Μια PaaS σουίτα θα πρέπει να λειτουργεί μέσω ενός φυλλομετρητή.
- Μια από άκρη σε άκρη (end-to-end) PaaS προσέγγιση θα πρέπει να παρέχει ένα ολοκληρωμένο περιβάλλον ανάπτυξης (integrated development environment IDE) που να τρέχει στην πλατφόρμα διανομής, ώστε η αποσφαλμάτωση και τα δοκιμαστικά σενάρια να γίνονται στο ίδιο περιβάλλον με αυτό της ανάπτυξης της εφαρμογής.
- Μια PaaS λύση θα πρέπει να παρέχει ενοποίηση με εξωτερικές υπηρεσίες Web και βάσεις δεδομένων.
- Μια PaaS λύση θα πρέπει να παρέχει αναλυτική παρακολούθηση της εφαρμογής και της δραστηριότητας των χρηστών, ώστε να βοηθά τους προγραμματιστές να καταλαβαίνουν καλύτερα τις εφαρμογές τους και να προβαίνουν σε βελτιώσεις.
- Η ευελιξία, η αξιοπιστία, και ασφάλεια θα πρέπει να είναι ενσωματωμένες σε μια PaaS λύση χωρίς να χρειάζεται επιπλέον ανάπτυξη, διαμόρφωση ή άλλο κόστος. Επίσης η ικανότητα μιας εφαρμογής να εξυπηρετεί πολλούς χρήστες (multitenancy) θα πρέπει να παρέχεται χωρίς επιπλέον δουλειά.
- Μια PaaS λύση θα πρέπει να παρέχει τόσο μια τυπική, όσο και μια κατά απαίτηση (on demand) συνεργασία σε όλη την διάρκεια ανάπτυξης λογισμικού (ανάπτυξη, δοκιμή, τεκμηρίωση, λειτουργία), ενώ παράλληλα να διασφαλίζει την ασφάλεια του πηγαίου κώδικα και της σχετιζόμενης πνευματικής ιδιοκτησίας.
- Μια PaaS λύση θα πρέπει να υποστηρίζει μια μέθοδο πληρωμής ανάλογα με την χρήση.

Ο πίνακας 2-1 παρουσιάζει τα διαφορετικά συστατικά του PaaS.

Πίνακας 2-1 Συστατικά του PaaS

Δυνατότητες πελατών	Εργαλεία ανάπτυξης βασισμένα στον φυλλομετρητή : Google Web Toolkit, Google Gears, Mashup Editor, Google Gadgets κτλ.

Υπηρεσίες του cloud computing	Περιβάλλον εκτέλεσης βασισμένο στο cloud : EC2, Google App Engine κτλ.
Υπηρεσίες υποστήριξης γενικής χρήσης	Υπηρεσίες web εργαλείων : Simple Storage Service, Simple DB, MTurk, GAE Datastore, GDate, Google Accounts, Social Graph API κτλ.

Οι πλατφόρμες του μοντέλου PaaS έχουν και λειτουργικές διαφορές από τις παραδοσιακές πλατφόρμες ανάπτυξης. Αυτές είναι:

Πολύ-μισθωτικά εργαλεία ανάπτυξης: Τα παραδοσιακά εργαλεία ανάπτυξης προορίζονται για έναν μόνο χρήστη, ενώ οι σουίτες που σχεδιάζονται για το Cloud πρέπει να υποστηρίζουν πολλαπλούς χρήστες, ο καθένας τους με πολλαπλά ενεργά project.

Πολύ-μισθωτική αρχιτεκτονική ανάπτυξης: Η ευελιξία δεν αποτελεί ανησυχία στην αρχική προσπάθεια ανάπτυξης, και αφήνεται να διαχειριστεί από τους διαχειριστές του συστήματος όταν το έργο αναπτύσσεται. Στην PaaS πλατφόρμα η ευελιξία της εφαρμογής και η βαθμίδα των δεδομένων (data tier) πρέπει να είναι ενσωματωμένη (π.χ η ισορροπία φόρτου εργασίας, και η επανάκαμψη (failover) πρέπει να είναι βασικά στοιχεία της πλατφόρμας ανάπτυξης).

Ολοκληρωμένη διαχείριση: Οι παραδοσιακές λύσεις ανάπτυξης δεν συνδέονται με παρακολούθηση κατά τον χρόνο εκτέλεσης, αλλά στην PaaS πλατφόρμα η δυνατότητα παρακολούθησης πρέπει να είναι ενσωματωμένη.

Ολοκληρωμένη πληρωμή: Η παροχή PaaS απαιτεί μηχανισμούς για χρέωση με βάση την χρήση , οι οποίοι είναι μοναδικοί στον κόσμο του SaaS.

Ο πίνακας 2-2 παρουσιάζει την ελαστικότητα που προσφέρεται από τις παραδοσιακές πλατφόρμες και τις πλατφόρμες ως υπηρεσία

Πίνακας 2-2 Σύγκριση παραδοσιακών πλατφόρμων και πλατφόρμων ως υπηρεσία.

Υποστηριζόμενη Περιοχή	**Παραδοσιακές Πλατφόρμες**	**Πλατφόρμα ως υπηρεσία**
Τελικά σημεία : προσωπικοί υπολογιστές, φυλλομετρητές, φορητές	Τα περισσότερα τελικά σημεία και πελάτες υποστηρίζονται	Κυρίως βασισμένο στον φυλλομετρητή

συσκευές		
Επιχειρηματική λογική	Πολλαπλοί πωλητές υποστηρίζονται	Περιορισμός από το μοντέλο του PaaS
Πλαίσιο εργασίας ανάπτυξης εφαρμογών	Java platform, Enterprise Edition (java EE), .Net κτλ	Περιορισμός από το μοντέλο του PaaS
Εξυπηρετητές εφαρμογών	Πολλαπλοί πωλητές υποστηρίζονται	Περιορισμός από το μοντέλο του PaaS
Βάσεις Δεδομένων	Πολλαπλοί πωλητές υποστηρίζονται	Περιορισμός από το μοντέλο του PaaS
Εξυπηρετητές και Εικονικές Μηχανές	Πολλαπλοί πωλητές υποστηρίζονται	Περιορισμός από το μοντέλο του PaaS
Αποθήκευση	Πολλαπλοί πωλητές υποστηρίζονται	Περιορισμός από το μοντέλο του PaaS

2.4.3Το μοντέλο υποδομής ως υπηρεσία (Infrastructure-As-a-Service, IaaS)

Στο παραδοσιακό μοντέλο φιλοξενίας εφαρμογών, ο πωλητής παρέχει στον πελάτη όλη την υποδομή για να τρέχει την εφαρμογή του. Συχνά αυτή η υποδομή αγοράζεται ή ενοικιάζεται αποκλειστικά για μια συγκεκριμένη εφαρμογή. Το μοντέλο IaaS παρέχει της την υποδομή για να τρέχουν οι εφαρμογές, αλλά με την προσέγγιση του cloud computing παρέχει ένα μοντέλο πληρωμής ανάλογα με την χρήση και την ευελιξία να αλλάζει η υπηρεσία κατά απαίτηση. Από την πλευρά του παρόχου IaaS, μπορεί να στηθεί μια υποδομή η οποία να είναι σε θέση να ανταπεξέλθει της υψηλότερες απαιτήσεις των πελατών του, και να αυξάνει αυτή την υποδομή όσο αυξάνονται οι απαιτήσεις. Αντιστοίχως με το παραδοσιακό μοντέλο φιλοξενίας εφαρμογών, οι πωλητές IaaS μπορούν να καλύψουν μόνο την φιλοξενία των εφαρμογών ή να επεκταθούν και σε άλλες υπηρεσίες (όπως υποστήριξη εφαρμογών, ανάπτυξη εφαρμογών, αναβάθμιση). Επίσης μπορούν να υποστηρίξουν εκτενώς τις περισσότερες τεχνολογίες πληροφορικής που ανατίθενται ως δουλειές σε τρίτους (outsourcing).

Το μοντέλο IaaS είναι παρόμοιο με το utility computing, στο οποίο η βασική ιδέα είναι να παρέχει υπολογιστικές (computing) υπηρεσίες με τον ίδιο τρόπο που παρέχει εργαλεία (utilities). Αυτό σημαίνει ότι πληρώνεις για την ποσότητα της υπολογιστικής ισχύς, χώρου στον δίσκο, κ.τ.λ. που πραγματικά καταναλώνεις. Η υπηρεσία IaaS σχετίζεται με το cloud computing και απευθύνεται σε on-line υπηρεσίες που αποσπούν τον χρήστη από λεπτομέρειες της υποδομής, τους φυσικούς υπολογιστικούς πόρους, την τοποθεσία, τον διαμερισμό των δεδομένων,

την ασφάλεια, τα αντίγραφα ασφαλείας κ.α. Στο cloud computing ο πάροχος έχει τον πλήρη έλεγχο της υποδομής. Οι χρήστες του Utility computing αντίθετα ζητούν μια υπηρεσία που να τους επιτρέπει να αναπτύσσουν, και να διαχειρίζονται on-line υπηρεσίες χρησιμοποιώντας τους πόρους του παρόχου και πληρώνοντας μόνο για αυτούς τους πόρους που καταναλώνουν. Ωστόσο οι πελάτες θέλουν να έχουν τον έλεγχο της γεωγραφικής περιοχής της υποδομής και του τι τρέχει σε κάθε εξυπηρετητή.

Ένα τυπικό IaaS σύστημα περιλαμβάνει τα εξής χαρακτηριστικά:

Κλιμάκωση

Η δυνατότητα να αυξομειώνονται οι απαιτήσεις της υποδομής όπως υπολογιστικοί πόροι, μνήμη και αποθηκευτικός χώρος (σε πραγματικό χρόνο), βασισμένες στις απαιτήσεις που προκύπτουν από την χρήση.

Πληρωμή ανάλογα με την χρήση

Η δυνατότητα να αποκτάς την ακριβή ποσότητα της απαιτούμενης υποδομής κάθε συγκεκριμένη στιγμή.

Επιλογή της βέλτιστης τεχνολογικής λύσης

Πρόσβαση της καλύτερες τεχνολογικές λύσεις με το μικρότερο κόστος.

2.5 Μοντέλα εφαρμογής Cloud

Ο όρος Cloud είναι μια μεταφορά που χρησιμοποιείται για να περιγράψει το Internet, είναι μια απλοποιημένη αναπαράσταση της πολυπλοκότητας των διασυνδεδεμένων συσκευών και των συνδέσεων που αναπτύσσονται στο Internet. Τα ιδιωτικά κα δημόσια clouds είναι υποσύνολα του Internet και ορίζονται με βάση την σχέση τους με τον οργανισμό. Τα ιδιωτικά ή δημόσια clouds συχνά αναφέρονται ως εσωτερικά ή εξωτερικά clouds, η διαφοροποίηση αυτή βασίζεται στην σχέση του cloud με τον οργανισμό. Η έννοια των ιδιωτικών και δημόσιων clouds είναι σημαντική γιατί υποστηρίζουν το cloud computing το οποίο παρέχει τον αυτό-καθορισμό των πόρων, την αναλογικότητα των πόρων και την εικονικότητα μέσω των συνδέσεων του Internet που παρέχονται από τους πωλητές ή επιχειρήσεις τεχνολογιών πληροφορικής στους πελάτες κατόπιν

χρέωσης. Οι τελικοί χρήστες που χρησιμοποιούν τις υπηρεσίες που προσφέρονται μέσω του cloud computing μπορεί να μην έχουν γνώση, ειδικότητα ή έλεγχο στις τεχνολογικές υποδομές που τους υποστηρίζουν.

Η πλειοψηφία της υποδομής του cloud computing συνίσταται από αξιόπιστες υπηρεσίες που παραδίδονται μέσω των data center, και οι οποίες ενσωματώνονται σε servers με διαφορετικά επίπεδα τεχνολογιών εικονικότητας. Οι υπηρεσίες είναι προσβάσιμες από οπουδήποτε υπάρχει πρόσβαση σε υποδομές διαδικτύου. Οι εμπορικές προσφορές θα πρέπει να ανταπεξέρχονται στις απαιτήσεις των πελατών για ποιότητα, και συνήθως συνοδεύονται από συμφωνητικά για το επίπεδο των υπηρεσιών (service-level-agreement SLAs). Τα ανοιχτά πρότυπα είναι σημαντικά για την ανάπτυξη του cloud και το λογισμικό ανοιχτού κώδικα έχει αποτελέσει τα θεμέλια σε πολλές cloud υλοποιήσεις (για παράδειγμα η χρήση του Xen στο Amazon Web Services-AWS).

2.5.1 Δημόσια (Public) Clouds

Τα δημόσια (ή εξωτερικά clouds) περιγράφουν το cloud computing υπό μία γενική τάση, όπου οι πόροι παρέχονται δυναμικά, σε μια αυτό-εξυπηρετούμενη βάση μέσω του internet, μέσω web εφαρμογών ή web υπηρεσιών, από έναν εξωτερικό τρίτο πάροχο που μοιράζει της πόρους και χρεώνει σύμφωνα με την χρήση.

Ένα δημόσιο cloud φιλοξενείται, λειτουργεί και διαχειρίζεται από έναν τρίτο πωλητή, από ένα ή περισσότερα data center. Η υπηρεσία προσφέρεται σε πολλαπλούς πελάτες πάνω από μια κοινή υποδομή. Βλέπε εικόνα 1.8.

Σε ένα δημόσιο cloud η διαχείριση της ασφάλειας και οι καθημερινές λειτουργίες πραγματοποιούνται από έναν τρίτο πωλητή, ο οποίος είναι υπεύθυνος για της υπηρεσίες που προσφέρονται. Για αυτό το λόγο οι πελάτες του δημόσιου cloud έχουν ελάχιστο έλεγχο και επίβλεψη τόσο των φυσικών όσο και των λογικών ζητημάτων ασφάλειας.

Εικόνα 2.8 Δημόσιο Cloud

2.5.2 Ιδιωτικά (Private) Clouds

Τα ιδιωτικά και εσωτερικά clouds είναι όροι που χρησιμοποιούνται για να περιγράψουν προϊόντα που εξομοιώνουν το cloud computing στα ιδιωτικά δίκτυα. Αυτά τα προϊόντα ισχυρίζονται ότι παρέχουν τα προνόμια του cloud computing χωρίς της παγίδες που αφορούν στην ασφάλεια των δεδομένων και την αξιοπιστία. Οι οργανισμοί πρέπει να αγοράζουν, να στήνουν και να διαχειρίζονται τα προϊόντα αυτά, με αποτέλεσμα να μην μειώνονται τα κόστη και οι απαιτήσεις σε ανθρώπινο δυναμικό. Ο οργανισμός είναι υπεύθυνος για την λειτουργία του ιδιωτικού του cloud.

Το ιδιωτικό cloud διαφέρει από το δημόσιο cloud στο ότι η υποδομή δικτύου, υπολογιστών και αποθήκευσης που υλοποιεί το ιδιωτικό cloud παρέχεται μόνο σε έναν οργανισμό και δεν μοιράζεται σε άλλους οργανισμούς. Υπάρχουν διάφοροι τύποι ιδιωτικών cloud όπως:

Αφιερωμένο (dedicated)

Τα ιδιωτικά cloud φιλοξενούνται σε data center που ανήκουν στον χρήστη και διαχειρίζονται από τα εσωτερικά τμήματα τεχνολογίας πληροφορικής.

Κοινότητας (Community)

Τα ιδιωτικά cloud βρίσκονται στις εγκαταστάσεις ενός τρίτου, ανήκουν, διαχειρίζονται και λειτουργούν από έναν πωλητή ο οποίος

περιορίζεται από τον πελάτη με συμφωνητικά για το επίπεδο των υπηρεσιών (service-level-agreement SLAs), και συμμορφώνεται στις απαιτήσεις για ασφάλεια με δεσμευτικές ρήτρες.

Διαχειριζόμενα (managed)

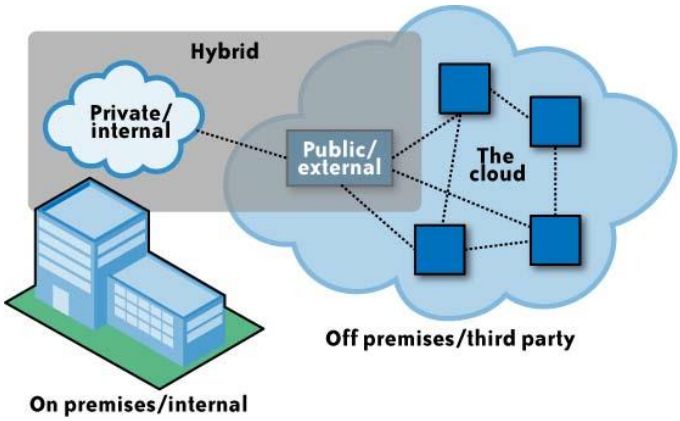
Η υποδομή του ιδιωτικού cloud ανήκει στον πελάτη και διαχειρίζεται από έναν πωλητή.

Γενικά σε ένα λειτουργικό μοντέλο ιδιωτικού cloud, η διαχείριση της ασφάλειας και οι καθημερινές λειτουργίες των σταθμών εκχωρούνται στο εξωτερικό τμήμα τεχνολογίας πληροφορικής ή σε έναν τρίτο με δεσμευτικά συμφωνητικά για το επίπεδο των υπηρεσιών (SLAs). Ως πλεονέκτημα αυτού του μοντέλου, ο πελάτης ενός ιδιωτικού cloud πρέπει να έχει έναν υψηλού βαθμού έλεγχο και επίβλεψη τόσο στα φυσικά όσο και στα λογικά ζητήματα ασφάλειας της υποδομής και των εικονικών συστημάτων (Hypervisor και hosted Oss). Με αυτόν τον υψηλό βαθμό ελέγχου και διαφάνειας, είναι πιο εύκολο για τον πελάτη να συμμορφώνεται με τα καθιερωμένα πρότυπα ασφάλειας και της πολιτικές που εφαρμόζονται.

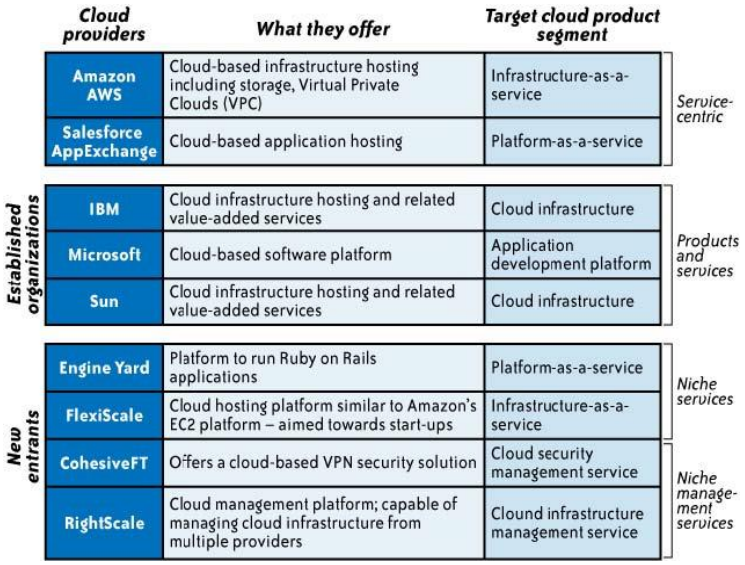
2.5.3 Υβριδικά (Hybrid) Clouds

Ένα υβριδικό cloud αποτελείται από πολλαπλούς εσωτερικούς και /ή εξωτερικούς παρόχους. Με ένα υβριδικό cloud οι οργανισμοί πρέπει να τρέχουν non-core εφαρμογές σε ένα δημόσιο cloud, ενώ να διατηρούν τις core εφαρμογές και τα ευαίσθητα δεδομένα εντός του οργανισμού σε ένα ιδιόκτητο δίκτυο.

Εικόνα 2.9 Υβριδικό Cloud



Εικόνα 2.10 Παραδείγματα παρόχων και των αντίστοιχων προσφορών τους



Οι υπηρεσίες που παρέχονται από την ενσωμάτωση των συστατικών (components) του cloud εξελίσσονται και τα εμπόδια υπέρσκελίζονται. Ένα ζήτημα ζωτικής σημασίας είναι να υπάρχει εμπιστοσύνη ότι οι πληροφορίες μιας εταιρίας ή ενός ιδιώτη είναι και ασφαλείς και απόρρητες. Η εγκαθίδρυση της εμπιστοσύνης αποτελεί ορόσημο για την πλήρη υιοθέτηση των δυνατοτήτων του Cloud.

2.6 Κύριοι λόγοι για την υιοθέτηση του Cloud

Για να συγκριθεί η client/server αρχιτεκτονική με το cloud computing ο πίνακας 2-3 παρουσιάζει μερικά από τα πλεονεκτήματα του cloud computing. Ωστόσο με το cloud computing είναι σημαντικό να γίνει κατανοητό το πώς ενσωματώνονται οι τεχνολογίες του cloud στην υπάρχουσα αρχιτεκτονική της επιχείρησης.

Πίνακας 2-3 Cloud computing : Η προοπτική των πελατών

Dedicated/Traditional IT	**Cloud domputing**
Αρχικές υψηλές επενδύσεις για νέα κτήρια	Χαμηλές αρχικές επενδύσεις, μοντέλο πληρωμής με βάση την χρήση
Υψηλό κόστος για αξιόπιστη υποδομή	Η αξιοπιστία είναι ενσωματωμένη στην αρχιτεκτονική του cloud
Υψηλή πολυπλοκότητα του περιβάλλοντος τεχνολογίας πληροφορικής	Αρθρωτή αρχιτεκτονική περιβάλλοντος τεχνολογίας πληροφορικής
Πολύπλοκη υποδομή	Καθόλου υποδομή

2.6.1 Μικρή αρχική επένδυση και χαμηλό τρέχων κόστος

Με το δημόσιο cloud αποφεύγονται οι επενδύσεις σε κεφάλαιο γιατί δεν χρειάζεται να αγοραστεί υλικό, λογισμικό ή δικτυακές συσκευές. Η χρέωση του cloud γίνεται με βάση την χρήση, κάτι τέτοιο διευκολύνει το ξεκίνημα μιας επιχείρησης γιατί μειώνει το αρχικό κόστος της επένδυσης. Ανάλογα με το συμβόλαιο που έχει υπογραφεί οι εταιρείες μπορούν να το τερματίσουν όποτε το επιθυμούν, επομένως σε δύσκολες οικονομικές περιόδους το κόστος του cloud computing μπορεί να διαχειριστεί πολύ αποδοτικά.

2.6.2 Economies of Scale

Τα περισσότερα έργα ανάπτυξης έχουν μία φάση κατά την οποία ορίζονται οι απαραίτητοι πόροι, σε αυτή την φάση γίνεται μια προσπάθεια να υπολογιστούν οι απαιτήσεις σε υπολογιστική ισχύ, αποθήκευση, και μνήμη κατά την διάρκεια της ανάπτυξης, των δοκιμών και της παραγωγής. Συχνά είναι δύσκολο να γίνουν ακριβείς εκτιμήσεις και είναι σύνηθες το φαινόμενο να υπερεκτιμώνται ή να υποεκτιμώνται οι απαιτήσεις αυτές. Πολλές φορές το χρονικό διάστημα που χρειάζεται για να υπολογιστούν αυτοί οι πόροι μπορεί να είναι μεγάλο και προστίθεται στον χρόνο που χρειάζεται για να ολοκληρωθεί το έργο. Με την ευελιξία που προσφέρει το cloud computing οι εταιρείες μπορούν να ζητούν υπηρεσίες όταν τις χρειάζονται και για όσο τις χρειάζονται, πράγμα που σημαίνει ότι τα έργα που αναπτύσσουν διατρέχουν μικρότερο κίνδυνο να βρεθούν εκτός χρονικών ορίων.

2.6.3 Ανοιχτά Πρότυπα

Ορισμένες δυνατότητες του cloud computing βασίζονται σε ανοιχτά πρότυπα για να δομηθεί μια αρθρωτή (modular) αρχιτεκτονική η οποία να μπορεί να αναπτυχθεί γρήγορα και να αλλάζει όποτε αυτό απαιτείται. Το ανοιχτό λογισμικό ορίζεται ως λογισμικό που χορηγείται υπό την γενική δημόσια άδεια (General Public License) ή που ακολουθεί τον ορισμό της πρωτοβουλίας ανοιχτού κώδικα (OSI – Open Source Initiative) που επιτρέπει στους χρήστες να χρησιμοποιούν, να αλλάζουν και να βελτιώνουν το λογισμικό. (Open Source Initiave, http://www.opensource.org/docs/osd 17/10/2010 , GNU, http://www.gnu.org/licenses/licenses.html, 17/10/2010) Η δυνατότητα του να αλλάζει ο πηγαίος κώδικας είναι ουσιαστική στην συνεχή ανάπτυξη του cloud. Το ανοιχτό λογισμικό είναι θεμελιώδες στο cloud computing και πολύ σημαντικό για την εξέλιξη του.

2.6.4 Sustainability (Σταθερότητα)

Οι πάροχοι υπηρεσιών cloud επενδύουν σημαντικά ποσά για την δημιουργία μιας ευπροσάρμοστης αρχιτεκτονικής η οποία να παρέχει ένα πολύ σταθερό

περιβάλλον. Οι εταιρίες συχνά καταβάλουν μεγάλη προσπάθεια να συντηρήσουν τις υπηρεσίες τεχνολογίας πληροφορικής εξαιτίας είτε κάποιας βλάβης στο δίκτυο, είτε λόγω της έλλειψης συγχρονισμού με τις επιχειρησιακές αλλαγές τόσο σε όγκο όσο και στην φύση των συναλλαγών. Με το cloud computing οι εταιρείες βασίζονται στον πάροχο για να περιορίζει στο ελάχιστο τις βλάβες, να παρέχει μεγαλύτερη προσαρμοστικότητα μέσω του cluster, και να επενδύει σε κορυφαίες τεχνολογικές λύσεις.

2.7 Η επίδραση του Cloud Computing στους χρήστες

2.7.1 Ατομικοί καταναλωτές

Πολλοί ατομικοί χρήστες υπολογιστών είναι σήμερα βασικοί χρήστες του cloud computing, γιατί παρόλο που οι προσωπικοί υπολογιστές διαθέτουν αποθηκευτικά μέσα, βασίζονται στους παρόχους του cloud για πολλές από τις απαιτήσεις τους για αποθήκευση και υπολογιστικούς πόρους.

Οι χρήστες αποθηκεύουν τα προσωπικά τους email και τις φωτογραφίες τους στο cloud, αγοράζουν μουσική από κάποιον πάροχο cloud, αποθηκεύουν το προφίλ τους και πληροφορίες σε ιστοσελίδες κοινωνικής δικτύωσης (π.χ Facebook, LinkedIn, Myspace), λαμβάνουν πληροφορίες πλοήγησης, αναπτύσσουν ιστοσελίδες και συνεργάζονται με άλλους χρήστες του cloud. Οι καταναλωτές κάνουν αγορές, πραγματοποιούν αναζητήσεις, τηλεφωνούν ή επικοινωνούν με βίντεο, διαβάζουν ειδήσεις στο internet ή τακτοποιούν τις φορολογικές τους συναλλαγές μέσω του cloud. Οι καταναλωτές συνήθως αποδέχονται τους όρους χρήσης σαν μια διαδικασία ρουτίνας πράγμα που μπορεί να αποτελεί ρίσκο για την ιδιωτικότητα και θα πρέπει να τους απασχολεί κάτι τέτοιο. Φυσικά υπάρχει και το ενδεχόμενο να χαθούν πληροφορίες από κάποιο λάθος ή από μη εξουσιοδοτημένη από τον πάροχο πρόσβαση σε δεδομένα.

2.7.2 Ατομικές Επιχειρήσεις

Το χαμηλό αρχικό κόστος των υπηρεσιών του cloud κάνει όλο και περισσότερους ατομικούς καταναλωτές που έχουν τις τεχνικές γνώσεις να χρησιμοποιούν cloud εργαλεία για να αναπτύσσουν τις δικές τους επιχειρήσεις. Η προσδοκία είναι ότι δεν θα υπάρχει σχεδόν καθόλου χρέωση για το λογισμικό, αντί αυτού οι χρήστες θα πληρώνουν για κάποιες εξτρά υπηρεσίες ή δυνατότητες. Οι καταναλωτές μπορούν να χρησιμοποιούν κάποια ιστοσελίδα για να προσελκύουν πελάτες, να χρησιμοποιούν το ebay ή το Graigslist για να πουλήσουν προϊόντα, να διαχειριστούν τραπεζικούς λογαριασμούς online και να κάνουν κρατήσεις

εισιτηρίων ή να κανονίζουν τα ραντεβού τους. Όλα αυτά γίνονται με την υπολογιστική ισχύ που υπάρχει στο cloud.

2.7.3 Start Ups (επιχειρήσεις στο ξεκίνημα?)

Όταν ένας επιχειρηματίας ξεκινάει μια καινούργια δουλειά το να επενδύσει στο τμήμα τεχνολογίας πληροφορικής δεν αποτελεί υψηλή προτεραιότητα σε σχέση με την επένδυση του μάρκετινγκ ή της έρευνας και ανάπτυξης του προϊόντος. Παλαιότερα οι εταιρίες κατασκεύαζαν και λειτουργούσαν οι ίδιες το λογισμικό που χρειαζόντουσαν, τώρα αναθέτουν σε κάποιον τρίτο το μεγαλύτερο μέρος της ανάπτυξης του λογισμικού και διατηρούν ένα μικρό τμήμα τεχνολογίας πληροφορικής. Πλέον η μεγαλύτερη πρόκληση είναι να μπορεί ο πάροχος να βελτιώνει τις υποδομές καθώς ο όγκος των εργασιών αυξάνεται και να μετατρέπει την υπηρεσία για να υποστηρίζει νέα προϊόντα, αγορές και επιχειρηματικά μοντέλα. Το σημαντικότερο όμως είναι να επιτυγχάνεται η δια-συνεργασία μεταξύ διαφορετικών πλατφόρμων που βρίσκονται εντός και εκτός του cloud.

2.7.4 Μικρού και μεσαίου μεγέθους επιχειρήσεις

Υπάρχουν αρκετοί ορισμοί για τις μικρές και μεσαίες επιχειρήσεις και η κύρια κατηγοριοποίηση έχει να κάνει με τα οικονομικά μεγέθη. Αλλά όταν πρόκειται για τεχνολογικές απαιτήσεις πρέπει να λαμβάνεται υπόψη ο αριθμός τον προϊόντων, οι χώρες στις οποίες λειτουργεί η επιχείρηση, και η αλυσίδα προμηθειών. Ο όρος μικρή επιχείρηση έχει να κάνει δηλαδή με την πολυπλοκότητα της επιχείρησης. Η ανάγκη για ασφάλεια και ιδιωτικότητα στις μικρές επιχειρήσεις δεν διαφέρει σε τίποτα από τις μεγάλες επιχειρήσεις. Οι μικρές επιχειρήσεις συνήθως διαθέτουν μικρά τμήματα τεχνολογίας πληροφορικής τα οποία δεν διαθέτουν τις απαραίτητες ικανότητες και την γνώση που διαθέτουν τα αντίστοιχα τμήματα των μεγάλων εταιριών. Σε σημαντικά έργα αντιμετωπίζουν δυσκολίες στην ανάπτυξη, η υποδομή πολλές φορές θεωρείται ξεπερασμένη, και το τμήμα τεχνολογίας πληροφορικής δυσκολεύεται να ανταποκριθεί στις ανάγκες της επιχείρησης. Οι μικρές και μεσαίες επιχειρήσεις έχουν χαρακτηρίστηκα που μπορούν να έχουν μεγάλη ανάπτυξη με την ευρεία χρήση του cloud. Ενδεχομένως οι εταιρείες αυτές να είναι οι πρώτες που η υποδομή τους και τα τμήματα τεχνολογίας πληροφορικής θα βρίσκονται εξολοκλήρου στο cloud και θα παρέχονται από συνδυασμό διαφόρων παρόχων cloud.

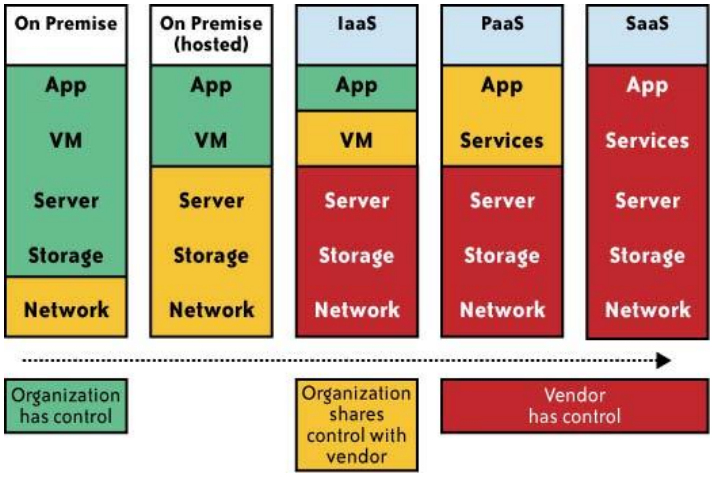
2.7.5 Μεγάλες επιχειρήσεις

Οι μεγάλες επιχειρήσεις διευρύνουν την χρήση του cloud computing, σε έναν ελάχιστο βαθμό αυτό σημαίνει πώς επιτρέπουν στους χρήστες να έχουν πρόσβαση σε υπηρεσίες πέρα από το τοίχος προστασίας της εταιρείας. Μια ευρύτερη χρήση των υπηρεσιών του cloud περιλαμβάνει εργαλεία που υποστηρίζουν την παραγωγικότητα όπως online έρευνα ή ταξιδιωτικές υπηρεσίες. Οι εταιρίες που υιοθετούν το cloud computing μπορεί να χρησιμοποιούν εφαρμογές σε σημαντικά τμήματα και δραστηριότητες, όπως τις εφαρμογές του Salesforce.com, εφαρμογές διαχείρισης εγγράφων, εφαρμογές αγορών και logistic. Σε αυτές τις περιπτώσεις οι χρήστες έχουν πρόσβαση στις εφαρμογές και αποθηκεύουν δεδομένα στο cloud που περιλαμβάνουν προσωπικές και ευαίσθητες πληροφορίες, πράγμα που σημαίνει ότι εμπεριέχονται ζητήματα ασφάλειας και ιδιωτικότητας. Μια σημαντική επίσης ανησυχία είναι τα αντίγραφα των δεδομένων που κρατάει ο πάροχος και πως αυτά διαχειρίζονται.

2.8 Η διαχείριση στο Cloud

Η εικόνα 2.11 παρουσιάζει την επίδραση του cloud computing στην διαχείριση των δομών των οργανισμών τεχνολογίας πληροφορικής. Παραδοσιακά, οι περισσότεροι οργανισμοί τεχνολογίας πληροφορικής διαχειρίζονται τα πέντε τεχνολογικά επίπεδα που φαίνονται στην εικόνα. Τα δύο on-premise (μέσα στην επιχείρηση) μοντέλα δείχνουν ότι το τμήμα τεχνολογίας πληροφορικής έχει τον πλήρη έλεγχο και ευθύνη και των πέντε τεχνολογικών επιπέδων. Ωστόσο καθώς προχωράμε από το IaaS στο PaaS και στο SaaS το επίπεδο ελέγχου από τον οργανισμό μειώνεται και αυξάνεται το επίπεδο ελέγχου παρόχου. Παρόλο όμως που το επίπεδο ελέγχου του παρόχου αυξάνει η ευθύνη παραμένει στον οργανισμό. Είναι σημαντικό για τους οργανισμούς τεχνολογίας πληροφορικής να αναπτύσσουν ισχυρά πλαίσια εργασίας (framework) παρακολούθησης πάνω από το SPI μοντέλο διανομής, για να διασφαλίζουν ότι το επίπεδο των υπηρεσιών τους συμβαδίζει με τις δεσμευτικές τους υποχρεώσεις.

Εικόνα 2.11 Η επίδραση του cloud computing στην διαχείριση των δομών των οργανισμών τεχνολογιών πληροφορικής.



2.9 Φραγμοί στην υιοθέτηση του cloud από τις επιχειρήσεις

Παρόλο που υπάρχουν πολλά προνόμια για την υιοθέτηση του cloud computing υπάρχουν επίσης και σημαντικοί φραγμοί. Οι δύο ποιο σημαντικοί φραγμοί είναι η ασφάλεια και η ιδιωτικότητα.

2.9.1 Ασφάλεια

Επειδή το cloud computing αντιπροσωπεύει ένα νέο υπολογιστικό μοντέλο υπάρχουν αρκετές ανακρίβειες σχετικά με το πώς η ασφάλεια σε όλα τα επίπεδα (π.χ. επίπεδο δικτύου, φιλοξενίας, εφαρμογών, και επίπεδο δεδομένων) επιτυγχάνεται. Αυτές οι ανακρίβειες αποτελούν την νούμερο ένα ανησυχία των διοικητικών στελεχών για το cloud computing.

2.9.2 Ιδιωτικότητα

Η ικανότητα του cloud computing να επιλυθεί επαρκώς την διατήρηση της ιδιωτικότητας τίθεται υπό αμφισβήτηση. Οι οργανισμοί σήμερα αντιμετωπίζουν πολυάριθμες διαφορετικές απαιτήσεις προσπαθώντας να προστατέψουν την ιδιωτικότητα των προσωπικών πληροφοριών. Δεν είναι ξεκάθαρο κατά πόσο το μοντέλο του cloud computing περιέχει επαρκή προστασία ή κατά πόσο οι οργανισμοί θα βρεθούν να παραβιάζουν τους κανονισμούς εξαιτίας του νέου αυτού μοντέλου.

2.9.3 Συνδεσιμότητα και ανοιχτή πρόσβαση

Οι πλήρεις δυνατότητες του cloud computing εξαρτώνται από τη διαθεσιμότητα πρόσβασης υψηλών ταχυτήτων. Μια τέτοια συνδεσιμότητα όπως για παράδειγμα η παροχή ηλεκτρικού ρεύματος, δίνει προοπτική στις βιομηχανίες σε παγκόσμιο επίπεδο και ανοίγει δρόμους για νέα προϊόντα. Η συνδεσιμότητα και η ανοιχτή

πρόσβαση σε υπολογιστική ισχύ και πληροφορίες που διαθέτονται μέσω του cloud computing οδηγεί σε μια νέα εποχή εκβιομηχάνισης.

2.9.4 Αξιοπιστία

Οι εφαρμογές για τις εταιρίες είναι ζωτικής σημασίας και πρέπει να είναι αξιόπιστες και διαθέσιμες για λειτουργία 24/7. Σε περιπτώσεις βλάβης ή διακοπής λειτουργίας θα πρέπει να λειτουργεί κάποιο σχέδιο έκτακτης ανάγκης, και σε περιπτώσεις καταστροφών θα πρέπει να υπάρχει σχέδιο αποκατάστασης με την μικρότερη δυνατή αναστάτωση. Κάθε πλευρά της αξιοπιστίας πρέπει να εξετάζεται προσεκτικά όταν κάποιος συμβάλλεται με έναν πάροχο cloud και να διαπραγματεύεται σαν όρος του SLA. Επίσης θα πρέπει να πραγματοποιούνται δοκιμαστικά σενάρια βλάβης.

2.9.5 Διασυνεργασία (Interoperability)

Η διασυνεργασία και η φορητότητα των πληροφοριών μεταξύ ιδιωτικών και δημόσιων cloud είναι ζωτικής σημασίας για την ευρεία υιοθέτηση του cloud computing από τις επιχειρήσεις. Πολλές εταιρίες έχουν σημειώσει σημαντική πρόοδο στην προσπάθεια προτυποποίησης των διαδικασιών, των δεδομένων, και των συστημάτων μέσω της υλοποίησης των ERP. Αυτή η διαδικασία επιτυγχάνεται με υποδομές που δημιουργούν απλά στιγμιότυπα (instances) , ή ισχυρές ενιαίες συνδέσεις μεταξύ των στιγμιότυπων, για να διαχειρίζονται την συνέπεια των δεδομένων και να παράγουν αξιόπιστες και ενιαίες πληροφορίες. Ακόμα και με αυτές τις βελτιωμένες πλατφόρμες, η ταχύτητα με την οποία αλλάζουν οι επιχειρήσεις μπορεί να υπερνικήσει την ικανότητα των οργανισμών τεχνολογίας πληροφορικής να ανταπεξέλθουν σε αυτές τις αλλαγές. Οι εφαρμογές SaaS που παρέχονται μέσω του cloud αποτελούν μια επιλογή που υλοποιείται γρήγορα και με μικρό κεφάλαιο. Ανάλογα με την εφαρμογή είναι σημαντικό να συνεργάζεται και με άλλες εφαρμογές που βρίσκονται στο cloud ή σε μια κλασική τεχνολογία.

2.9.6 Ανεξαρτησία από τον πάροχο του cloud

Υπάρχουν παραδείγματα συμβολαίων που κρατάνε τους καταναλωτές σε υπηρεσίες που δεν παρέχουν αυτά που πραγματικά χρειάζεται ο πελάτης. Αυτό οφείλεται σε διάφορους λόγους και θα πρέπει να δίνεται προσοχή από τον πελάτη για το αν υπάρχει η δυνατότητα να αλλάξει γρήγορα πάροχο, χωρίς μεγάλο μεταβατικό στάδιο και χρηματικές ποινές. Ο πάροχος μπορεί να κρατάει σημαντικά δεδομένα που να μην μπορούν εύκολα να μετακινηθούν σε άλλον πάροχο.

Πρότυπα που θα επέτρεπαν την μεταφορά από το ένα cloud στο άλλο και το “plug and play” των συστατικών του cloud θα βοηθούσαν. Για παράδειγμα μια εταιρία σήμερα δεν εξαρτάται από τον πάροχο του φυλλομετρητή, αλλά μπορεί να εξαρτάται από την χρήση μιας ιδιωτικής δομής δεδομένων. Το να ξεχωρίζει μια εταιρία τον πάροχο αποθήκευσης από κάποιον άλλον πάροχο επεξεργαστικής ισχύς μπορεί να έχει μεγαλύτερη ευελιξία. Βέβαια αυτή η επιλογή έχει το μειονέκτημα ότι ο πελάτης θα πρέπει να αναλάβει την ενοποίηση αυτών των υπηρεσιών.

2.9.7 Οικονομικά οφέλη

Με το να μοιράζονται οι πόροι, με την πληρωμή ανάλογα με την χρήση και με τις χαμηλές απαιτήσεις σε αρχικά κεφάλαια υπάρχουν σημαντικά οικονομικά οφέλη. Υπάρχει όμως και η ανάγκη να υπολογιστούν προσεκτικά όλα τα κόστη και τα πλεονεκτήματα του cloud computing τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα. Στα κόστη συμπεριλαμβάνονται και κρυφές χρεώσεις όπως υποστήριξη, επαναφορά από καταστροφές, τροποποιήσεις εφαρμογών, και ασφάλεια απώλειας δεδομένων. Πέρα από κάποιο οικονομικό όριο οι ενιαίες επενδύσεις ή οι συνδυασμένες υπηρεσίες του cloud γίνονται πιο συμφέρουσες. Για παράδειγμα μπορεί να μην είναι αποδοτικό να χρησιμοποιούνται πολλαπλές αυτόνομες εφαρμογές SaaS γιατί για κάθε εφαρμογή μπορεί να απαιτείται μια έξτρα υπηρεσία επαναφοράς από καταστροφή. Για αυτό όλες οι λειτουργίες θα πρέπει να συνδυαστούν ως μια ενιαία υπηρεσία.

2.9.8 Διαχείριση τεχνολογιών πληροφορικής

Τα οικονομικά οφέλη είναι σημαντικοί παράγοντες στην διαχείριση τεχνολογιών πληροφορικής. Για μια αποδοτική διαχείριση είναι σημαντικό να προσδιοριστεί το κατάλληλο περιεχόμενο για να παρθούν επενδυτικές αποφάσεις και να ισορροπήσουν οι βραχυπρόθεσμες και μακροπρόθεσμες ανάγκες.

ΕΠΙΛΟΓΟΣ

Με την υπερβολική προβολή του cloud computing και τους πολλούς ορισμούς που έχουν δοθεί για αυτό, είναι δύσκολο να γίνει αντιληπτό το τι ακριβώς είναι το cloud computing. Το πρόβλημα αυτό γίνεται πιο έντονο όσο οι κατασκευαστές βιάζονται να ισχυριστούν ότι είναι πλέον εταιρίες cloud, ενώ ξαφνικά ολόκληρος ο τεχνολογικός τομέας έγινε “Cloudy”. Στο κεφάλαιο αυτό έγινε μια παρουσίαση των σημερινών προτύπων μοντέλων διανομής, SPI, και των τύπων του Cloud computing. Επίσης παρουσιάστηκαν τα προνόμια της χρήσης του cloud computing και οι σημαντικότεροι λόγοι για την υιοθέτηση του. Στο επόμενο κεφάλαιο θα εξεταστεί εκτενέστερα η περιοχή της ασφάλειας στο cloud, οι ευπάθειες, οι μηχανισμοί και τα μοντέλα ασφάλειας.

ΚΕΦΑΛΑΙΟ 3 Ζητήματα ασφάλειας το Cloud

ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα γίνει παρουσίαση των απειλών που σχετίζονται με την ασφάλεια της υποδομής ενός οργανισμού στο επίπεδο δικτύου, φιλοξενίας και εφαρμογών καθώς και τρόποι προστασία από αυτές. Επίσης προσεγγίζεται η ασφάλεια υποδομής στο πλαίσιο του SPI μοντέλου διανομής του Cloud (SaaS, PaaS, IaaS) και του επιχειρησιακού μοντέλου (δημόσιο, ιδιωτικό και υβριδικό cloud). Τέλος γίνεται παρουσίαση της τρέχουσας κατάστασης της πρακτικής διαχείρισης ταυτοποίησης και πρόσβασης (IAM- Identity and Access Management) και χαρακτηριστικών της IAM που ενισχύουν την Αυθεντικοποίηση, Εξουσιοδότηση και τον Έλεγχο της πρόσβασης των χρηστών στις υπηρεσίες του Cloud.

3.1 Ασφάλεια Υποδομής: Επίπεδο Δικτύου

Όταν προσεγγίζουμε την ασφάλεια της υποδομής στο επίπεδο δικτύου είναι σημαντικό να υπάρχει η διάκριση μεταξύ του δημόσιου και ιδιωτικού cloud . Στο ιδιωτικό cloud δεν υπάρχουν νέες επιθέσεις, ευπάθειες ή αλλαγές στους κινδύνους της συγκεκριμένης τεχνολογίας, τις οποίες το προσωπικό της ασφάλειας πρέπει να λάβει υπόψη. Παρόλο που η αρχιτεκτονική της τεχνολογίας πληροφορικής ενός οργανισμού μπορεί να αλλάξει με την υλοποίηση ενός ιδιωτικού cloud, η τοπολογία του δικτύου πιθανότατα δεν θα αλλάξει σημαντικά. Αν υπάρχει εγκατεστημένο ένα ιδιωτικό extranet (π.χ για προνομιούχους πελάτες ή στρατηγικούς συνεργάτες) , για πρακτικούς λόγους πιθανότατα υπάρχει εγκατεστημένη η τοπολογία δικτύου για ένα ιδιωτικό cloud. Τα ζητήματα ασφάλειας που υπάρχουν στον οργανισμό ήδη, ταιριάζουν με αυτά της αρχιτεκτονικής ιδιωτικού cloud. Επίσης τα εργαλεία που υπάρχουν (ή που θα έπρεπε να υπάρχουν) είναι αναγκαία για το ιδιωτικό cloud και δουλεύουν με τον ίδιο τρόπο. Η εικόνα 3.1 περιγράφει ομοιότητες μεταξύ της τοπολογίας ενός ασφαλούς extranet και ενός ιδιωτικού cloud.

Ωστόσο αν χρησιμοποιήσουμε υπηρεσίες δημόσιου cloud, τότε το να αλλάξουν οι απαιτήσεις ασφάλειας, προϋποθέτει αλλαγές στην τοπολογία του δικτύου. Πρέπει να προσδιοριστεί πώς η υπάρχουσα αρχιτεκτονική δικτύου αλληλεπιδρά με την τοπολογία δικτύου του παρόχου. Υπάρχουν τέσσερεις σημαντικές απαιτήσεις ασφάλειας σε αυτή την περίπτωση (Mather κ.α., 2009) :

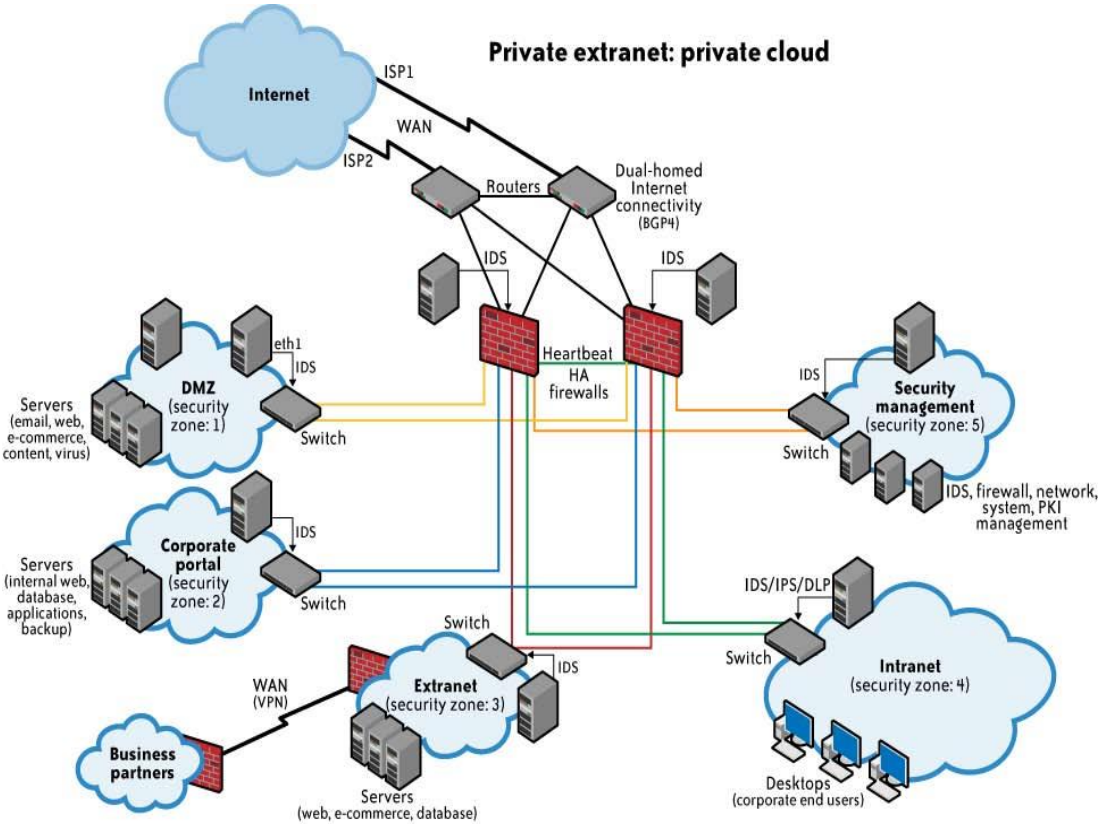
- Διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων του οργανισμού που μεταδίδονται από και προς το δημόσιο cloud του παρόχου.

- Διασφάλιση των κατάλληλων ελέγχων πρόσβασης (αυθεντικοποίηση, εξουσιοδότηση, έλεγχος), σε οποιοσδήποτε πόρους χρησιμοποιούνται στο δημόσιο cloud του παρόχου.
- Διασφάλιση της διαθεσιμότητας των πόρων που παρέχονται μέσω του internet σε ένα δημόσιο cloud και χρησιμοποιούνται από τον οργανισμό ή έχουν εξουσιοδοτηθεί στον οργανισμό από τον πάροχο δημόσιου cloud.
- Αντικατάσταση του υπάρχοντος μοντέλου που αποτελείται από ζώνες δικτύου και βαθμίδες με περιοχές αναφοράς

3.1.1 Διασφάλιση της ακεραιότητας και της Εμπιστευτικότητας των Δεδομένων

Μερικοί πόροι και δεδομένα που πριν ήταν περιορισμένα σε ένα ιδιωτικό δίκτυο τώρα εκτίθενται στο internet και σε ένα κοινό δημόσιο δίκτυο που ανήκει σε κάποιον τρίτο πάροχο cloud. Ένα παράδειγμα προβλημάτων που σχετίζονται με τον πρώτο παράγοντα ρίσκου είναι ένα κενό ασφαλείας του Amazon Web Services (AWS) που δημοσιεύτηκε το 2008 (http://www.daemonology.net/blog/2008-12.html ,AWS signature version 1 is insecure). Ο συγγραφέας του άρθρου δημοσίευσε σε ένα blog λεπτομέρειες σχετικά με μια ατέλεια στον αλγόριθμο ψηφιακής υπογραφής, εκτελώντας ένα ερώτημα (Query request) στο Amazon SimpleDB, στο Amazon Elastic Compute Cloud (EC2) ή στο Amazon Simple Queue Service (SQS) μέσω του πρωτοκόλλου HTTP. Παρόλο που οι χρήση του πρωτοκόλλου HTTPS (σε αντίθεση με το HTTP) θα άμβλυνε τον κίνδυνο της ακεραιτότητας , οι χρήστες που δεν χρησιμοποιούσαν το HTTPS (αλλά χρησιμοποιούσαν το HTTP) αντιμετώπισαν έναν αυξημένο κίνδυνο να αλλάξουν τα δεδομένα τους κατά την μετάδοση εν αγνοία τους.

Εικόνα 3-1Τοπολογία δικτύου ιδιωτικού cloud computing



3.1.2 Διασφάλιση κατάλληλου ελέγχου πρόσβασης

Από την στιγμή που κάποια τμήματα ή και όλοι οι πόροι είναι τώρα εκτεθειμένοι στο internet, ένας οργανισμός που χρησιμοποιεί ένα δημόσιο δίκτυο αντιμετωπίζει εμφανώς αυξημένους κινδύνους στα δεδομένα του. Η δυνατότητα να ελέγχει τις λειτουργίες του δικτύου του παρόχου cloud (π.χ επίβλεψη σε πραγματικό χρόνο όπως θα έκανε στο δίκτυο του) ή ακόμα και μετά από κάποιο γεγονός , πιθανότατα δεν υπάρχει. Ο οργανισμός έχει μειωμένη πρόσβαση σε ουσιώδη logs και δεδομένα σε επίπεδο δικτύου και περιορισμένη δυνατότητα να ερευνήσει και να συγκεντρώσει δεδομένα forensic.

Ένα παράδειγμα προβλήματος που σχετίζεται με τον δεύτερο παράγοντα ρίσκου είναι το ζήτημα της επαναχρησιμοποίησης (επαναεκχώρησης) διευθύνσεων IP. Μιλώντας γενικά οι πάροχοι cloud δεν διαχειρίζονται με ασφάλεια και επάρκεια τις ip όταν δεν χρειάζονται πλέον σε έναν πελάτη. Οι διευθύνσεις συνήθως

επαναεκχωρούνται και επαναχρησιμοποιούνται από άλλους πελάτες όταν αυτές γίνονται διαθέσιμες. Από την οπτική γωνία του παρόχου κάτι τέτοιο έχει νόημα γιατί οι διευθύνσεις IP είναι μια πεπερασμένη ποσότητα και ένας χρεώσιμος πόρος. Ωστόσο από την οπτική γωνία της ασφάλειας του πελάτη η παραμονή διευθύνσεων IP που δεν είναι πλέον σε χρήση μπορεί να αποτελέσει πρόβλημα. Ο πελάτης δεν μπορεί να υποθέσει ότι η πρόσβαση στους πόρους του έχει τερματιστεί μετά την απελευθέρωση της διεύθυνσης IP.Υπάρχει απαραίτητα ένας χρόνος καθυστέρησης μεταξύ της αλλαγής μια διεύθυνσης IP στον DNS και της οριστικής εκκαθάρισης αυτής της διεύθυνσης από την μνήμη Cache του DNS. Αυτό σημαίνει ότι ακόμα και αν αυτές οι διευθύνσεις έχουν αλλάξει, οι (τωρινές) παλιές διευθύνσεις είναι ακόμα διαθέσιμες στην cache,επομένως επιτρέπουν ακόμα τους χρήστες να φτάνουν αυτούς τους υποθετικά ανύπαρκτους πόρους.

Το πρόβλημα με τις διευθύνσεις IP και τη μη εξουσιοδοτημένη πρόσβαση σε πόρους, δεν συναντάται μόνο στις δρομολογήσιμες (routable) IP διευθύνσεις (π.χ πόροι που προορίζονται να είναι διαθέσιμοι απευθείας από το Internet). Το ζήτημα αυτό συναντάται επίσης στα εσωτερικά δίκτυα των παρόχων Cloud που χρησιμοποιούνται από τους πελάτες και την ανάθεση μη δρομολογίσιμων διευθύνσεων IP. Αν και οι πόροι μπορεί να μην είναι προσβάσιμοι απευθείας από το internet, για λόγους διαχείρισης κάθε δημόσιος πόρος έχει επίσης μια ιδιωτική διεύθυνση. Άλλοι πελάτες του παρόχου Cloud με κακόβουλη διάθεση μπορεί να είναι ικανοί να προσπελάσουν πόρους άλλων πελατών μέσω του ιδιωτικού δικτύου του παρόχου. Καλύτερες τεχνικές εμφανίστηκαν στην αγορά βοηθώντας να ανακουφιστεί το πρόβλημα της επαναχρησιμοποίησης διευθύνσεων IP, ένα παράδειγμα είναι και το VPN-Cubed της CohesiveFT (http://www.cohesiveft.com/vpncubed/) αλλά αυτό το προϊόν δεν παρέχεται ως υπηρεσία από τους περισσότερους παρόχους cloud.

3.1.3 Διασφάλιση διαθεσιμότητας των προσβάσιμων μέσω Internet πόρων

Η εξάρτηση στην ασφάλεια δικτύου έχει αυξηθεί εξαιτίας της αύξησης των δεδομένων ή της αύξησης του προσωπικού των οργανισμών που τώρα εξαρτώνται από συσκευές που φιλοξενούνται εξωτερικά, για να εξασφαλίσουν την διαθεσιμότητα των πόρων του παρόχου Cloud. Συμπερασματικά οι τρείς παράγοντες (ακεραιότητα και εμπιστευτικότητα, έλεγχοι πρόσβασης,

διαθεσιμότητα πόρων) που απαριθμούνται πιο πάνω πρέπει να είναι αποδεκτοί από τον οργανισμό.

Ένα καλό παράδειγμα του τρίτου παράγοντα ρίσκου είναι το hijacking στο πρόθεμα του BGP.Το hijacking του προθέματος αναγκάζει ένα αυτόνομο σύστημα να ανακοινώσει ένα διάστημα (εύρος) διευθύνσεων που ανήκει σε κάποιον άλλον χωρίς την άδεια του. Τέτοιες ανακοινώσεις συχνά συμβαίνουν εξαιτίας λαθών στην διαμόρφωση, αλλά αυτή η λανθασμένη διαμόρφωση μπορεί ακόμα να επηρεάσει την διαθεσιμότητα των πόρων που βασίζονται στο Cloud. Σύμφωνα με μια μελέτη που παρουσιάστηκε στο North American Networks Group (NANOG) (http://www.nanog.org/meetings/nanog36/presentations/boothe.pdf) το Φεβρουάριο του 2006 αρκετές εκατοντάδες τέτοιων λανθασμένων διαμορφώσεων συμβαίνουν κάθε μήνα.

Σε αντίθεση με τις λανθασμένες διαμορφώσεις υπάρχουν επίσης και εσκεμμένες επιθέσεις. Αν και το ζήτημα του hijacking του προθέματος μέσω εσκεμμένων επιθέσεων συναντάται λιγότερο από ότι οι λανθασμένες διαμορφώσεις, παρόλα αυτά ακόμα υπάρχει και μπορεί να μπλοκάρει την πρόσβαση σε δεδομένα. Σύμφωνα με την ίδια μελέτη που παρουσιάστηκε στο NANOG, οι επιθέσεις αυτές συμβαίνουν λιγότερο από εκατό φορές ανά μήνα. Αν και το και το hijacking δεν είναι κάτι καινούργιο , η εμφάνιση αυτών των επιθέσεων θα αυξηθεί και πιθανώς σε σημαντικό βαθμό , όσο διαδίδεται το Cloud computing. Όσο η χρήση του cloud computing αυξάνεται, τόσο αυξάνεται για τους πελάτες η αξία της διαθεσιμότητας των πόρων που βρίσκονται στο cloud. Η αυξημένη αξία για τους πελάτες μεταφράζεται σε ένα αυξημένο ρίσκο κακόβουλων ενεργειών για την απειλή και διατάραξη αυτής της διαθεσιμότητας.

Οι επιθέσεις στον DNS είναι ένα ακόμα παράδειγμα προβλήματος που σχετίζεται με τον τρίτο παράγοντα ρίσκου. Είναι γεγονός ότι υπάρχουν διάφορες μορφές επιθέσεων στον DNS με πρόθεση το cloud computing που προκαλούν ανησυχία. Παρόλο που οι επιθέσεις στον DNS δεν είναι κάτι νέο και δεν σχετίζονται απευθείας με την χρήση του Cloud, το ζήτημα είναι σημαντικό για έναν οργανισμό ως προς το ρίσκο σε επίπεδο δικτύου εξαιτίας της αύξησης των εξωτερικών ερωτημάτων στον DNS. Μειώνεται έτσι η αποτελεσματικότητα του “split horizon” στην διαμόρφωση του DNS, και επίσης αυξάνεται ο αριθμός του προσωπικού που

εξαρτώνται περισσότερο από την ασφάλεια του δικτύου για την διασφάλιση της διαθεσιμότητας των πόρων του παρόχου cloud που χρησιμοποιούν.

Παρόλο που το σφάλμα γνωστό ως “Kaminsky Bug” τράβηξε την μεγαλύτερη προσοχή στην περιοχή της ασφάλειας το 2008, άλλα προβλήματα του DNS επηρεάζουν επίσης το Cloud. Όχι μόνο υπάρχουν ευπάθειες στο DNS πρωτόκολλο και στην υλοποίηση του DNS, αλλά υπάρχουν και αρκετά διαδεδομένες επιθέσεις στην cache μνήμη του DNS μέσω των οποίων ένας DNS εξυπηρετητής εξαπατάται και λαμβάνει λανθασμένες πληροφορίες. Αν και πολλοί άνθρωποι πιστεύουν ότι αυτού του είδους οι επιθέσεις καταπολεμήθηκαν πριν χρόνια, αυτό δεν είναι αλήθεια, και αυτές οι επιθέσεις εξακολουθούν να είναι σημαντικό πρόβλημα, ειδικά στο περιβάλλον του Cloud. Διαφορετική εκδοχή της βασικής επίθεσης στην μνήμη cache περιλαμβάνει την ανακατεύθυνση του στόχου του DNS εξυπηρετητή (NS), ανακατεύθυνση της εγγραφής NS σε ένα άλλο Domain και ανταπόκριση πριν του πραγματικού NS.

Ένα τελικό παράδειγμα προβλήματος που σχετίζεται με τον τρίτο παράγοντα ρίσκου, είναι οι επιθέσεις άρνησης υπηρεσίας (denial of service, DoS) και κατανεμημένης άρνησης υπηρεσίας (distributed denial of service, DDoS). Ξανά αν και οι επιθέσεις DoS/DDoS δεν είναι καινούργιες και δεν σχετίζονται άμεσα με την χρήση του Cloud computing, το ζήτημα για αυτές τις επιθέσεις και το cloud computing είναι σημαντικό για τον οργανισμό ως προς το ρίσκο σε επίπεδο δικτύου εξαιτίας της αυξημένης χρήσης πόρων που βρίσκονται εξωτερικά του δικτύου του.

Ωστόσο όταν χρησιμοποιείται IaaS ο κίνδυνος DDoS επιθέσεων δεν είναι μόνο εξωτερικός . Υπάρχει επίσης ο κίνδυνος μιας εσωτερικής επίθεσης DDoS, μέσα από το τμήμα του δικτύου του παρόχου IaaS που χρησιμοποιείται από τους χρήστες (ξεχωριστά από το εξωτερικό δίκτυο του παρόχου IaaS). Αυτό το εσωτερικό (μη δρομολογήσιμο) δίκτυο είναι ένας διαμοιραζόμενος πόρος που χρησιμοποιείται από τους πελάτες για να έχουν πρόσβαση στους μη δημόσια στιγμιότυπα (π.χ Amazon Machine Images ή AMIS) καθώς και από τους παρόχους για να διαχειρίζονται τους πόρους δικτύου (όπως π.χ φυσικούς εξυπηρετητές).

Δεν υπάρχει κάτι που να αποτρέπει έναν πελάτη που έχει πρόσβαση στο εσωτερικό δίκτυο στο να βρει και να επιτεθεί σε άλλους πελάτες , ή την υποδομή του παρόχου IaaS, και ο πάροχος πιθανότατα να μην έχει κάποιο έλεγχο εντοπισμού έστω για να ενημερωθεί για μια επίθεση. Ο μόνος αποτρεπτικός μηχανισμός που έχουν οι άλλοι πελάτες είναι το πόσο ανθεκτικά είναι τα στιγμιότυπα τους (π.χ AMIS) και αν ο πάροχος εφαρμόζει μηχανισμούς άμυνας μέσω firewall.

3.1.4 Αντικατάσταση του υπάρχοντος μοντέλου που αποτελείται από ζώνες δικτύου και βαθμίδες με περιοχές διαβαθμισμένης εμπιστοσύνης

Το καθιερωμένο απομονωμένο μοντέλο με ζώνες δικτύου και βαθμίδες δεν υπάρχει πλέον στο δημόσιο IaaS και στο PaaS cloud. Για χρόνια, η ασφάλεια δικτύου βασιζόταν στην ύπαρξη ζωνών όπως αυτές του intranet και του extranet για να απομονωθεί η κίνηση του δικτύου και να βελτιωθεί η ασφάλεια. Το μοντέλο αυτό βασίζεται στον αποκλεισμό, μόνο άτομα και συστήματα με συγκεκριμένο ρόλο έχουν πρόσβαση σε συγκεκριμένες ζώνες. Παρομοίως, συστήματα μέσα σε μια συγκεκριμένη βαθμίδα συχνά έχουν πρόσβαση μόνο μέσα σε ή διαμέσου μιας συγκεκριμένης βαθμίδας. Για παράδειγμα, συστήματα μέσα στη βαθμίδα παρουσίασης δεν επιτρέπεται να επικοινωνούν απευθείας με συστήματα στην βαθμίδα βάσεων δεδομένων, αλλά μπορούν να επικοινωνούν μόνο με ένα εξουσιοδοτημένο σύστημα μέσα στην ζώνη εφαρμογών. Τα SaaS cloud που χτίζονται μέσα σε δημόσια IaaS ή PaaS cloud έχουν παρόμοια χαρακτηριστικά . Ωστόσο ένα δημόσιο SaaS που χτίζεται μέσα σε ένα ιδιωτικό IaaS (π.χ Salesforce.com) μπορεί να ακολουθεί το παραδοσιακό απομονωμένο μοντέλο, αλλά συνήθως αυτή η πληροφορία για την τοπολογία δεν μοιράζεται με τους πελάτες.

Το παραδοσιακό μοντέλο με ζώνες δικτύου και βαθμίδες έχει αντικατασταθεί στο δημόσιο cloud computing με “ομάδες ασφάλειας (security group)”, “περιοχές ασφάλειας”, ή “εικονικά κέντρα δεδομένων” τα οποία έχουν λογικό διαχωρισμό μεταξύ των βαθμίδων αλλά είναι λιγότερο ακριβή και απαιτούν λιγότερη προστασία από το προηγούμενο καθιερωμένο μοντέλο. Για παράδειγμα, οι ομάδες ασφάλειας χαρακτηριστικό στο AWS επιτρέπει τις εικονικές μηχανές να έχουν πρόσβαση η μία στην άλλη χρησιμοποιώντας ένα εικονικό firewall το οποίο έχει την ικανότητα να φιλτράρει την κίνηση με βάση τις IP διευθύνσεις (μια συγκεκριμένη διεύθυνση ή ένα εύρος διευθύνσεων), τους τύπους των πακέτων (TCP, UDP, ή ICMP), και τις πόρτες ή ένα εύρος τους.

Στο υπάρχων μοντέλο με ζώνες και βαθμίδες, όχι μόνο τα συστήματα ανάπτυξης είναι λογικά διαχωρισμένα από τα συστήματα παραγωγής στο επίπεδο δικτύου, αλλά οι δύο αυτές ομάδες συστημάτων είναι επίσης φυσικά διαχωρισμένα στο επίπεδο φιλοξενίας (host)(π.χ τρέχουν σε διαφορετικούς φυσικούς εξυπηρετητές και σε λογικά διαχωρισμένες ζώνες δικτύου).Με το cloud computing αυτός ο διαχωρισμός δεν υφίσταται πλέον. Το μοντέλο διαχωρισμού του cloud computing σε domains παρέχει λογικό διαχωρισμό μόνο για λόγους διεύθυνσιοδότησης. Δεν είναι απαραίτητος πλέον κανένας φυσικός διαχωρισμός, αφού το domain δοκιμών και το domain παραγωγής μπορούν να είναι στον ίδιο φυσικό εξυπηρετητή. Επιπλέον ο προηγούμενος λογικός διαχωρισμός στο επίπεδο δικτύου δεν υπάρχει, ο λογικός διαχωρισμός πλέον είναι στο επίπεδο φιλοξενίας με τα δύο domain να τρέχουν στον ίδιο φυσικό εξυπηρετητή και να διαχωρίζονται λογικά μόνο από τον υπερ-επόπτη(hypervisor) της εικονικής μηχανής (VM).

3.1.5 Μετριασμός των κινδύνων στο επίπεδο δικτύου

Αρχικά να σημειωθεί ότι οι κίνδυνοι στο επίπεδο δικτύου υπάρχουν ασχέτως με τον τύπο του cloud computing που χρησιμοποιείται (π.χ SaaS, IaaS, PaaS) Ο πρώτος καθορισμός του επιπέδου κινδύνου δεν είναι ποια αρχιτεκτονική Cloud χρησιμοποιούμε αλλά εάν και κατά πόσο ένας οργανισμός σκοπεύει ή χρησιμοποιεί ήδη ένα δημόσιο, ιδιωτικό ή υβριδικό cloud.Παρόλο που μερικά IaaS cloud παρέχουν εικονικές ζώνες δικτύου, μπορεί να μην ταιριάζουν με το εσωτερικό ιδιωτικό περιβάλλον cloud που πραγματοποιεί stateful packet inspection (SPI) στο Firewall και άλλες τεχνικές ασφάλειας δικτύου.

Εάν ο οργανισμός είναι αρκετά μεγάλος ώστε να έχει τους πόρους για ένα ιδιωτικό cloud , οι κίνδυνοι μειώνονται θεωρώντας ότι έχει ένα πραγματικό ιδιωτικό cloud που βρίσκεται εσωτερικά του δικτύου του. Σε μερικές περιπτώσεις , ένα ιδιωτικό cloud βρίσκεται στις εγκαταστάσεις ενός παρόχου cloud μπορεί να ανταποκριθεί στις απαιτήσεις ασφάλειας του οργανισμού αλλά εξαρτάται από τις δυνατότητες και την ωριμότητα του παρόχου.

Οι κίνδυνοι της εμπιστευτικότητας μπορούν να μειωθούν με την χρήση της κρυπτογράφησης, ειδικά με την χρήση ισχυρών εφαρμογών κρυπτογράφησης για την εισερχόμενη κίνηση δεδομένων. Οι ψηφιακές υπογραφές καθιστούν πολύ πιο

δύσκολο ως ακατόρθωτο για κάποιον να “σκαλίζει” τα δεδομένα και διασφαλίζει την ακεραιότητα των δεδομένων.

Τα προβλήματα της διαθεσιμότητας στο επίπεδο δικτύου είναι ακόμα πιο δύσκολο να αμβλυνθούν με το cloud computing εκτός και αν ο οργανισμός χρησιμοποιεί ένα ιδιωτικό cloud το οποίο βρίσκεται εσωτερικά της τοπολογίας του δικτύου του.

3.2 Επίπεδο Host Ασφάλεια σε SaaS και PaaS

Γενικά οι πάροχοι cloud δεν μοιράζονται δημοσίως πληροφορίες που σχετίζονται με τις πλατφόρμες φιλοξενίας, τα λειτουργικά συστήματα των σταθμών φιλοξενίας, και τις διαδικασίες που λαμβάνουν μέρος για την ασφάλεια των σταθμών, καθώς οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες όταν προσπαθούν να εισέλθουν σε υπηρεσίες του cloud. Συνεπώς στο SaaS (π.χ Salesforce.com, Workday.com) ή στο PaaS (π.χ Google App Engine , Salesforce.com’s Force.com) η ασφάλεια της φιλοξενίας είναι αδιαφανής στους πελάτες και η ευθύνη της ασφάλειας των σταθμών φιλοξενίας εκχωρείται στους παρόχους. Ο πάροχος εγγυάται την ασφάλεια των σταθμών και παρέχει πληροφορίες που σχετίζονται με την ασφάλεια μέσω της υπογραφής μια συμφωνίας μη κοινοποίησης (non-disclosure agreement NDA) ή μέσω ενός πλαισίου εκτίμησης ελέγχου όπως το SysTrust ή το ISO 27002.Επίσης διασφαλίζει ότι κατάλληλοι αποτρεπτικοί και ανιχνευτικοί έλεγχοι λαμβάνουν μέρος και να το πιστοποιεί μέσω μιας τρίτης έμπιστης αρχής ή με το ISO 27002.

Τόσο η πλατφόρμα PaaS όσο και η SaaS αφαιρούν και κρύβουν τις πληροφορίες του λειτουργικού συστήματος του σταθμού φιλοξενίας από τους χρήστες, μέσω ενός επιπέδου αφαιρετικότητας. Μια χαρακτηριστική διαφορά του PaaS και του SaaS είναι η προσβασιμότητα σε αυτό το επίπεδο αφαιρετικότητας που κρύβει τις υπηρεσίες του λειτουργικού συστήματος που οι εφαρμογές χρησιμοποιούν. Στην περίπτωση του SaaS, το επίπεδο αφαιρετικότητας δεν είναι ορατό στους χρήστες και είναι ορατό μόνο στους προγραμματιστές και στο προσωπικό του παρόχου. Στην περίπτωση το PaaS δίνεται έμμεση πρόσβαση στους χρήστες στο επίπεδο αφαιρετικότητας του σταθμού φιλοξενίας μεσω της διεπαφής προγραμματισμού εφαρμογών (API) το οποίο αλληλεπιδρά με το επίπεδο αφαιρετικότητας.

Συνοψίζοντας οι ευθύνες για την στις υπηρεσίες SaaS και PaaS μεταφέρονται στον πάροχο. Το γεγονός ότι ο πελάτης δεν χρειάζεται να ασχολείται με το να προστατεύει τους σταθμούς από τις διάφορες απειλές είναι ένα πρωτεύων προνόμιο από την άποψη της διαχείρισης και του κόστους της ασφάλειας. Ωστόσο ο πελάτης ακόμα κατέχει την ευθύνη της διαχείρισης των πληροφοριών που φιλοξενούνται στις υπηρεσίες cloud , είναι δική του ευθύνη να κατέχει το κατάλληλο επίπεδο εγγύησης σε σχέση με το πώς ο πάροχος διασφαλίζει την ασφάλεια.

3.2.1 Ασφάλεια σταθμών φιλοξενίας IaaS

Σε αντίθεση με το PaaS και το SaaS, οι πελάτες του IaaS είναι υπεύθυνοι για την ασφάλεια των σταθμών που τους παρέχονται στο cloud. Δεδομένου ότι όλες οι υπηρεσίες IaaS που είναι διαθέσιμες σήμερα χρησιμοποιούν τεχνολογίες εικονικότητας στο επίπεδο των σταθμών , η ασφάλεια στο IaaS διακρίνεται ως εξής :

Ασφάλεια εικονικότητας λογισμικού

Το επίπεδο λογισμικού παρέχει στους πελάτες την δυνατότητα να δημιουργούν και να καταστρέφουν εικονικά στιγμιότυπα. Η εικονικότητα στο επίπεδο των σταθμών πραγματοποιείται χρησιμοποιώντας οποιαδήποτε αρχιτεκτονική εικονικότητας συμπεριλαμβανομένου της εικονικότητας σε επίπεδο λειτουργικού συστήματος (Solaris containers, BSD jails, Linux –VServer), παραεικονικότητας (ένας συνδυασμός υλικού με το Xen και το VMware) ή εικονικότητα βασισμένη στο υλικό (Xen, VMware, Hyper-V). Είναι σημαντικό να υπάρχει ασφάλεια σε αυτό το επίπεδο λογισμικού που υπάρχει μεταξύ του υλικού και των εικονικών εξυπηρετητών. Στο δημόσιο IaaS οι πελάτες δεν έχουν πρόσβαση σε αυτό το επίπεδο λογισμικού και η διαχείριση γίνεται αποκλειστικά από τον πάροχο.

Ασφάλεια εικονικού εξυπηρετητή

Το εικονικό στιγμιότυπο ενός λειτουργικού συστήματος που παρέχεται στην κορυφή του επιπέδου εικονικότητας και είναι ορατό στους πελάτες μέσω του ιντερνετ π.χ Linux, Microsoft, Solaris. Οι πελάτες έχουν πλήρη πρόσβαση στους εικονικούς εξυπηρετητές.

3.2.2 Ασφάλεια λογισμικού εικονικότητας

Καθώς ο πάροχος διαχειρίζεται το λογισμικό εικονικότητας, οι πελάτες δεν μπορούν ούτε να δουν ούτε να προσπελάσουν αυτό το λογισμικό. Η εικονικότητα μέσω υλικού ή λογισμικού επιτρέπει το μοίρασμα του υλικού μεταξύ πολλαπλών φιλοξενούμενων εικονικών μηχανών χωρίς να παρεμβαίνει η μία στην άλλη, έτσι ώστε να τρέχουν με ασφάλεια διάφορα λειτουργικά συστήματα και εφαρμογές την ίδια στιγμή σε έναν απλό υπολογιστή. Το σύνηθες στο IaaS είναι να χρησιμοποιείται τεχνολογία επόπτη τύπου 1 γνωστό και ως “bare metal ή native

hypervisor" ο οποίος τρέχει απευθείας πάνω στο υλικό και διαχειρίζεται τα εικονικά λειτουργικά που βρίσκονται ένα επίπεδό πάνω από αυτόν και μόλις στο δεύτερο επίπεδο πάνω από το υλικό. Μερικοί τέτοιοι επόπτες είναι : VMware ESX, Xen, Oracle VM, και Microsoft Hyper-V και υποστηρίζουν πληθώρα λειτουργικών συστημάτων συμπεριλαμβανομένων των Microsoft Windows, διάφορες διανομές Linux και το OpenSolaris της Sun.

Δεδομένου ότι ο επόπτης εικονικότητας είναι το βασικό συστατικό που εγγυάται την διαίρεση σε κατηγορίες και την απομόνωση των πελατών που χρησιμοποιούν τις εικονικές μηχανές του ενός από τον άλλον σε ένα πολύχρηστικό περιβάλλον , είναι πολύ σημαντικό να προστατεύεται ο επόπτης από μη εξουσιοδοτημένους χρήστες. Από τότε που η εικονικότητα έγινε πολύ σημαντική στην αρχιτεκτονική του IaaS cloud, κάθε επίθεση που μπορεί να διαταράξει την ακεραιότητα των κατηγοριών μπορεί να είναι καταστροφική για όλη την βάση των πελατών σε αυτό το cloud. Παράδειγμα επίθεσης στον επόπτη είναι η "zero-day" επίθεση που δέχθηκε εταιρία Vaserv.com σε μια εφαρμογή εικονικότητας κατασκευασμένη από την εταιρία Lxlabs. Οι επιτιθέμενοι απέκτησαν την δυνατότητα εκτέλεσης σημαντικών εντολών Unix όπως ή "rm – rf". Αποτέλεσμα αυτής της επίθεσης ήταν η καταστροφή πάνω από 100,000 ιστοσελίδων που φιλοξενούσε η Vaserv.com όπου το περίπου 50% των χρηστών της είχε συμβόλαια που δεν προέβλεπαν την λήψη αντιγράφων ασφαλείας.

Ο πάροχος θα πρέπει να θεσπίσει τους απαραίτητους ελέγχους ασφάλειας περιορίζοντας την φυσική και την λογική πρόσβαση στον επόπτη και στις άλλες μορφές των επιπέδων εικονικότητας. Οι πελάτες θα πρέπει να κατανοήσουν την τεχνολογία και τις διεργασίες ασφάλειας που θεσπίζει ο πάροχος για να προστατεύσει τον επόπτη. Αυτό βοηθάει ώστε ο πελάτης να αντιληφθεί την συμμόρφωση και τα κενά του παρόχου σε σχέση με τα δικά του στάνταρ ασφάλειας και την πολιτική που ακολουθεί.

3.2.3 Ασφάλεια εικονικού εξυπηρετητή

Οι πελάτες του IaaS έχουν πλήρη πρόσβαση στις εικονικές μηχανές που φιλοξενούνται και απομονώνονται η μια από την άλλη με την χρήση τεχνολογίας επόπτη. Συνεπώς οι πελάτες είναι υπεύθυνοι για την διαχείριση και την ασφάλεια των εικονικών μηχανών.

Ένα δημόσιο IaaS όπως το Amazon Elastic Compute Cloud (EC2) παρέχει μια διεπαφή προγραμματισμού εφαρμογών για να εκτελούνται λειτουργίες διαχείρισης

όπως παροχή, παροπλισμός και εξακρίβωση εικονικών εξυπηρετητών στην πλατφόρμα IaaS. Αυτές οι λειτουργίες διαχείρισης συστήματος όταν οργανωθούν κατάλληλα μπορούν να παρέχουν ελαστικότητα στους πόρους ώστε να αυξάνονται ή να μειώνονται σε συνάρτηση με τον φόρτο εργασίας. Ο δυναμικός κύκλος ζωής των εικονικών εξυπηρετητών μπορεί να αυξήσει την πολυπλοκότητα αν η διεργασίες για την διαχείριση των εικονικών εξυπηρετητών δεν είναι αυτοματοποιημένη με κατάλληλες διεργασίες. Οι εικονικοί εξυπηρετητές μπορεί να είναι προσβάσιμοι στον καθένα στο ιντερνετ, γι'αυτό πρέπει να λαμβάνονται επαρκή μέτρα για τον περιορισμό της πρόσβασης στα εικονικά στιγμιότυπα. Τυπικά ο πάροχος κλείνει όλες τις πόρτες πρόσβασης στις εικονικές μηχανές, και προτρέπει τους πελάτες να χρησιμοποιούν την πόρτα 22 (Secure Shell- SSH) για την διαχείριση των εικονικών στιγμιότυπων. Η διεπαφή προγραμματισμού για τον έλεγχο του cloud προσθέτει ακόμα ένα αναδυόμενο επίπεδο επιθέσεων και πρέπει να προστεθεί στον στόχο της ασφάλειας των εικονικών εξυπηρετητών στο δημόσιο cloud. Μερικές από τις νέες απειλές ασφάλειας στο δημόσιο IaaS είναι (Mather κ.α., 2009) :

- Κλοπή κλειδιών που χρησιμοποιούνται για την πρόσβαση και διαχείριση των σταθμών (π.χ ιδιωτικά κλειδιά SSH)
- Επίθεση σε ευάλωτες μη διορθωμένες υπηρεσίες που ανταποκρίνονται σε συγκεκριμένες πόρτες (π.χ FTP, NetBios , SSH)
- Κλοπή λογαριασμών που δεν ασφαλίζονται κατάλληλα (π.χ αδύναμοι ή ανύπαρκτοι κωδικοί για συγκεκριμένους λογαριασμούς.)
- Επίθεση σε συστήματα που δεν είναι επαρκώς προστατευμένα με τοίχους προστασίας
- Ανάπτυξη Trojan που ενσωματώνονται στο λογισμικό της εικονικής μηχανής ή στο λειτουργικό σύστημα που φιλοξενεί την εικονική μηχανή

3.2.4 Ασφαλίζοντας τους εικονικούς εξυπηρετητές

Η απλότητα με την οποία οι πελάτες αυτό-προμηθεύονται με νέους εικονικούς εξυπηρετητές στην πλατφόρμα IaaS, δημιουργεί έναν νέο παράγοντα ρίσκου , αυτόν της ενδεχόμενης δημιουργίας μη ασφαλών εξυπηρετητών. Η ασφάλεια με

την εξορισμού διαμόρφωση χρειάζεται να εξασφαλιστεί ακολουθώντας ή και υπερβαίνοντας της βασικές γραμμές της βιομηχανίας.

Ασφαλίζοντας τους εικονικούς εξυπηρετητές στο cloud απαιτούνται ισχυρές λειτουργικές διεργασίες σε συνδυασμό με την αυτοματοποίηση των διεργασιών. Μερικές συστάσεις είναι :

- Χρήση μιας εξορισμού ασφαλούς διαμόρφωσης. Χρήση μιας πιο περιορισμένης εικόνας για την δημιουργία εικονικών μηχανών στο δημόσιο cloud. Μια καλή πρακτική για εφαρμογές που λειτουργούν στο cloud είναι να δημιουργείται μια συνηθισμένη εικόνα για την αρχικοποίηση εικονικών μηχανών που να έχει μόνο τις δυνατότητες και τις υπηρεσίες που είναι απαραίτητες για την υποστήριξη της στοίβας εφαρμογών. Περιορίζοντας τις δυνατότητες μόνο στο επίπεδο της στοίβας εφαρμογών, περιορίζεται όχι μόνο το εύρος των επιθέσεων αλλά και το πλήθος των απαραίτητων διορθώσεων που χρειάζονται για να διατηρηθεί η στοίβα ασφαλής.
- Λεπτομερή παρακολούθηση των εικόνων των εικονικών μηχανών που προετοιμάζονται για την φιλοξενία cloud. Ο πάροχος IaaS παρέχει μερικές από αυτές τις εικόνες. Όταν χρησιμοποιείται μια εικονική μηχανή του πάροχου IaaS θα πρέπει να υφίσταται το ίδιο επίπεδο επαλήθευσης της ασφάλειας όπως συμβαίνει με τους σταθμούς μέσα στην επιχείρηση. Η καλύτερη εναλλακτική είναι να παρέχει η επιχείρηση την δικιά της εικόνα που να συμμορφώνεται με τα δικά της στάνταρ ασφάλειας όπως οι εσωτερικοί έμπιστοι σταθμοί.
- Προστασία της ακεραιότητας της εικόνας από μη εξουσιοδοτημένη πρόσβαση.
- Διασφάλιση των ιδιωτικών κλειδιών που απαιτούνται για την πρόσβαση των σταθμών στο δημόσιο cloud.
- Απομόνωση των κλειδιών αποκρυπτογράφησης από το cloud που φυλάσσονται τα δεδομένα εκτός και αν είναι απαραίτητα για την κρυπτογράφηση, και αν ναι μόνο για την διάρκεια της διαδικασίας κρυπτογράφησης.

- Να μην συμπεριλαμβάνονται πιστοποιητικά αυθεντικοποίησης στις εικόνες των εικονικών μηχανών εκτός από ένα κλειδί για την αποκρυπτογράφηση του κλειδιού του αρχείου συστήματος.
- Να μην επιτρέπεται πρόσβαση στο shell με βάση τον κωδικό πρόσβασης.
- Να απαιτείται κωδικός για την εκτέλεση εντολών όπως η sudo.
- Ύπαρξη τοίχους προστασίας και άνοιγμα μόνο των απαραίτητων πορτών ώστε να λειτουργούν οι υπηρεσίες του σταθμού.
- Ενεργοποίηση μόνο των απαραίτητων υπηρεσιών και απενεργοποίηση όλων των άλλων μη χρησιμοποιούμενων (π.χ απενεργοποίηση του FTP, υπηρεσίες εκτυπωτή, βάσεων δεδομένων κ.α όταν δεν χρειάζονται).
- Εγκατάσταση ενός IDS συστήματος όπως το OSSEC ή το Samhain.
- Ενεργοποίηση του ελέγχου συστήματος και αρχειοθέτησης των σημαντικών γεγονότων. Αποθήκευση του ιστορικού των γεγονότων ασφάλειας σε έναν αφιερωμένο εξυπηρετητή καταγραφής ιστορικού και απομόνωση του εξυπηρετητή αυτού με υψηλότερη προστασία ασφάλειας συμπεριλαμβανομένου και του ελέγχου πρόσβασης.
- Αν υπάρχει υποψία ότι το στιγμιότυπο εκτέθηκε σε κίνδυνο τότε το τερματίζουμε, κρατάμε ένα αποτύπωμα , παίρνουμε αντίγραφο ασφαλείας του φακέλου root και αργότερα μπορούμε να διερευνήσουμε τι συνέβη.
- Καθιέρωση μιας διαδικασίας για την εγκατάσταση διορθώσεων τόσο σε ανενεργές όσο και σε τρέχουσες εικόνες.
- Περιοδικός έλεγχος του αρχείου ιστορικού για ύποπτες δραστηριότητες.

3.3 Ασφάλεια Υποδομής: Επίπεδο Εφαρμογών

Η ασφάλεια των εφαρμογών πρέπει να είναι ένα σημαντικό στοιχείο του προγράμματος ασφάλειας. Ο σχεδιασμός και η ανάπτυξη εφαρμογών στην πλατφόρμα του cloud απαιτεί από τα υπάρχοντα προγράμματα ασφάλειας εφαρμογών να επανεκτιμήσουν τις υπάρχουσες πρακτικές και τα στάνταρ. Το εύρος της ασφάλειας εφαρμογών ποικίλει από αυτόνομες ενός χρήστη εφαρμογές

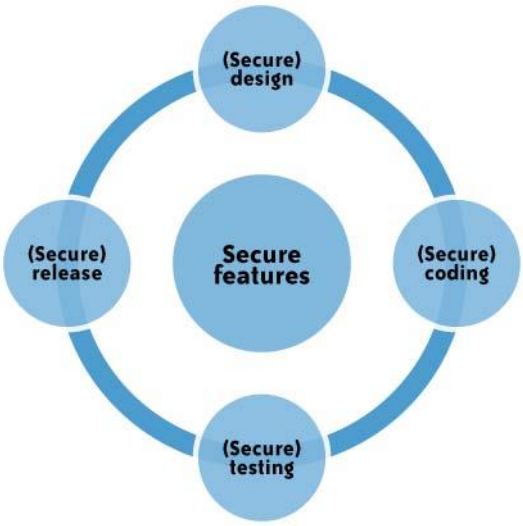
ως τις πιο εξεζητημένες πολλαπλών χρηστών ηλεκτρονικού εμπορίου εφαρμογές που χρησιμοποιούνται από χιλιάδες χρήστες. Web εφαρμογές όπως τα CMSs, Wiki, πόρταλ, bulletin board, φόρουμ συζητήσεων, χρησιμοποιούνται από μικρές και μεγάλες επιχειρήσεις. Ένας μεγάλος αριθμός επιχειρήσεων αναπτύσσει επίσης δικές του εφαρμογές web χρησιμοποιώντας διάφορα πλαίσια εργασίας όπως (PHP, .NET, J2EE, Python κ.α). Σύμφωνα με το SANS μέχρι το 2007 λίγες ήταν οι επιθέσεις σε ευπαθείς ιστοσελίδες καθώς δεν υπήρχε ιδιαίτερο κέρδος για τους επιτιθέμενους,. Ωστόσο με αυξανόμενο ρυθμό επιθέσεις όπως το “cross site scripting – XSS) και άλλες εμφανίζονται καθώς οι επιτιθέμενοι αποσκοπούν σε χρηματοοικονομικά κέρδη εκμεταλλευόμενοι κενά και λάθη στον διαδικτυακό προγραμματισμό βρίσκοντας έτσι έναν νέο τρόπο να διαπερνούν σημαντικούς οργανισμούς. Από τότε που ο φυλλομετρητής έγινε ο client του τελικού χρήστη για την πρόσβαση cloud εφαρμογών είναι σημαντικό για το πρόγραμμα ασφάλειας εφαρμογών να περιλαμβάνει και την ασφάλεια του φυλλομετρητή στον σκοπό της. Αυτός ο συνδυασμός καθορίζει την δύναμη της από άκρο σε άκρο ασφάλειας στο cloud που βοηθάει στην προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που χρησιμοποιούνται από υπηρεσίες του cloud.

3.3.1 Επίπεδο Εφαρμογών – Απειλές Ασφάλειας

Σύμφωνα με το SANS οι ευπάθειες των διαδικτυακών εφαρμογών τόσο με ανοιχτό όσο και κλειστό λογισμικό έφτασαν στο 50% των συνολικών ευπαθειών που μετρήθηκαν μεταξύ Νοεμβρίου 2006 και Οκτωβρίου 2007 (http://sans.org/top-cyber-security-risks/?ref=top20). Οι υπάρχουσες απειλές εκμεταλλεύονται γνωστές ευπάθειες των εφαρμογών (π.χ η λίστα με τις 10 σημαντικότερες απειλές της OWASP, http://www/owasp.org/index.php/Top_10_2010) συμπεριλαμβανομένων των cross site scripting XSS, SQL injection, εκτέλεση κακόβουλων αρχείων, και άλλες ευπάθειες που οφείλονται σε προγραμματιστικά λάθη και ελαττώματα στην σχεδίαση. Εξοπλισμένοι με γνώση και εργαλεία οι επιτιθέμενοι σαρώνουν διαδικτυακές εφαρμογές για να ανιχνεύσουν ευπάθειες . Έπειτα εκμεταλλεύονται αυτές τις ευπάθειες για διάφορες παράνομες πράξεις όπως χρηματοοικονομικές απάτες, πνευματικές κλοπές, μετατροπή ιστοσελίδων σε κακόβουλους εξυπηρετητές και απάτη με την τεχνική του phishing.

Είναι κοινή πρακτική να χρησιμοποιείται ένας συνδυασμός περιμετρικών ελέγχων ασφάλειας και ελέγχου πρόσβασης με βάση το δίκτυο και τους σταθμούς για να προστατευτούν οι διαδικτυακές εφαρμογές που αναπτύσσονται σε ένα σφιχτό περιβάλλον έλεγχου, συμπεριλαμβανομένων εταιρικών intranet, και ιδιωτικών cloud, από τους επιτιθέμενοι. Οι διαδικτυακές εφαρμογές που αναπτύσσονται στο δημόσιο cloud εκτίθενται σε μεγαλύτερο επίπεδο απειλής, σε επιθέσεις και δυνητικά εκμεταλλεύονται από επιτιθέμενους για να υποστηρίξουν δόλιες και παράνομες δραστηριότητες. Σε αυτό το μοντέλο απειλών οι διαδικτυακές εφαρμογές που αναπτύσσονται στο δημόσιο cloud πρέπει να σχεδιαστούν για το μοντέλο απειλών του internet και η ασφάλεια πρέπει να ενσωματωθεί στο κύκλο ανάπτυξης και ζωής του λογισμικού .

Εικόνα 3.2 Κύκλος ζωής ανάπτυξης λογισμικού

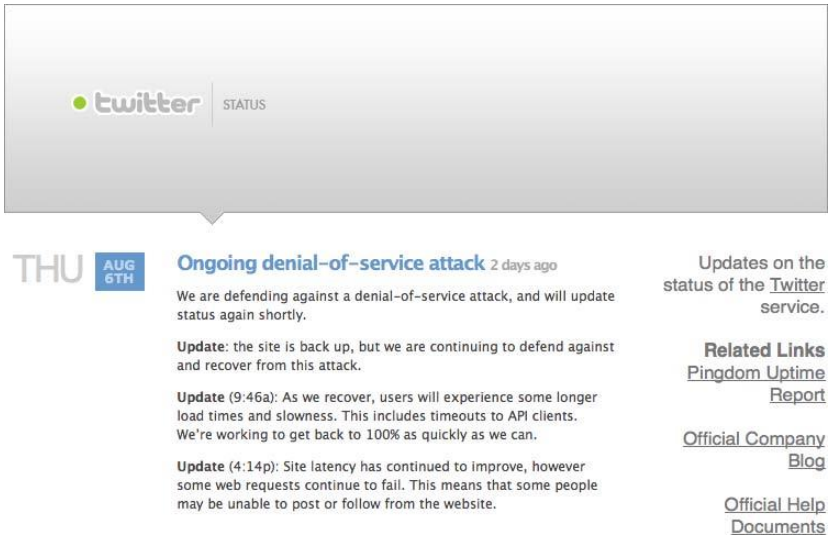


3.3.2 Επιθέσεις τύπου DoS και EDoS

Οι επιθέσεις στο επίπεδο εφαρμογών τύπου DoS και DDoS μπορούν να διαταράξουν τις υπηρεσίες του cloud για εκτεταμένο χρονικό διάστημα. Αυτές οι επιθέσεις συνήθως προέρχονται από μολυσμένους υπολογιστές που είναι συνδεδεμένοι στο internet(οι επιτιθέμενοι ελέγχουν υπολογιστές που έχουν μολυνθεί από ιούς, σκουλήκια και δούρειους ίππους και σε μερικές περιπτώσεις ισχυρούς απροστάτευτους εξυπηρετητές). Οι επιθέσεις τύπου DoS εκδηλώνονται ως μεγάλος όγκος ανανεώσεων ιστοσελίδων, XML αιτήματα (μέσω HTTP ή HTTPS, ή αιτήματα συγκεκριμένου πρωτοκόλλου που υποστηρίζεται από κάποια υπηρεσία του cloud. Επειδή αυτή η παράνομη κίνηση αναμιγνύεται με την νόμιμη κίνηση είναι πολύ δύσκολο να φιλτραριστεί επιλεκτικά χωρίς να επηρεαστεί η

υπηρεσία ως σύνολο. Για παράδειγμα μια επίθεση τύπου DDoS στο Twitter στις 6 Αυγούστου του 2009 κατέστησε την υπηρεσία μη διαθέσιμη για αρκετές ώρες.(βλέπε εικόνα 3.3)(http://blog.twitter.com/2009/08/denial-of-service-attack.html)

Εικόνα 3.3 Επίθεση DDoS στο Twitter



Εκτός από την διατάραξη των υπηρεσιών του cloud οι επιθέσεις τύπου DoS μπορούν να επηρεάσουν και τον προϋπολογισμό μιας εταιρείας που χρησιμοποιεί το cloud. Οι επιθέσεις DoS σε ένα περιβάλλον χρέωσης ανάλογα με την χρήση έχουν ως αποτέλεσμα την δραματική αύξηση του λογαριασμού, καθώς αυξάνεται η κίνηση του δικτύου, ο φόρτος της CPU, και η κατανάλωση αποθηκευτικού χώρου. Αυτός ο τύπος επίθεσης χαρακτηρίζεται επίσης και ως EDoS (economic denial of sustainability).

Ίσως στο όχι και τόσο μακρινό μέλλον να δούμε τους επιτιθέμενους να εκμεταλλεύονται κλεμμένους λογαριασμούς πελατών του cloud για να εξαπολύουν επιθέσεις εκμεταλλευόμενοι τον συνδυασμό διαφορετικών υπολογιστικών πόρων στο cloud, πετυχαίνοντας έτσι μεγάλη υπολογιστική ισχύ χωρίς το κόστος της υποδομής. Ενδεχομένως να υπάρξουν και επιθέσεις DoS από το IaaS ή PaaS cloud εναντίων άλλων cloud κάτι που χαρακτηρίζεται ως “dark cloud”.

3.3.3 Ασφάλεια Τελικού Χρήστη

Ο πελάτης του cloud φέρει την ευθύνη για την ασφάλεια του τελικού χρήστη και της ασφάλεια του υπολογιστή με τον οποίο συνδέεται στο ιντερνέτ. Τα μέτρα προστασίας περιλαμβάνουν την χρήση λογισμικού ασφαλείας όπως anti-malware,

antivirus, τοίχο προστασίας, εγκατάσταση ενημερώσεων, και λογισμικό εντοπισμού και πρόληψης παράνομων εισβολών. Η νέα φιλοσοφία είναι ότι ο browser είναι το λειτουργικό σύστημα μέσω του οποίου απολαμβάνουμε τις υπηρεσίες του cloud. Όλοι οι browser υποφέρουν από ευπάθειες που τους καθιστούν ευάλωτους σε επιθέσεις. Γιαυτό θα πρέπει οι χρήστες προκειμένου να διατηρούν την από άκρο σε άκρο ασφάλεια να αναβαθμίζουν τον browser (π.χ Internet Explorer, Firefox, Safari, Opera) τους τακτικά, και να εγκαθιστούν όλες τις ενημερώσεις ασφάλειας ώστε να διατρέχουν τον μικρότερο δυνατό κίνδυνο.

3.3.4 Ευθύνη ασφάλειας διαδικτυακών εφαρμογών στο cloud

Ανάλογα με το μοντέλο διανομής του cloud (SPI) και το επίπεδο της συμφωνίας της υπηρεσίας (SLA) η εύθηνη της ασφάλειας πέφτει τόσο στους ώμους του πελάτη όσο και του παρόχου. Το κλειδί είναι να γίνει κατανοητό ποιες από τις ευθύνες ασφάλειας του πελάτη είναι αντίθετες με αυτές του παρόχου. Σε αυτό το πλαίσιο πρόσφατες μελέτες δείχνουν ότι η έλλειψη διαφάνειας στο θέμα της ασφάλειας και στις πρακτικές που ακολουθούνται από μεριά του παρόχου αποτελούν εμπόδιο στην υιοθέτηση του cloud.

Οι πελάτες του cloud δεν έχουν την διαφάνεια που χρειάζεται στο θέμα των ευπαθειών του λογισμικού στις υπηρεσίες του cloud. Αυτό αποτρέπει τους πελάτες από το να διαχειριστούν τον λειτουργικό κίνδυνο που απορρέει από αυτές τις ευπάθειες. Επιπλέον οι πάροχοι αντιμετωπίζοντας το λειτουργικό ως ιδιοκτησία τους, εμποδίζουν τους ερευνητές ασφάλειας να αναλύσουν το λογισμικό για κενά ασφάλειας και σφάλματα. Εξαίρεση αποτελούν οι πάροχοι που χρησιμοποιούν λογισμικό ανοιχτού κώδικα. Έτσι οι πελάτες εξαιτίας της αδιαφάνειας αυτής, μένουν με μόνη επιλογή να εμπιστευτούν τον πάροχο και ότι αυτός θα αναλάβει να ανακαλύψει νέες ευπάθειες που μπορεί να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα ή την διαθεσιμότητα των εφαρμογών τους.

3.3.5 Ασφάλεια Εφαρμογών SaaS

Το μοντέλο διανομής του SaaS υπαγορεύει ότι ο πάροχος διαχειρίζεται ολόκληρη την σουίτα των εφαρμογών που παρέχεται στους χρήστες. Επομένως ο πάροχος φέρει και την ευθύνη να ασφαλίσει τις εφαρμογές που προσφέρει τους πελάτες. Οι πελάτες είναι συνήθως υπεύθυνοι για λειτουργίες ασφάλειας στην διαχείριση των χρηστών και της πρόσβασης όπως αυτό υποστηρίζεται από τον πάροχο. Είναι κοινή πρακτική για μελλοντικούς πελάτες να ζητούν πληροφορίες που σχετίζονται

με τις πρακτικές ασφάλειας του παρόχου, με την υπογραφή μια σύμβασης μη κοινοποίησης (NDA). Αυτές οι πληροφορίες πρέπει να περιλαμβάνουν το σχέδιο, την αρχιτεκτονική, την ανάπτυξη, δοκιμές ασφάλειας των εφαρμογών, και την διαχείριση της κυκλοφορίας των εκδόσεων.

Ιδιαίτερη προσοχή χρειάζεται να δοθεί στα χαρακτηριστικά της αυθεντικοποίησης και του έλεγχο πρόσβασης που προσφέρονται από τον πάροχο του SaaS. Συνήθως αυτός είναι ο μόνος διαθέσιμος έλεγχος ασφάλειας για την διαχείριση του κινδύνου των πληροφοριών. Οι περισσότερες υπηρεσίες όπως το Salesforce.com και η Google προσφέρουν μια διαδικτυακή διεπαφή διαχείρισης της αυθεντικοποίησης και του ελέγχου πρόσβασης της εφαρμογής. Μερικές εφαρμογές SaaS όπως η Google Apps έχουν ενσωματωμένα χαρακτηριστικά με τα οποία οι τελικοί χρήστες μπορούν να αναθέσουν δικαιώματα ανάγνωσης και εγγραφής σε άλλους χρήστες. Ωστόσο η διαχείριση προνομίων μπορεί να μην είναι τόσο εξελιγμένη και μπορεί να έχει αδυναμίες που να μην συμβαδίζουν με τα στάνταρ της ασφάλειας ελέγχου πρόσβασης του οργανισμού. Ένα παράδειγμα για αυτό το πρόβλημα είναι ο μηχανισμός που υλοποιεί το Google Docs για να διαχειρίζεται τις φωτογραφίες που ενσωματώνονται σε έγγραφα, όπως επίσης και τα προνόμια πρόσβασης σε παλιότερες εκδόσεις ενός εγγράφου. Αποδεδειγμένα οι ενσωματωμένες εικόνες που αποθηκεύονται στο Google Docs δεν προστατεύονται με τον ίδιο τρόπο όπως προστατεύεται ένα έγγραφο με ελέγχους διαμοιρασμού. Αυτό σημαίνει πώς αν κάποιος μοιράζει ένα έγγραφο που περιέχει ενσωματωμένες φωτογραφίες ένα άλλο πρόσωπο θα είναι σε θέση να βλέπει αυτές τις φωτογραφίες ακόμα και μετά από την διακοπή μοιράσματος του αρχείου αυτού.

Ακόμα ένα περιστατικό που σχετίζεται με το Google Docs είναι μια δυσλειτουργία στην ιδιωτικότητα. Σε ένα μικρό κομμάτι (η Google ισχυρίζεται ότι το 0,05% των εγγράφων επηρεάστηκε) εγγράφων κειμένου και παρουσιάσεων που αποθηκεύονται στο Google Apps cloud μοιράστηκε η πρόσβαση σε ακατάλληλους χρήστες. Παρόλο που τα έγγραφα αυτά μοιράστηκαν μόνο σε χρήστες που ήδη μοιράζονταν αρχεία μεταξύ τους το πρόβλημα αυτό δείχνει την ανάγκη να εκτιμηθεί και να κατανοηθεί ο μηχανισμός ελέγχου πρόσβασης στο cloud (http://www.techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/).

Οι πελάτες του cloud θα πρέπει να κατανοήσουν τον μηχανισμό ελέγχου πρόσβασης στο cloud συμπεριλαμβάνοντας την υποστήριξη για ισχυρή αυθεντικοποίηση και διαχείριση προνομίων βασισμένη σε ρόλους και λειτουργίες, και να λαμβάνουν τα απαραίτητα μέτρα για την προστασία των πληροφοριών που φιλοξενούνται στο cloud. Πρόσθετοι έλεγχοι πρέπει να υλοποιηθούν για την διαχείριση των προνομίων πρόσβασης στο εργαλείο διαχείρισης του SaaS και να επιβληθεί διαχωρισμός των καθηκόντων ώστε να ασφαλίζονται οι εφαρμογές από εσωτερικές απειλές. Σε συνάρτηση με τις πολιτικές ασφάλειας οι πελάτες θα πρέπει να εφαρμόζουν πολιτική ισχυρών κωδικών τέτοια που να αναγκάζει τους χρήστες να επιλέγουν ισχυρούς κωδικούς όταν αυθεντικοποιούνται σε μια εφαρμογή.

Είναι κοινή πρακτική για τους παρόχους SaaS να αναμιγνύουν τα δεδομένα των πελατών τους (δομημένα και αδόμητα) σε μια απλή εικονική βάση δεδομένων και να βασίζονται στην σήμανση των δεδομένων για τον μεταξύ τους διαχωρισμό. Σε αυτό το πολύ-χρηστικό μοντέλο βάσεων δεδομένων όπου η κρυπτογράφηση δεν είναι εφικτή εξαιτίας περιορισμών στην διαχείριση των κλειδιών τα δεδομένα σηματοδοτούνται με έναν μοναδικό προσδιοριστικό για κάθε πελάτη. Είναι πιθανό ότι το επίπεδο εφαρμογής που υλοποιεί αυτόν τον διαχωρισμό να παρουσιάσει ευπάθειες καθώς ο πάροχος αναβαθμίζει το λογισμικό αυτό. Έτσι οι πελάτες θα πρέπει να κατανοήσουν την αρχιτεκτονική της εικονικής βάσης αποθήκευσης και τον μηχανισμών που παρέχει ο πάροχος το SaaS για να εγγυηθεί τον διαχωρισμό που απαιτείται σε ένα εικονικό πολύ-χρηστικό περιβάλλον.

3.3.6 Ασφάλεια εφαρμογών PaaS

Οι πωλητές PaaS παγκοσμίως χωρίζονται σε δύο κύριες κατηγορίες:

- Πωλητές λογισμικού (π.χ Bungee, Etelos, GigaSpaces, Eucalyptus)
- Παρόχους cloud(π.χ Google App Engine, Salesforce.com Force.com, Microsoft Azure, IntuitQuickBase)

Εξ ορισμού ένα PaaS cloud προσφέρει ένα ενιαίο περιβάλλον για σχεδίαση, ανάπτυξη, δοκιμή , και υποστήριξη “custom” εφαρμογών αναπτυγμένων στην γλώσσα που υποστηρίζει η πλατφόρμα. Η ασφάλεια εφαρμογών PaaS περιλαμβάνει δύο επίπεδα λογισμικού:

- Ασφάλεια της ίδιας την πλατφόρμας (π.χ μηχανή χρόνου εκτέλεσης - runtime engine)
- Ασφάλεια των εφαρμογών που αναπτύσσουν οι πελάτης στην πλατφόρμα PaaS

Γενικά οι πάροχοι PaaS (π.χ Google, Microsoft, Force.com) είναι υπεύθυνοι για την ασφάλεια της στοίβας λογισμικού της πλατφόρμας που περιλαμβάνει την μηχανή χρόνου εκτέλεσης που τρέχει τις εφαρμογές των πελατών. Εφόσον οι εφαρμογές PaaS μπορεί να χρησιμοποιούν εφαρμογές τρίτων ή συστατικά, ή διαδικτυακές υπηρεσίες, ο τρίτος πάροχος των εφαρμογών αυτών είναι υπεύθυνος να ασφαλίσει αυτές τις υπηρεσίες. Οι πελάτες πρέπει να κατανοούν την εξάρτηση των δικών τους εφαρμογών σε όλες τις υπηρεσίες και να εξακριβώνουν τους κινδύνους που σχετίζονται με τρίτους παρόχους υπηρεσιών. Μέχρι τώρα οι πάροχοι είναι απρόθυμοι να μοιραστούν πληροφορίες που σχετίζονται στην ασφάλεια της πλατφόρμας με το επιχείρημα ότι αυτές μπορεί να χρησιμοποιηθούν από επιτιθέμενους. Ωστόσο οι εταιρικοί πελάτες θα πρέπει να απαιτούν διαφάνεια από τους παρόχους και να ζητούν πληροφορίες απαραίτητες για την εκτέλεση αξιολόγησης κινδύνων και διαχείρισης της ασφάλειας.

Στο πολύ-μησθωτικό μοντέλο διανομής του PaaS , το κεντρικό δόγμα της ασφάλειας είναι η περιστολή και απομόνωση των πολύ-μισθωτικών εφαρμογών της μιας από την άλλη. Σε αυτό το μοντέλο η πρόσβαση στα δεδομένα μιας επιχείρησης πρέπει να περιορίζεται στους χρήστες της εταιρείας και στις εφαρμογές που της ανήκουν και που διαχειρίζεται. Το μοντέλο ασφάλειας της μηχανής χρόνου εκτέλεσης του PaaS είναι ουσιώδες για να επιτευχθεί η αρχιτεκτονική “sandbox” σε ένα πολύ-μισθωτικό υπολογιστικό μοντέλο. Συνεπώς το sandbox είναι χαρακτηριστικό της μηχανής εκτέλεσης χρόνου της πλατφόρμας για να διατηρηθεί η εμπιστευτικότητα και η ακεραιότητα των εφαρμογών που αναπτύσσονται στο PaaS. Οι πάροχοι είναι υπεύθυνοι να εντοπίζουν νέα κενά και ευπάθειες που μπορεί να χρησιμοποιηθούν για να εκμεταλλευτούν την πλατφόρμα PaaS και να σπάσουν την αρχιτεκτονική του sandbox. Αυτό είναι το χειρότερο σενάριο για έναν πάροχο καθώς η απώλεια της ιδιωτικότητας είναι πολύ σημαντική για τις ευαίσθητες πληροφορίες των πελατών και μπορεί να προκαλέσει μεγάλες ζημίες σε μια επιχείρηση. Επομένως οι εταιρικοί πελάτες θα πρέπει να

ζητούν πληροφορίες από τους παρόχους για την αρχιτεκτονική απομόνωσης των υπηρεσιών PaaS.

Η παρακολούθηση της ασφάλειας του δικτύου και των σταθμών έξω από την πλατφόρμα του PaaS είναι επίσης ευθύνη του παρόχου (π.χ παρακολούθηση ενός διαμοιραζόμενου δικτύου και της υποδομής των σταθμών που φιλοξενούν εφαρμογές πελατών).Οι πελάτες του PaaS θα πρέπει να κατανοούν πώς ο πάροχος διαχειρίζεται την πλατφόρμα του π.χ πως αναβαθμίζει ή αλλάζει την μηχανή χρόνου εκτέλεσης, τις εκδόσεις και την εγκατάσταση ενημερώσεων ασφάλειας.

3.3.7 Ασφάλεια Εφαρμογών που αναπτύσσονται από τους Πελάτες

Οι παραγωγοί λογισμικού στο PaaS πρέπει να εξοικειωθούν με συγκεκριμένες διεπαφές προγραμματισμού εφαρμογών για να αναπτύξουν και να διαχειριστούν κομμάτια λογισμικού που ενισχύουν τους ελέγχους ασφάλειας. Επιπλέον δεδομένου ότι αυτές οι διεπαφές είναι μοναδικές για κάθε PaaS cloud, οι παραγωγοί πρέπει να εξοικειώνονται με πλατφορμοκεντρικά χαρακτηριστικά ασφάλειας που είναι διαθέσιμα σε αυτούς με την μορφή αντικειμένων ασφάλειας και διαδικτυακών υπηρεσιών για την διαμόρφωση ελέγχων αυθεντικοποίησης και εξουσιοδότησης μέσα στην εφαρμογή. Στον σχεδιασμό της διεπαφής προγραμματισμού εφαρμογών στο PaaS δεν υπάρχει κανένα στάνταρ, ούτε καν μια προσπάθεια από τους παρόχους να αναπτύξουν μια ενιαία και σύμφωνη από όλους διεπαφή καθιστώντας έτσι πολύ δύσκολη την λειτουργία μας εφαρμογής σε διαφορετικά PaaS. Αυτή την περίοδο το Google App Engine υποστηρίζει μόνο Python και Java, και το Salesforce.com Force.com υποστηρίζει μόνο μια ιδιωτική γλώσσα προγραμματισμού με το όνομα Apex. Η Apex διαφέρει από γλώσσες όπως η C++, Java, .Net και σε αντίθεση με αυτές της γλώσσες είναι περιορισμένος ο σκοπός της στην δημιουργία εμπορικών εφαρμογών στην πλατφόρμα του Force.com. Έτσι οι υπηρεσίες του cloud διατηρούν τους πελάτες τους σε σχέση με το παραδοσιακό λογισμικό. Η έλλειψη στάνταρ στις διεπαφές έχει αντίκτυπο και στην διαχείριση της ασφάλειας και στην μεταφερσιμότητα των εφαρμογών μέσα στο cloud.

Οι παραγωγοί θα πρέπει να αναμένουν από τους παρόχους να τους προσφέρουν ένα σύνολο από χαρακτηριστικά ασφάλειας όπως αυθεντικοποίηση χρήστη, single

sign-on (SSO), κατανεμημένα συστήματα, εξουσιοδότηση (διαχείριση προνομίων), και υποστήριξη SSL και TLS μέσω της διεπαφής. Για την ώρα δεν υπάρχει κανένα στανταρ διαχείρισης ασφάλειας στο PaaS, οι πάροχοι έχουν μοναδικά μοντέλα ασφάλειας, και τα χαρακτηριστικά ασφάλειας διαφέρουν από πάροχο σε πάροχο. Στην περίπτωση του Google App Engine ο παραγωγός που χρησιμοποιεί Python ή Java μπορεί να διαμορφώσει το προφίλ του χρήστη και να επιλέξει το HTTPS ως πρωτόκολλο μεταφοράς. Ομοίως το Force.com προσφέρει μια διεπαφή της Apex για την διαμόρφωση παραμέτρων ασφάλειας ελέγχοντας διάφορες διαμορφώσεις χρόνου εκτέλεσης και καθορίζει συγκεκριμένες πόρτες του TCP για σύνδεση εφαρμογής με εφαρμογή χρησιμοποιώντας αντικείμενα τύπου Apex.

Οι περισσότεροι πάροχοι PaaS περιορίζονται στο να παρέχουν τα βασικά χαρακτηριστικά ασφάλειας όπως διαμόρφωση SSL, βασική διαχείριση προνομίων, και αυθεντικοποίηση χρηστών Σε μερικές μόνο περιπτώσεις υποστηρίζονται τα κατανεμημένα συστήματα με την χρήση προτύπων όπως π.χ της γλώσσας SAML.

3.3.8 Ασφάλεια Εφαρμογών IaaS

Οι πάροχοι IaaS (π.χ Amazon EC2, GoGrid και Joyent) αντιμετωπίζουν τις εφαρμογές των πελατών τους ως μαύρο κουτί και έτσι αγνοούν κάθε λειτουργία διαχείρισης τους. Ολόκληρη η στοίβα –εφαρμογές πελατών, πλατφόρμα χρόνου εκτέλεσης εφαρμογών (Java, .NET, PHP, Ruby on Rails, κτλ.) και ότι άλλο, τρέχουν σε εικονικούς εξυπηρετητές των πελατών που αναπτύσσονται και διαχειρίζονται από τους πελάτες. Σε αυτό το άκρο οι πελάτες έχουν την πλήρη εύθηνη ασφάλισης των εφαρμογών τους που αναπτύσσονται στο IaaS cloud. Επομένως οι πελάτες δεν θα πρέπει να περιμένουν καμιά βοήθεια στην ασφάλιση εφαρμογών από τους παρόχους εκτός από την βασική καθοδήγηση σε χαρακτηριστικά που σχετίζονται με την πολιτική του τοίχου προστασίας που μπορεί να επηρεάζει την επικοινωνία των εφαρμογών με άλλες εφαρμογές, χρήστες ή υπηρεσίες εντός ή εκτός του cloud.

Οι πελάτες είναι υπεύθυνοι να διατηρούν τις εφαρμογές τους και την πλατφόρμα χρόνου εκτέλεσης ενημερωμένη για να προστατεύουν το σύστημα τους από malware και χάκερς που ψάχνουν για ευπάθειες προκειμένου να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του cloud. Προτείνεται να παράγονται εφαρμογές με το χαμηλότερο δυνατόν επίπεδο προνομίων κατά τον χρόνο

εκτέλεσης (π.χ να διαμορφώνεται η εφαρμογή ώστε να τρέχει χρησιμοποιώντας έναν λογαριασμό με χαμηλότερα δικαιώματα).

Οι παραγωγοί που παράγουν εφαρμογές για το IaaS cloud πρέπει να δημιουργούν τα δικά τους χαρακτηριστικά για να χειρίζονται την αυθεντικοποίηση και την εξουσιοδότηση. Σε αντιστοιχία με τις πρακτικές ταυτοποίησης των εταιρειών, οι εφαρμογές στο cloud πρέπει να σχεδιάζονται έτσι ώστε να υποστηρίζουν υπηρεσίες αυθεντικοποίησης από έναν Πάροχο Ταυτοποίησης (π.χ OpenSSO, Oracle IAM, IBM CA) ή από τρίτο πάροχο ταυτοποίησης (π.χ Ping Identity, Simplified, TriCipher). Οι ατομικές υλοποιήσεις αυθεντικοποίησης και ταυτοποίησης μπορεί να οδηγήσουν σε αδύναμους συνδέσμους αν δεν υλοποιηθούν κατάλληλα και γιαυτό συνίσταται να αποφεύγονται όπου είναι δυνατόν.

3.4 Σύνορο Εμπιστοσύνης και Διαχείριση Ταυτοποίησης και Πρόσβασης (IAM- Identity and Access Management)

Στους τυπικούς οργανισμούς όπου οι εφαρμογές αναπτύσσονται μέσα στην περίμετρο του οργανισμού τα όρια εμπιστοσύνης είναι πιο στατικά και ελέγχονται από τον ίδιο τον οργανισμό. Σε αυτό το παραδοσιακό μοντέλο το όριο εμπιστοσύνης περιλαμβάνει το δίκτυο, τα συστήματα, και τις εφαρμογές που φιλοξενούνται σε έναν εικονικό εξυπηρετητή. Επίσης η πρόσβαση στο δίκτυα, τα συστήματα και τις εφαρμογές ασφαλίζεται μέσω ελέγχων ασφάλειας δικτύου όπως : εικονικά ιδιωτικά δίκτυα (VPN) συστήματα εντοπισμού και αποτροπής εισβολών (IDS – IPS) και αυθεντικοποίηση.

Με την υιοθέτηση του cloud computing το σύνορο εμπιστοσύνης του οργανισμού γίνεται δυναμικό και ξεφεύγει από τον έλεγχο του τμήματος τεχνολογίας πληροφορικής του οργανισμού. Με το cloud computing το όριο του δικτύου των συστημάτων και των εφαρμογών του οργανισμού επεκτείνεται στο domain του παρόχου.

Για να αντισταθμίσουν οι οργανισμοί την απώλεια του ελέγχου του δικτύου, στηρίζονται σε ελέγχους του λογισμικού σε υψηλότερο επίπεδο όπως η ασφάλεια των εφαρμογών και έλεγχοι της πρόσβασης των χρηστών. Αυτοί οι έλεγχοι εκδηλώνονται ως ισχυρή αυθεντικοποίηση, εξουσιοδότηση βασισμένοι σε ρόλους, ομοσπονδία ταυτοποίησης, σύστημα ενιαίας πρόσβασης-single sign-on (SSO),

παρακολούθηση των δραστηριοτήτων των χρηστών και έλεγχος. Ιδιαιτέρως οι οργανισμοί πρέπει να δώσουν προσοχή στην αρχιτεκτονική της ομοσπονδία ταυτοποίησης και τις διεργασίες, καθώς μπορεί να ενδυναμώσει τους ελέγχους και την εμπιστοσύνη μεταξύ των οργανισμών και των παρόχων cloud.

Η κατανεμημένη ταυτοποίηση είναι στην αιχμή της τεχνολογίας σήμερα η οποία συμβάλει στην αλληλεπίδραση των συστημάτων και των εφαρμογών που διαχωρίζονται από το σύνορο εμπιστοσύνης του οργανισμού. Η ομοσπονδία ταυτοποίησης συνδυάζεται με με την IAM και μπορεί να παίξει σημαντικό ρόλο στην υιοθέτηση του cloud από τους οργανισμούς.

Οι πάροχοι πρέπει να υποστηρίζουν τα στάνταρ της IAM (π.χ SAML) και πρακτικές όπως η ομοσπονδία ταυτοποίησης. Οι υπηρεσίες cloud που υποστηρίζουν IAM θα επιταχύνουν το πέρασμα από τα έμπιστα εταιρικά δίκτυα στο έμπιστο μοντέλο υπηρεσιών του cloud. Για τους πελάτες μια καλά υλοποιημένη IAM θα βοηθήσει στην προστασία της εμπιστευτικότητας της ακεραιότητας και της διαχείρισης των πληροφοριών που αποθηκεύονται στο cloud.

3.4.1 Γιατί IAM?

Παραδοσιακά, οι οργανισμοί επενδύουν σε IAM για να βελτιώσουν την λειτουργική αποδοτικότητα και να συμμορφωθούν με τις απαιτήσεις για ιδιωτικότητα και προστασία των δεδομένων.

Βελτίωση λειτουργικής αποδοτικότητας

> Η κατάλληλη αρχιτεκτονική IAM με τις διεργασίες της μπορεί να βελτιώσει την αποδοτικότητα αυτοματοποιώντας την είσοδο των χρηστών και άλλες επαναλαμβανόμενες διαδικασίες όπως π.χ η αυτοεξυπηρέτηση για χρήστες που ζητάνε να ρυθμίσουν εκ νέου τον κωδικό τους που σε αντίθετη περίπτωση θα απαιτούσε την εμπλοκή του διαχειριστή.

Ρυθμιστική διαχείριση συμμόρφωσης

> Για να προστατέψουν τα συστήματα, τις εφαρμογές και τις πληροφορίες από εξωτερικές και εσωτερικές απειλές (π.χ δυσαρεστημένοι υπάλληλοι διαγράφουν σημαντικά αρχεία), αλλά και για να συμμορφωθούν με απαιτήσεις ρυθμιστικές, ιδιωτικότητας και προστασίας των δεδομένων οι

οργανισμοί υλοποιούν ένα πλαίσιο εργασίας όπως το ISO 27002. Οι διεργασίες και οι πρακτικές της IAM βοηθούν τους οργανισμούς στην περιοχή του ελέγχου πρόσβασης και της λειτουργικής ασφάλειας (π.χ συμμόρφωση με τις απαιτήσεις για διαχωρισμό καθηκόντων και ανάθεση περιορισμένων προνομίων σε μέλη του προσωπικού για την διεκπεραίωση των καθηκόντων τους).

Εκτός του να βελτιώνει την λειτουργική αποδοτικότητα η IAM μπορεί να φέρει και να αναπτύσσει νέα μοντέλα τεχνολογίας πληροφορικής (π.χ υπηρεσίες cloud). Για παράδειγμα η ομοσπονδία ταυτοποίησης, ένα κύριο συστατικό της IAM επιτρέπει την διασύνδεση και την φορητότητα των πληροφοριών ταυτοποίησης μεταξύ συνόρων εμπιστοσύνης. Έτσι επιτρέπει τις επιχειρήσεις και τους παρόχους cloud να γεφυρώνουν domain ασφάλειας μέσω διαδικτυακού single sign-on.

Μερικές από τις περιπτώσεις χρήσης του cloud που απαιτούν IAM που υποστηρίζεται από τον πάροχο είναι:

- Υπάλληλοι ενός οργανισμού χρησιμοποιούν μια υπηρεσία SaaS που χρησιμοποιεί ομοσπονδία ταυτοποίησης (π.χ το προσωπικό πωλήσεων και υποστήριξης αποκτούν πρόσβαση στο Salesforce.com με εταιρικές ταυτότητες και πιστοποιητικά)
- Διαχειριστές του τμήματος τεχνολογίας πληροφορικής χρησιμοποιούν την κονσόλα διαχείρισης για τον εφοδιασμό πόρων και πρόσβασης των χρηστών με εταιρική ταυτότητα (π.χ διαχειριστές της Newco.com προμηθεύουν νέες εικονικές μηχανές στο Amazon EC2 διαμορφωμένες με ταυτοποίηση και πιστοποιητικά για τον χειρισμό των μηχανών [π.χ εκίνηση, διακοπή και διαγραφή μιας εικονικής μηχανής])
- Τελικοί χρήστες προσπελαύνουν υπηρεσίες αποθήκευσης στο cloud (π.χ Amazon S3) και μοιράζονται αρχεία και αντικείμενα με χρήστες μέσα και εκτός του domain χρησιμοποιώντας χαρακτηριστικά διαχείρισης πολιτικής πρόσβασης.
- Μια εφαρμογή που διανέμεται από έναν πάροχο cloud (π.χ Amazon EC2) χρησιμοποιεί υπηρεσία αποθήκευσης από έναν άλλον πάροχο (π.χ Mosso)

Τα χαρακτηριστικά της IAM όπως το SSO επιτρέπει στις εφαρμογές να εξωτερικεύουν χαρακτηριστικά αυθεντικοίησης, έτσι οι επιχειρήσεις μπορούν να

υιοθετήσουν γρήγορα οτιδήποτε ως υπηρεσία (για παράδειγμα Salesforce.com) μειώνοντας τον χρόνο που απαιτείται για την ενοποίηση με τον πάροχο. Οι δυνατότητες της IAM βοηθούν επίσης τις επιχειρήσεις να αναθέσουν σε εξωτερικούς συνεργάτες διεργασίες ή υπηρεσίες με μειωμένη επίπτωση στην ασφάλεια και την ιδιωτικότητα της επιχείρησης.

3.4.2 Καθορισμός Εννοιών IAM

Αυθεντικοποίηση

Αυθεντικοποίηση είναι η διαδικασία πιστοποίησης της ταυτότητας ενός χρήστη ή συστήματος (π.χ το Lightweight Directory Access Protocol – LDAP πιστοποιεί τα διαπιστευτήρια που παρουσιάζει ο χρήστης, όπου το αναγνωριστικό είναι ένα εταιρικό αναγνωριστικό χρήστη όπου είναι μοναδικό και εκχωρείται σε ένα υπάλληλο. Σε μερικές περιπτώσεις όπως αλληλεπίδραση μεταξύ υπηρεσιών η αυθεντικοποίηση εμπλέκεται πιστοποιώντας το δίκτυο της υπηρεσίας που ζητάει πρόσβαση σε πληροφορίες που βρίσκονται σε μια άλλη υπηρεσία (π.χ μια διαδικτυακή υπηρεσία συνδέεται σε μια υπηρεσία πιστωτικών καρτών για να πιστοποιήσει την πιστωτική κάρτα για λογαριασμό του πελάτη)

Εξουσιοδότηση

Εξουσιοδότηση είναι η διαδικασία με την οποία καθορίζονται τα προνόμια που δικαιούται ο χρήστης ή το συστήματα αφότου εξακριβωθεί η ταυτότητα του. Στον κόσμο των ψηφιακών υπηρεσιών η εξουσιοδότηση συνήθως ακολουθεί την αυθεντικοποίηση και χρησιμοποιείται για να καθορίσει πότε ένας χρήστης ή μια υπηρεσία έχει τα απαραίτητα προνόμια για να πραγματοποιήσει μια λειτουργία.

Έλεγχος

Στο πλαίσιο της IAM ο έλεγχος συνεπάγεται την διαδικασία της επανεξέτασης των καταγραφών της αυθεντικοποίησης και της εξουσιοδότησης και των ενεργειών που λαμβάνουν χώρα ώστε να προσδιοριστεί η επάρκεια του συστήματος ελέγχων της IAM. Επίσης πιστοποιείται η συμμόρφωση με την καθιερωμένη πολιτική ασφάλειας,

εντοπίζονται παραβιάσεις στις υπηρεσίες ασφάλειας και προτείνονται οι όποιες απαραίτητες αλλαγές.

3.4.3 Αρχιτεκτονική IAM

Η IAM είναι περισσότερο μια άποψη αρχιτεκτονικής (βλέπε εικόνα 2-1) και μια συλλογή από τεχνολογικά συστατικά , διαδικασίες, και στάνταρ πρακτικές. Η στάνταρ IAM αρχιτεκτονική περιλαμβάνει ένα συνδυασμό τεχνολογίας, υπηρεσιών και διαδικασιών. Στον πυρήνα της αρχιτεκτονικής υλοποίησης βρίσκεται η υπηρεσία καταλόγου (π.χ LDAP ή Active Directory) που λειτουργεί ως πηγή πληροφοριών για την ταυτοποίηση, πιστοποίηση και τα χαρακτηριστικά των χρηστών. Η υπηρεσία καταλόγου αλληλεπιδρά με τα συστατικά τεχνολογίας της IAM και δεν είναι ασυνήθιστο οργανισμοί να χρησιμοποιούν διάφορους καταλόγους που δημιουργούνται για συγκεκριμένα λειτουργικά συστήματα (π.χ Τα Windows χρησιμοποιούν Active Directory, το Unix χρησιμοποιεί LDAP).

Οι διαδικασίες της IAM μπορούν να κατηγοριοποιηθούν γενικά ως εξής:

Διαχείριση Χρηστών

Δραστηριότητες για την αποτελεσματική διαχείριση του κύκλου ζωής της ταυτοποίησης

Διαχείριση Αυθεντικοποίησης

Δραστηριότητες για την αποτελεσματική διαχείριση της διαδικασίας προσδιορισμού ότι μια οντότητα είναι αυτός ή αυτό που ισχυρίζεται ότι είναι

Διαχείριση Εξουσιοδότησης

Δραστηριότητες για την αποτελεσματική διαχείριση της διαδικασίας προσδιορισμού των δικαιωμάτων μιας οντότητας με τα οποία αποφασίζεται ποιους πόρους επιτρέπεται να χρησιμοποιεί σύμφωνα με την πολιτική του οργανισμού

Διαχείριση Πρόσβασης

Εφαρμογή πολιτικών για τον έλεγχο πρόσβασης σε ανταπόκριση στο αίτημα μιας οντότητας (χρήστης, υπηρεσία) που θέλει να προσπελάσει πόρους τεχνολογίας πληροφορικής μέσα στον οργανισμό

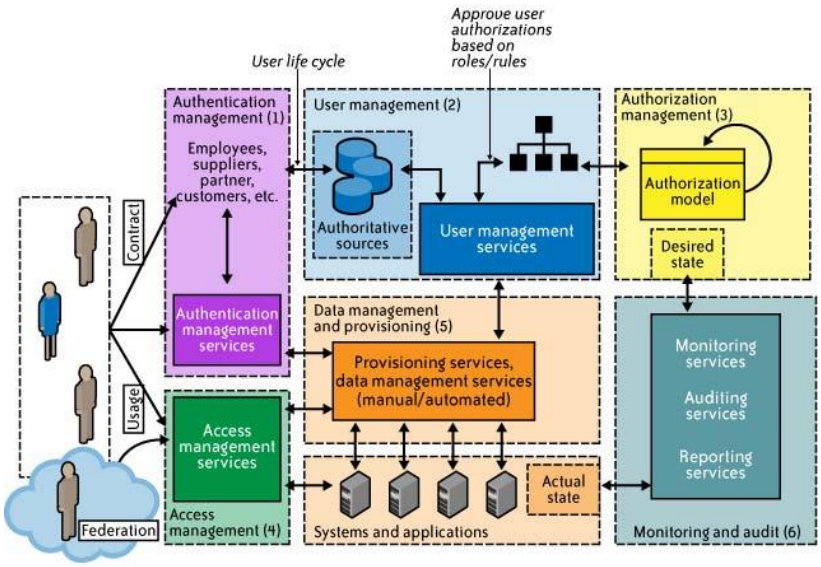
Διαχείριση Δεδομένων και εφοδιασμός

Διάδοση της ταυτότητας και των δεδομένων για χορήγηση άδειας IT πόρων μέσω αυτοματοποιημένων ή χειροκίνητων διαδικασιών

Παρακολούθηση και Έλεγχος

Παρακολούθηση, έλεγχος και αναφορά συμμόρφωσης των χρηστών με βάση την καθορισμένη πολιτική του οργανισμού

Εικόνα 3.4 Εταιρική αρχιτεκτονική IAM



Οι διαδικασίες της IAM υποστηρίζουν τις παρακάτω λειτουργικές δραστηριότητες :

Απονομή προνομίων

Απονομή προνομίων είναι η διαδικασία της εισαγωγής των χρηστών στα συστήματα και τις εφαρμογές . Αυτή η διαδικασία παρέχει στους χρήστες με την απαραίτητη πρόσβαση στα δεδομένα και στους πόρους τεχνολογίας. Η απονομή προνομίων είναι ένας συνδυασμός των καθηκόντων του τμήματος ανθρώπινου δυναμικού με το τμήμα τεχνολογίας πληροφορικής, όπου δίνεται στους χρήστες πρόσβαση σε αποθήκες δεδομένων, εφαρμογές και βάσεις δεδομένων με βάση ένα μοναδικό αναγνωριστικό χρήστη. Η αντίθετη διαδικασία συμβαίνει όταν διαγράφεται ή απενεργοποιείται μια οντότητα ή τα δικαιώματα που εκχωρήθηκαν σε αυτή

Διαχείριση Πιστοποιητικών και Ιδιοτήτων

Οι διαδικασίες αυτές διαχειρίζονται τον κύκλο ζωής των πιστοποιητικών και των χαρακτηριστικών των χρηστών – δημιουργία, έξοδος, ανάκληση, διαχείριση – για να περιοριστεί ο επιχειρηματικός κίνδυνος που σχετίζεται με την πλαστοπροσωπία και την ακατάλληλη χρήση του λογαριασμού ενός χρήστη. Τα πιστοποιητικά περιορίζονται σε ένα άτομο και πιστοποιούνται κατά την διαδικασία της αυθεντικοποίησης. Οι διαδικασίες αυτές περιλαμβάνουν τον εφοδιασμό χαρακτηριστικών όπως στατικά (π.χ στάνταρ κωδικός κειμένου) και δυναμικά (π.χ κωδικός μιας χρήσης), πιστοποιητικά που συμμορφώνονται με τα στάνταρ των κωδικών (π.χ κωδικοί ανθεκτικοί σε επιθέσεις λεξικού), χειρισμός λήξης των κωδικών, διαχείριση κρυπτογράφησης των πιστοποιητικών κατά την μεταφορά και τέλος πολιτικές πρόσβασης των χρηστών

Διαχείριση Τιτλοδότησης

Η τιτλοδότηση αναφέρεται και ως πολιτική εξουσιοδότησης. Η κατάλληλη διαχείριση της τιτλοδότησης εξασφαλίζει ότι ανατίθενται στους χρήστες μόνο τα απαιτούμενα προνόμια που ταιριάζουν με τις λειτουργίες της δουλειάς τους. Η τιτλοδότηση μπορεί να χρησιμοποιηθεί για την ενίσχυση της ασφάλειας των διαδικτυακών εφαρμογών, των αρχείων και των εγγράφων, και των φυσικών συστημάτων.

Διαχείριση Συμμόρφωσης

Η διαδικασία αυτή υποδηλώνει ότι τα δικαιώματα πρόσβασης και τα προνόμια παρακολουθούνται ώστε να διασφαλιστεί η ασφάλεια των πόρων. Η διαδικασία αυτή επίσης βοηθάει στο να πιστοποιηθεί η συμμόρφωση με τις διάφορες πολιτικές ελέγχου πρόσβασης και τα στάνταρ που περιλαμβάνουν πρακτικές όπως τον διαχωρισμό των καθηκόντων , παρακολούθηση πρόσβασης, περιοδικός έλεγχος, και δημιουργία αναφορών. Ένα παράδειγμα είναι το πιστοποιητικό ενός χρήστη που επιτρέπει στους ιδιοκτήτες μιας εφαρμογής να πιστοποιούν ότι μόνο εξουσιοδοτημένοι χρήστες έχουν τα προνόμια να προσπελαύνουν ευαίσθητες επιχειρησιακές πληροφορίες

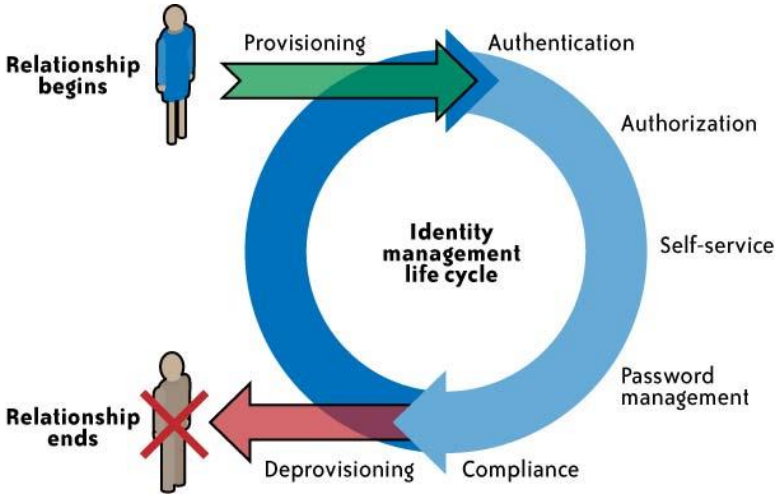
Διαχείριση Ομοσπονδίας Ταυτοποίησης

Η ομοσπονδία ταυτοποίησης διαχειρίζεται την εμπιστοσύνη των σχέσεων που εγκαθιδρύονται πέρα από το σύνορο του εσωτερικού δικτυού ανάμεσα σε διακριτούς οργανισμούς. Η ομοσπονδία είναι μια σύμπραξη οργανισμών που ανταλλάσουν πληροφορίες σχετικά με τους χρήστες τους και τους πόρους ώστε να διευκολύνουν την συνεργασία και τις συναλλαγές.

Συγκεντρωτισμός της αυθεντικοποίησης (authN) και της εξουσιοδότησης (authZ)

Μια κεντρική διαδικασία αυθεντικοποίησης και εξουσιοδότησης μειώνει την ανάγκη των δημιουργών εφαρμογών να κατασκευάζουν ατομικές λύσεις αυθεντικοποίησης και εξουσιοδότησης στις εφαρμογές τους. Επιπλέον προωθεί μια πιο χαλαρή αρχιτεκτονική όπου οι εφαρμογές δεν χρειάζεται να αγνοούν τις μεθόδους και τις πολιτικές της αυθεντικοποίησης. Αυτή η προσέγγιση αποκαλείται επίσης «εξωτερίκευση του authN και AuthZ" από τις εφαρμογές.

Εικόνα 3.5 Κύκλος ζωής Ταυτοποίησης



3.4.4 IAM στάνταρ και προδιαγραφές για Οργανισμούς

Τα παρακάτω στάνταρ και προδιαγραφές της IAM βοηθάνε τους οργανισμούς να υλοποιήσουν αποτελεσματικές και αποδοτικές πρακτικές διαχείρισης πρόσβασης στο cloud. Αυτές οι προδιαγραφές κατηγοριοποιούνται με βάση τις τέσσερεις πιο σημαντικές προκλήσεις στην διαχείριση πρόσβασης που αντιμετωπίζουν οι χρήστες του cloud (Mather κ.α., 2009):

1. Πώς μπορεί να αποφευχθεί η αντιγραφή της ταυτότητας, των χαρακτηριστικών και των πιστοποιητικών των χρηστών? SAML.

2. Πώς γίνεται με αυτοματοποιημένες διαδικασίες να προμηθεύονται οι χρήστες με υπηρεσίες cloud καθώς και να αφαιρούνται οι υπηρεσίες αυτές με τον ίδιο τρόπο? SPML.
3. Πώς γίνεται να προμηθεύονται οι λογαριασμοί των χρηστών με τα κατάλληλα προνόμια και διαχείριση της τιτλοδότησης των χρηστών?XACML.
4. Πώς γίνεται να εξουσιοδοτεί η υπηρεσία X να προσπελάσει τα δεδομένα της μια υπηρεσία Y χωρίς να εκτεθούν τα πιστοποιητικά?OAuth.

3.5 Πρωτόκολλα και μηχανισμοί για IAS

3.5.1 Security Assertion Markup Language (SAML)(Γλώσσα σήμανσης ισχυρισμού ασφάλειας)

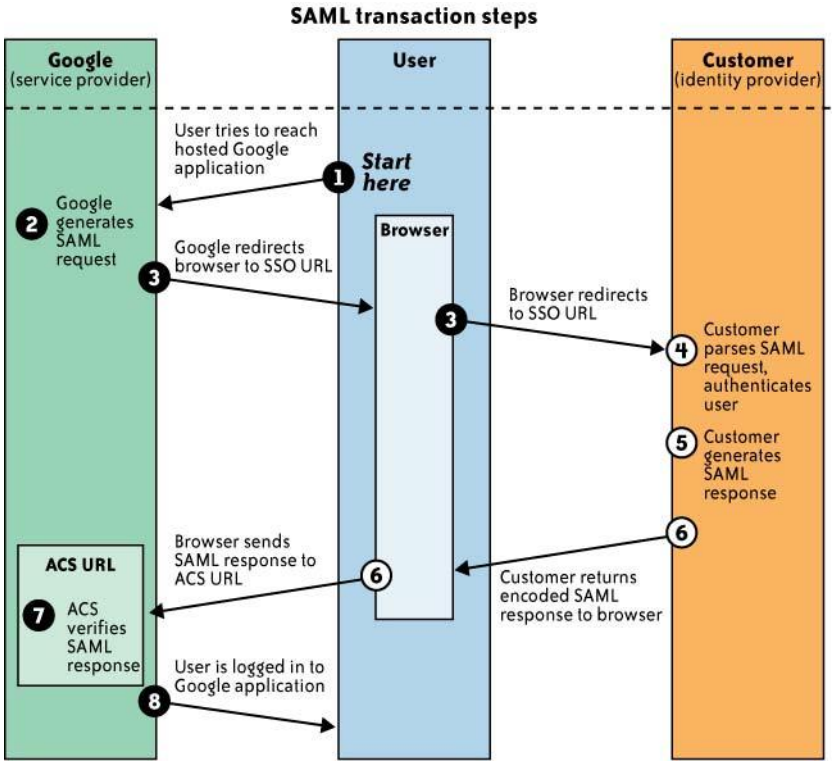
Η γλώσσα SAML είναι η πιο ώριμη, λεπτομερής και ευρέως αποδεκτή οικογένεια προδιαγραφών για την είσοδο των χρηστών του cloud μέσω browser. Μόλις ο χρήστης αυθεντικοποιηθεί από την υπηρεσία ταυτοποίησης, μπορεί ελεύθερα να έχει πρόσβαση σε όλες τις υπηρεσίες του cloud που βρίσκονται μέσα στο έμπιστο domain, έτσι ξεπερνιέται το πρόβλημα ύπαρξης μιας διαδικασίας εισόδου ειδικά σχεδιασμένης για το cloud. Δεδομένου ότι η SAML επιτρέπει την είσοδο στους χρήστες χρησιμοποιώντας πολιτικές αυθεντικοποίησης που εμπεριέχουν ρίσκο, γιαυτό οι πελάτες θα πρέπει να επιλέγουν ισχυρή αυθεντικοποίηση για συγκεκριμένες υπηρεσίες του cloud. Αυτό μπορεί εύκολα να επιτευχθεί χρησιμοποιώντας τον πάροχο ταυτοποίησης (IdP) του οργανισμού, ο οποίος παρέχει ισχυρή αυθεντικοποίηση. Υλοποιώντας τεχνικές ισχυρής αυθεντικοποίησης όπως αυθεντικοποίηση δύο συντελεστών , οι χρήστες είναι λιγότερο ευάλωτοι σε επιθέσεις phishing που όλο και αυξάνονται στο ιντερνέτ. Η ισχυρή αυθεντικοποίηση στις υπηρεσίες cloud ενδείκνυται για να προστατεύει τα πιστοποιητικά των χρηστών από επιθέσεις τύπου “man in the middle” ; όταν υπολογιστές ή φυλλομετρητές πέφτουν θύματα επιθέσεων Trojan. Οι πάροχοι υποστηρίζοντας την SAML αναθέτουν τις πολιτικές αυθεντικοποίησης στους πελάτες τους.

Η εικόνα 3-3 παρουσιάζει ένα SSO στο Google Apps από τον φυλλομετρητή. Στην εικόνα παρουσιάζονται τα παρακάτω βήματα που εμπεριέχονται σε μια διαδικασία SSO.

1. Ο χρήστης ενός οργανισμού προσπαθεί να φτάσει σε μια εφαρμογή που φιλοξενείται στο Google όπως το Gmail, Start Pages ή κάποια άλλη υπηρεσία της Google.
2. Η Google δημιουργεί ένα SAML αίτημα αυθεντικοποίησης. Το SAML αίτημα κωδικοποιείται και ενσωματώνεται στο URL για τον πάροχο πιστοποίησης του οργανισμού που υποστηρίζει την υπηρεσία SSO. Η αναμεταδιδόμενη παράμετρος που εμπεριέχει το κωδικοποιημένο URL της Google εφαρμογής που ο χρήστης προσπαθεί να φτάσει εμπεριέχεται επίσης στο SSO URL. Αυτή η παράμετρος είναι ένας αδιαφανής προσδιοριστής που επιστρέφει χωρίς καμιά αλλαγή.
3. Η Google στέλνει μια ανακατεύθυνση στον φυλλομετρητή του χρήστη. Το ανακατευθυνόμενο URL περιέχει το κωδικοποιημένο SAML αίτημα αυθεντικοποίησης που πρέπει να υποβληθεί στον πάροχο ταυτοποίησης (IdP) του οργανισμού.
4. Ο πάροχος ταυτοποίησης αποκωδικοποιεί το SAML αίτημα και εξάγει τα URL για την υπηρεσία ισχυρισμού καταναλωτή (Assertion consumer service ACS) της Google και το URL προορισμού του πελάτη (αναμεταδιδόμενη παράμετρος). Ο πάροχος ταυτοποίησης τότε αυθεντικοποιεί τον χρήστη είτε ζητώντας του έγκυρα πιστοποιητικά εισόδου είτε ελέγχοντας για έγκυρα session cookies.
5. Ο πάροχος ταυτοποίησης τότε παράγει μια SAML ανταπόκριση που περιέχει το όνομα χρήστη του αυθεντικοποιημένου χρήστη. Σύμφωνα με τις προδιαγραφές της SAML 2.0 αυτή η ανταπόκριση υπογράφεται ψηφιακά από τον πάροχο ταυτοποίησης με τα δημόσια και ιδιωτικά κλειδιά DSA/RSA.
6. Ο πάροχος ταυτοποίησης κωδικοποιεί την ανταπόκριση SAML και την αναμεταδιδόμενη παράμετρο και την επιστρέφει στον φυλλομετρητή του χρήστη . Ο πάροχος παρέχει έναν μηχανισμό ώστε ο φυλλομετρητής να μπορέσει να προωθήσει αυτή την πληροφορία στη ACS της Google. Για παράδειγμα παρέχει ένα κουμπί το οποίο ο χρήστης μπορεί να πατήσει ώστε να υποβάλει στη Google μια φόρμα που περιέχει την ανταπόκριση SAML ;ή μπορεί να γίνει αυτόματα μέσω της χρήσης Javascript.

7. Η ACS της Google πιστοποιεί την ανταπόκριση SAML χρησιμοποιώντας το δημόσιο κλειδί του παρόχου ταυτοποίησης. Αν η ανταπόκριση πιστοποιηθεί με επιτυχία η ACS ανακατευθύνει τον χρήστη στο URL προορισμού.
8. Ο χρήστης έχει ανακατευθυνθεί στο URL προορισμού και έχει εισαχθεί στο Google App.

Εικόνα 3.6 Βήματα συναλλαγής SSO με χρήση SAML

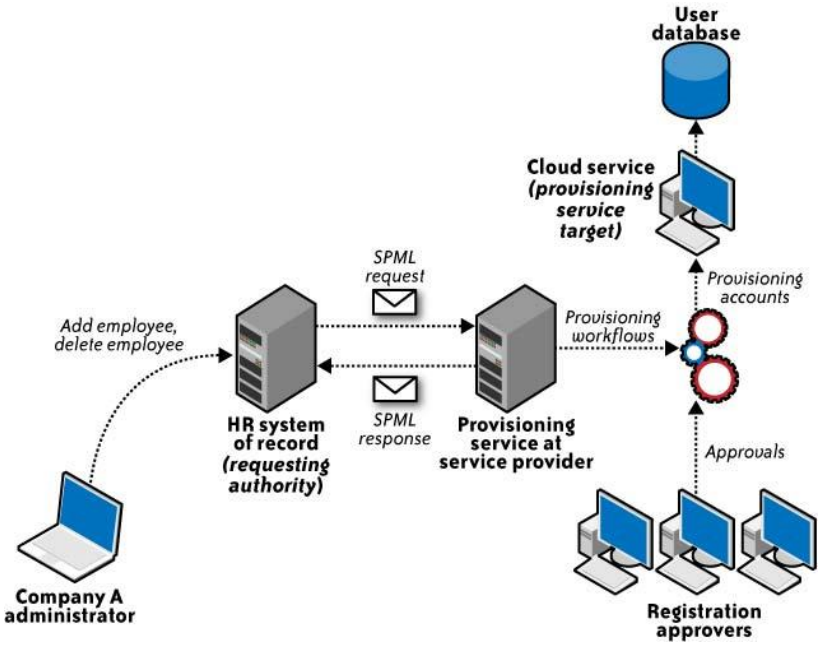


3.5.2 Service Provisioning Markup Language (SPML)

Η γλώσσα SPML βασίζεται στο πλαίσιο εργασίας της XML και αναπτύχθηκε από την OASIS για την ανταλλαγή χρηστών, πόρων, και προμήθεια υπηρεσιών μεταξύ συνεργαζόμενων οργανισμών. Η SPAML είναι ένα νέο στάνταρ που βοηθάει τους οργανισμούς να προμηθεύονται αυτόματα ταυτότητες χρηστών για υπηρεσίες cloud (π.χ μια εφαρμογή ή υπηρεσία που τρέχει στην ιστοσελίδα ενός πελάτη αιτείται νέους λογαριασμούς από το Salesforce.com). Όταν η SPML υποστηρίζεται οι πάροχοι SaaS μπορούν να ενεργοποιήσουν την προμήθεια και δημιουργία χρηστών σε πραγματικό χρόνο. Σε αυτό το μοντέλο ο πάροχος cloud εξάγει χαρακτηριστικά από το SAML του νέου χρήστη, δημιουργεί ένα SPML μήνυμα και το παραδίδει σε μια υπηρεσία εφοδιασμού όπου προσθέτει την ταυτότητα του χρήστη στην βάση δεδομένων των χρηστών του cloud.

Η υιοθέτηση της SPML μπορεί να ηγηθεί στην προτυποποίηση και αυτοματοποίηση της πρόσβασης των χρηστών ή των συστημάτων και στην τιτλοδότηση δικαιωμάτων στις υπηρεσίες του cloud έτσι ώστε οι πελάτες να μην παγιδεύονται σε ιδιωτικές λύσεις.

Η εικόνα 3.7 παρουσιάζει μια περίπτωση χρήσης της SPML στην οποία ένα σύστημα HR αιτείται ένα σύστημα προμήθειας στο cloud με ένα SPML αίτημα. Στην εικόνα το HR σύστημα καταγραφής είναι ένας πελάτης SPML που αλληλεπιδρά με μια SPML υπηρεσία προμήθειας στον πάροχο υπηρεσιών cloud, ο οποίος είναι υπεύθυνος να προμηθεύει με λογαριασμούς χρηστών τις υπηρεσίες cloud.

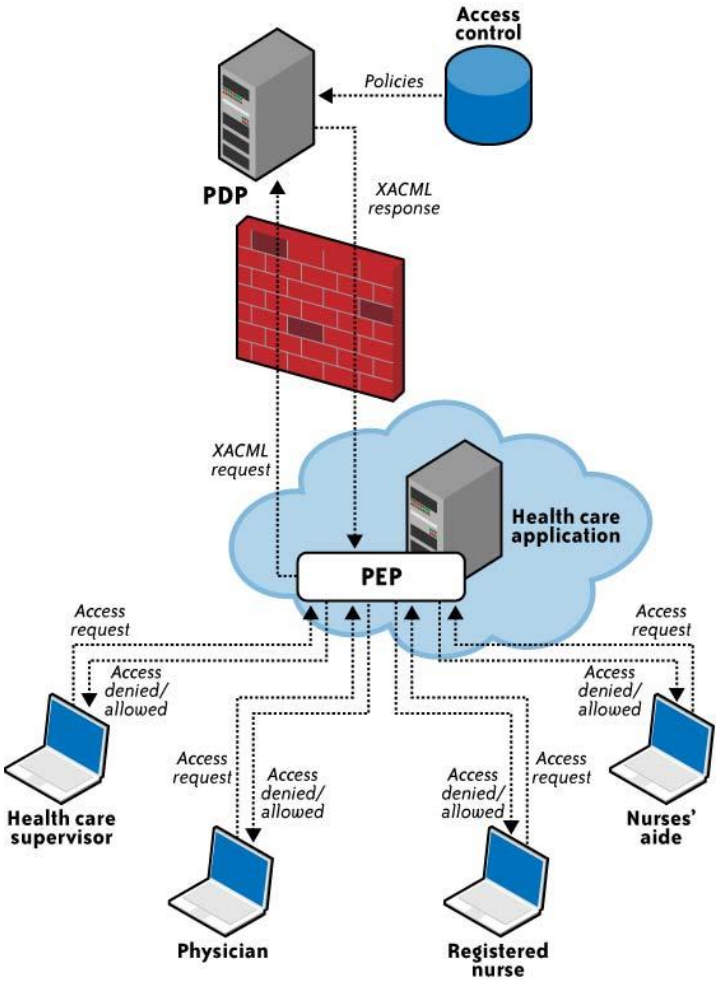


3.5.3 eXensible Access Control Markup Language (XACML)

Η XACML είναι ένα πρότυπο που επικυρώθηκε από την OASIS βασίζεται στην XML και χρησιμοποιείται για τον έλεγχο πρόσβασης, για την διαχείριση της πολιτικής και τις αποφάσεις πρόσβασης. Παρέχει ένα XML σχήμα για μια γλώσσα γενικής πολιτικής που χρησιμοποιείται για να προστατεύει κάθε είδους πόρους και να λαμβάνει αποφάσεις πρόσβασης για αυτούς τους πόρους. Η XACML προσδιορίζει επίσης το πρωτόκολλο με το οποίο το περιβάλλον της εφαρμογής επικοινωνεί με το σημείο αποφάσεων, η ανταπόκριση για ένα αίτημα πρόσβασης γίνεται με την χρήση XML.

Οι περισσότερες εφαρμογές έχουν έναν ενσωματωμένο μηχανισμό εξουσιοδότησης που παρέχει ή αρνείται την πρόσβαση σε συγκεκριμένες εφαρμογές ή πόρους που βασίζονται σε τίτλους που έχουν καταχωρηθεί στον χρήστη. Σε μια κεντρική αρχιτεκτονική IAM τα μοντέλα εξουσιοδότησης για συγκεκριμένες εφαρμογές καθιστά δύσκολο την ανάθεση δικαιωμάτων πρόσβασης σε ατομικούς χρήστες για όλες τις εφαρμογές. Η XACML παρέχει μια στάνταρ γλώσσα με μέθοδο ελέγχου πρόσβασης, εφαρμογή πολιτικής σε όλες τις εφαρμογές και υλοποίηση ενός κοινού προτύπου εξουσιοδότησης. Αυτές οι αποφάσεις εξουσιοδότησης βασίζονται σε διάφορες πολιτικές εξουσιοδότησης και ρόλους.

Η εικόνα 3.8 παρουσιάζει την αλληλεπίδραση μεταξύ διάφορων συμμετεχόντων με μοναδικούς ρόλους που προσπελαύνουν ευαίσθητες εγγραφές ασθενών που αποθηκεύονται σε μια ιατρική εφαρμογή.



Η εικόνα παρουσιάζει τα ακόλουθα βήματα που περιπλέκονται στην διαδικασία στης XACML:

1. Η ιατρική εφαρμογή διαχειρίζεται διάφορους εμπλεκόμενους που προσπελαύνουν διάφορα στοιχεία των ασθενών.
2. Το PEP είναι η διεπαφή της εφαρμογής. Λαμβάνει το αίτημα πρόσβασης και αξιολογείται με την βοήθεια της πολιτικής του σημείου αποφάσεων (PDP). Έπειτα επιτρέπει ή όχι την πρόσβαση στους πόρους.
3. Το PEP έπειτα στέλνει το αίτημα στο PDP το οποίο είναι το κεντρικό σημείο αποφάσεων. Συλλέγει όλες τις απαραίτητες πληροφορίες από τις διαθέσιμες πηγές πληροφοριών και καταλήγει σε μια απόφαση ως προς τι πρόσβαση να παρέχει.
4. Μετά την αξιολόγηση το PDP στέλνει μια XACML ανταπόκριση στο PEP.
5. Το PEP εκπληρώνει την υποχρέωση επιβάλλοντας την απόφαση του PDP.

3.5.4 Open Authentication (OAuth)

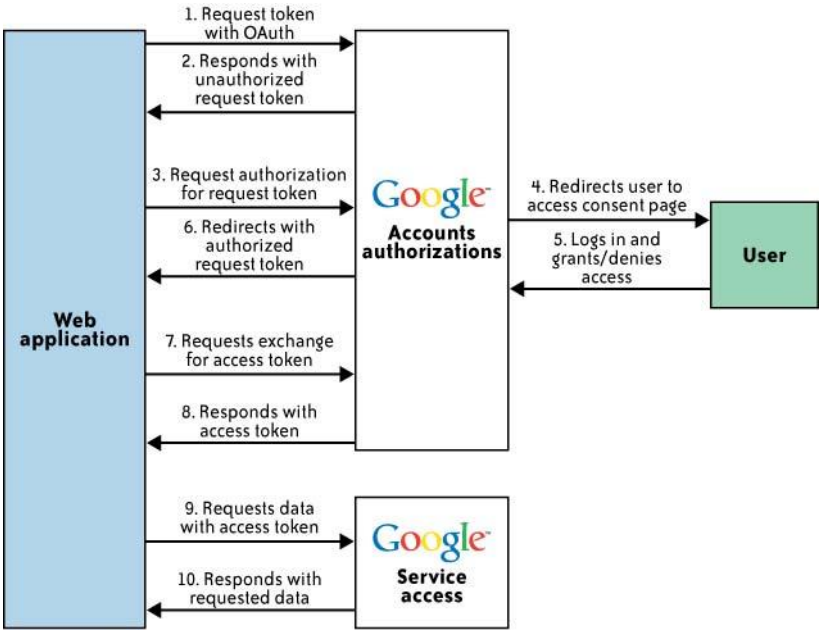
Το OAuth είναι ένα αναδυόμενο στάνταρ αυθεντικοποίησης το όποιο επιτρέπει τους πελάτες να ανταλλάσουν τους ιδιωτικούς τους πόρους (π.χ φωτογραφίες, βίντεο, λίστες επαφών, λογαριασμούς τραπεζών) που είναι αποθηκευμένα σε έναν πάροχο cloud με έναν άλλον πάροχο χωρίς να πρέπει να εκθέσουν πληροφορίες αυθεντικοποίησης (όνομα χρήστη και κωδικό). Το OAuth είναι ένα ανοιχτό πρότυπο και δημιουργήθηκε με σκοπό την παροχή αυθεντικοποίησης μέσω μιας διεπαφής προγραμματισμού ασφαλών εφαρμογών, μια απλή και στάνταρ μέθοδος για εφαρμογές σταθερών υπολογιστών, φορητών συσκευών και διαδικτυακών εφαρμογών. Το OAuth είναι μια μέθοδος δημοσίευσης και αλληλεπίδρασης με προστατευμένα δεδομένα. Για τους παρόχους, το OAuth παρέχει έναν τρόπο ώστε οι πελάτες να προσπελαύνουν τα δεδομένα τους που φιλοξενούνται από έναν άλλον πάροχο, ενώ ταυτόχρονα προστατεύουν τα πιστοποιητικά των λογαριασμών τους.

Μέσα σε έναν οργανισμό το OAuth παίζει τον ρόλο του SSO με έναν έμπιστο πάροχο υπηρεσιών υλοποιώντας ένα διαδικτυακό μοντέλο υπηρεσίας SSO. Το OAuth διευκολύνει την αυθεντικοποίηση ενός ζεύγους υπηρεσιών που αλληλεπιδρούν χωρίς την ανάγκη αναλυτικής αρχιτεκτονικής ομοσπονδίας. Όπως το OpenID το OAuth ξεκίνησε στον πελατοκεντρικό κόσμο για να βοηθήσει τις

υπηρεσίες των πελατών να προσπελαύνουν τα δεδομένα τους που φιλοξενούνται σε διάφορους παρόχους. Πρόσφατα η Google ανακοίνωσε μια υβριδική έκδοση του OpenID και του OAuth πρωτοκόλλου που συνδυάζει την εξουσιοδότηση και την αυθεντικοποίηση σε λιγότερα βήματα και με μεγαλύτερη ευχρηστία. Η Gdata διεπαφή προγραμματισμού της Google πρόσφατα ανακοίνωσε την υποστήριξη του OAuth (υποστηρίζει επίσης και την SAML για SOO μέσω φυλλομετρητή).

Η εικόνα 3-9 παρουσιάζει την αλληλουχία της αλληλεπίδρασης μεταξύ μιας διαδικτυακής εφαρμογής ενός πελάτη ή συνεργάτη, της Google υπηρεσίας και του τελικού χρήστη :

Εικονα 3.9 Περίπτωση χρήσης OAuth



1. Η διαδικτυακή εφαρμογή επικοινωνεί με την υπηρεσία εξουσιοδότησης της Google, ζητώντας τεκμήρια για μια ή περισσότερες εφαρμογές της Google.
2. Η Google πιστοποιεί ότι η διαδικτυακή εφαρμογή είναι καταχωρημένη και ανταποκρίνεται με ένα μη εξουσιοδοτημένο τεκμήριο.
3. Η διαδικτυακή εφαρμογή κατευθύνει τον τελικό χρήστη στην σελίδα εξουσιοδότησης της Google, αναφέροντας το αίτημα τεκμηρίωσης.
4. Στην σελίδα εξουσιοδότησης της Google ο χρήστης παρακινείται να εισάγει τα στοιχεία του για να πιστοποιηθούν και έπειτα είτε χορηγεί είτε αρνείται την περιορισμένη πρόσβαση στα δεδομένα του στην υπηρεσία τη Google από την διαδικτυακή εφαρμογή.

5. Ο χρήστης αποφασίζει πότε θα χορηγήσει ή όχι πρόσβαση στην διαδικτυακή εφαρμογή. Εάν ο χρήστης αρνηθεί την πρόσβαση, ανακατευθύνεται σε μια σελίδα της Google και όχι πίσω στην σελίδα της διαδικτυακής εφαρμογής.
6. Εάν ο χρήστης χορηγήσει πρόσβαση τότε η υπηρεσία εξουσιοδότησης τον ανακατευθύνει στην σελίδα που
7. Η διαδικτυακή εφαρμογή στέλνει ένα αίτημα στην υπηρεσία εξουσιοδότησης της Google για να αλλάξει το τεκμήριο εξουσιοδότησης σε τεκμήριο πρόσβασης.
8. Η Google πιστοποιεί το αίτημα και επιστρέφει ένα έγκυρο τεκμήριο πρόσβασης.
9. Η διαδικτυακή εφαρμογή στέλνει μια αίτηση στην υπηρεσία της Google, η αίτηση υπογράφεται και περιέχει μέσα το τεκμήριο εισόδου.
10. Εάν η Google αναγνωρίσει το τεκμήριο παρέχει τα δεδομένα που αιτήθηκαν.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό έγινε παρουσίαση των απειλών που σχετίζονται με την ασφάλεια της υποδομής ενός οργανισμού στο επίπεδο δικτύου, φιλοξενίας και εφαρμογών καθώς και τρόποι προστασία από αυτές. Επίσης προσεγγίστηκε η ασφάλεια υποδομής στο πλαίσιο του SPI μοντέλου διανομής του Cloud (SaaS, PaaS, IaaS) και του επιχειρησιακού μοντέλου (δημόσιο, ιδιωτικό και υβριδικό cloud). Τέλος έγινε παρουσίαση της τρέχουσας κατάστασης της πρακτικής διαχείρισης ταυτοποίησης και πρόσβασης (IAM- Identity and Access Management) και χαρακτηριστικών της IAM που ενισχύουν την Αυθεντικοποίηση, Εξουσιοδότηση και τον Έλεγχο της πρόσβασης των χρηστών στις υπηρεσίες του Cloud. Στο επόμενο κεφάλαιο θα υλοποιηθεί μια υποδομή cloud computing στις εγκαταστάσεις του ΑΤΕΙΘ, θα παρουσιαστούν μερικά παραδείγματα παρόχων Cloud και τέλος θα περιγραφούν οι δυσκολίες που προέκυψαν από την υλοποίηση αυτή.

ΚΕΦΑΛΑΙΟ 4

Υλοποιώντας το Cloud Computing

ΕΙΣΑΓΩΓΗ

Προκειμένου να αντιληφθούμε καλύτερα την έννοια του Cloud Computing καθώς και για να είμαστε σε θέση περαιτέρω έρευνας πάνω σε θέματα ασφάλειας κρίθηκε απαραίτητη η υλοποίηση ενός cloud με δικές μας υποδομές και εντός του ΑΤΕΙΘ. Αρχικά γίνεται μια σύντομη παρουσίαση των μεγάλων παρόχων που βρίσκονται στον χώρο του cloud computing καθώς και τι αυτοί προσφέρουν, έπειτα παρουσιάζονται ορισμένες πλατφόρμες cloud ανοιχτού κώδικα προκειμένου να επιλεχθεί ένα από αυτά για την δική μας υλοποίηση. Τέλος μέσα από την εμπειρία της υλοποίησης αυτής περιγράφονται οι δυσκολίες που αντιμετωπίσαμε σε συνδυασμό με τις αρχικές ιδέες και τι τελικά μπορεί να συμβεί στην πράξη.

4.1 Παραδείγματα Παρόχων υπηρεσιών Cloud

4.1.1 Amazon Web Service (IaaS)

Το Amazon Web Service (AWS) παρέχει την υποδομή ως υπηρεσία στο Cloud σε οργανισμούς που χρειάζονται υπολογιστική ισχύ, αποθήκευση και άλλες υπηρεσίες. Σύμφωνα με την Amazon το AWS προσφέρει στους πελάτες του το πλεονέκτημα της παγκόσμιας υπολογιστικής υποδομής του Amazon.com η οποία αποτελεί την καρδιά του Amazon.com στο λιανικό εμπόριο και τις συναλλακτικές επιχειρήσεις.

Το AWS παρέχει μια σειρά από υπηρεσίες υποδομής συμπεριλαμβανομένων των παρακάτω :

4.1.2 Elastic Compute Cloud (EC2)

Το EC2 είναι μια διαδικτυακή υπηρεσία που παρέχει ευμετάβλητη υπολογιστική ισχύ στο Cloud. Το EC2 επιτρέπει την ανάπτυξη ευμετάβλητων εφαρμογών με το να παρέχει μια διεπαφή μέσω της οποίας οι πελάτης μπορούν να δημιουργήσει εικονικές μηχανές (VM's) - οι οποίες είναι στιγμιότυπα εξυπηρετητών στους οποίους ο πελάτης μπορεί να φορτώσει οποιοδήποτε λογισμικό της επιλογής του. Ο πελάτης μπορεί να δημιουργήσει, προσπελάσει, και τερματίσει στιγμιότυπα εξυπηρετητών ανάλογα με τις ανάγκες του και να πληρώσει ανάλογα με το πόση ώρα είναι ενεργά αυτά τα στιγμιότυπα.

Simple Storage Service (S3)

Το S3 παρέχει μια διεπαφή διαδικτυακής υπηρεσίας η οποία χρησιμοποιείται για αποθήκευση και ανάκτηση απεριόριστων ποσοτήτων δεδομένων, οποιαδήποτε στιγμή και από οπουδήποτε στο Παγκόσμιο Δίκτυο.

Simple Queue Service (SQS)

Το SQS είναι μια κατανεμημένη υπηρεσία ουράς μηνυμάτων που επιτρέπει την προγραμματική αποστολή μηνυμάτων μέσω διαδικτυακών εφαρμογών σαν τρόπο επικοινωνίας στο διαδίκτυο. Ο σκοπός του SQS είναι να παρέχει μια κλιμακωτή ουρά μηνυμάτων η οποία επιλύει ζητήματα που προέρχονται από απλά προβλήματα μεταξύ δημιουργού –καταναλωτή ή προβλήματα συνδεσιμότητας μεταξύ τους.

4.1.3 CloudFront

Το CloudFront είναι ένα δίκτυο παράδοσης περιεχομένου το οποίο χρησιμοποιεί ένα παγκόσμιο δίκτυο κόμβων. Η αιτήσεις για αντικείμενα δρομολογούνται αυτόματα στον κοντινότερο κόμβο ώστε το περιεχόμενο να παραδίδεται με την καλύτερη δυνατή απόδοση. Το CloudFront δουλεύει με το S3 που αποθηκεύει τις αυθεντικές, τελικές εκδόσεις των αρχείων.

4.1.4 SimpleDB

Το SimpleDB είναι μια διαδικτυακή υπηρεσία που παρέχει καίριες λειτουργίες μιας βάσης δεδομένων όπως ευρετήριο δεδομένων και ερωτήματα. Αυτή η υπηρεσία συνεργάζεται στενά με το S3 και το EC2 προσφέροντας την δυνατότητα αποθήκευσης, επεξεργασίας και ερωτημάτων στο Cloud καθιστώντας την υπολογιστική μέσω διαδικτύου ευκολότερη και οικονομικά αποδοτικότερη για τους δημιουργούς λογισμικού.

Πίνακας 4-1 Περιπτώσεις Χρήσης AWS

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Φιλοξενία διαδικτυακών εφαρμογών	Οι κατασκευαστές διαδικτυακών εφαρμογών μπορούν να χρησιμοποιούν την υποδομή του AWS για υπολογιστική ισχύ και αποθήκευση αντί να φιλοξενούν εσωτερικά τις εφαρμογές τους, μειώνοντας το κόστος και αυξάνοντας την αποδοτικότητα που σχετίζεται με την διαχείριση της υποδομής και του χρόνου στην αγορά.	EC2, S3, SimpleDB, SQS
Αποθήκευση και Αντίγραφα Ασφαλείας	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το AWS για να διαχειριστούν την εσωτερική αποθήκευση και την λήψη αντιγράφων ασφαλείας ως εναλλακτική στην εσωτερική υποδομή αποθήκευσης. Παρόλο που το κόστος του υλικού αποθήκευσης μειώνεται, το μέγεθος των δεδομένων μεγαλώνει αυξάνοντας και τις ανάγκες για αποθήκευση.	S3
Παράδοση Περιεχομένου	Οργανισμοί που σχετίζονται με την παράδοση περιεχομένου όπως τη ροή δεδομένων μπορούν να χρησιμοποιήσουν το παγκόσμιο δίκτυο κόμβων του AWS για να μειώσουν την καθυστέρηση στην παράδοση και να βελτιώσουν την υπηρεσία.	CloudFront, S3
Υπολογιστική Υψηλής Απόδοσης	Οργανισμοί που έχουν ανάγκη από υψηλής απόδοσης υπολογιστική μπορούν να χρησιμοποιήσουν κατά απαίτηση την υπολογιστική ισχύ του AWS για να επεξεργαστούν μεγάλες ποσότητες δεδομένων χωρίς να χρειάζεται να δημιουργήσουν μια	EC2, S3

	εσωτερική υποδομή. Μειώνοντας έτσι το κόστος και αυξάνοντας την αποδοτικότητα .	
Φιλοξενία δεδομένων Media	Οργανισμοί που εμπλέκοντε στην διανομή και αποθήκευση αρχείων media μπορούν να χρησιμοποιήσουν το AWS για να διαχειριστούν τις απρόβλεπτες απαιτήσεις που σχετίζονται με την αποθήκευση και την επεξεργασία.	EC2, S3, CloudFront, SQS
MapReduse	Το MapReduse είναι μια διαδικτυακή υπηρεσία που επιτρέπει σε επιχειρήσεις, ερευνητές, αναλυτές δεδομένων, και κατασκευαστές λογισμικού να επεξεργάζονται τεράστιες ποσότητες δεδομένων χρησιμοποιώντας το πλαίσιο εργασίας Hadoop.	EC2, S3
Cloud “bursting”	Η ικανότητα να αντιμετωπίζονται οι αστραπιαίες αυξομειώσεις στις απαιτήσεις επεξεργασίας.	EC2

4.1.5 Google (SaaS, PaaS)

Το Google App Engine είναι η πλατφόρμα που παρέχεται ως υπηρεσία από την Google για την κατασκευή και φιλοξενία διαδικτυακών εφαρμογών στην υποδομή της. Προς το παρόν οι υποστηριζόμενες γλώσσες προγραμματισμού είναι η Python και η Java. Το App Engine παρέχεται δωρεάν μέχρι ένα σημείο χρήσης των πόρων από το οποίο και έπειτα υπάρχει χρέωση για τους επιπλέον πόρους (αποθήκευση, χρήση δικτύου, επεξεργαστικής ισχύς) που απαιτούνται από την εφαρμογή.

Το Google Apps είναι το λογισμικό ως υπηρεσία που παρέχεται από την Google και προσφέρει λογισμικό ηλεκτρονικού ταχυδρομείου και συνεργασίας. Παρέχει διάφορες εφαρμογές με παρόμοια λειτουργικότητα όπως οι παραδοσιακές σουίτες γραφείου, συμπεριλαμβάνοντας το Gmail, Ημερολόγιο, έγγραφα, και ιστοσελίδες. Επιπλέον το Google Apps περιέχει έναν αριθμό προϊόντων ασφάλειας για να παρέχει ασφάλεια στο ηλεκτρονικό ταχυδρομείο και να συμμορφώνεται με τις υπάρχουσες υποδομές ηλεκτρονικού ταχυδρομείου. Η βασική έκδοση παρέχεται δωρεάν και προσφέρει τον ίδιο αποθηκευτικό χώρο με τους απλούς λογαριασμούς του Gmail, η έκδοση Premier βασίζεται στο μοντέλο αδειοδότησης ανα χρήστη και το συσχετιζόμενο επίπεδο αποθήκευσης.

Πίνακας 4-2 Περιπτώσεις χρήσεις της Google

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Υπηρεσία μηνυμάτων	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το Google Apps για τα εσωτερικά ηλεκτρονικά μηνύματα και υπηρεσίες ημερολογίου χωρίς να επενδύουν και να συντηρούν την αντίστοιχη υποδομή.	Gmail, Google Calendar
Ασφάλεια στα υπάρχοντα συστήματα ηλεκτρονικών μηνυμάτων	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το Google Apps για να ασφαλίσουν τα υπάρχοντα συστήματα ηλεκτρονικού ταχυδρομείου φιλτράροντας τις απειλές όπως είναι οι ιοί και η ανεπιθύμητη αλληλογραφία, χωρίς να επενδύουν και να συντηρούν το αντίστοιχο λογισμικό και υλικό.	Google Email Security

Διατήρηση και αρχειοθέτηση μηνυμάτων ηλεκτρονικού ταχυδρομείου στα υπάρχοντα συστήματα	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το Google Apps για να διαχειριστούν την διατήρηση και αρχειοθέτηση των ηλεκτρονικών μηνυμάτων με την δυνατότητα αναζήτησης, ώστε να μπορούν να τα εντοπίζουν γρήγορα χωρίς να επενδύουν και να συντηρούν το αντίστοιχο λογισμικό και υλικό.	Google Email Archiving and Discovery
Συνεργασία	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το Google Apps για υπηρεσίες σουίτας γραφείου και συνεργασίας χωρίς να χρειάζεται την εγκατάσταση λογισμικού στους τοπικούς σταθμούς εργασίας και τους εξυπηρετητές.	Google Docs, Google Sites
Ανάπτυξη εφαρμογών	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την πλατφόρμα Google App Engine για να αναπτύξουν δικές τους εφαρμογές βασισμένες στην Java και την Python και τις συσχετιζόμενες υπηρεσίες χωρίς να επενδύσουν σε εσωτερική υποδομή.	App Engine

4.1.6 Microsoft Azure πλατφόρμα ως Υπηρεσία (PaaS)

Η πλατφόρμα υπηρεσιών Azure της Microsoft είναι κομμάτι της στρατηγικής της εταιρείας να μειώσει την έμφαση στα προϊόντα για υπολογιστές γραφείου και να μετατοπίσει περισσότερους πόρους στα διαδικτυακά προϊόντα. Το Azure παρέχει ένα λειτουργικό σύστημα που ονομάζεται Windows Azure, το οποίο εξυπηρετεί σαν σε πραγματικό χρόνο εκτέλεσης τις εφαρμογές και παρέχει ένα σύνολο υπηρεσιών που επιτρέπουν την ανάπτυξη, διαχείριση και φιλοξενία διαχειριζόμενων εφαρμογών στα κέντρα δεδομένων της Microsoft.

Η πλατφόρμα περιλαμβάνει τις ακόλουθες υπηρεσίες:

Υπηρεσίες .NET

Ένα σύνολο υπηρεσιών προσανατολισμένες στους δημιουργούς λογισμικού που παρέχουν βασικά κομμάτια που χρειάζονται σε πολλές εφαρμογές που βασίζονται στο Cloud (έλεγχο πρόσβασης, ροή εργασίας, κ.α)

Υπηρεσίες SQL

Ένα σύνολο υπηρεσιών που επεκτείνουν τις δυνατότητες του εξυπηρετητή Microsoft SQL στο Cloud ως διαδικτυακή, κατανεμημένη σχεσιακή βάση δεδομένων. Παρέχει διαδικτυακές υπηρεσίες που επιτρέπουν τα σχεσιακά ερωτήματα, την αναζήτηση και τον συγχρονισμό των δεδομένων με μετακινούμενους χρήστες, απομακρυσμένα γραφεία και εταιρικούς συνεργάτες.

Υπηρεσίες Live

Ένα σύνολο υπηρεσιών που παρέχουν στους δημιουργούς λογισμικού την δυνατότητα να συνδέσουν τις εφαρμογές τους με τους χρήστες του Windows Live. Επιπλέον οι υπηρεσίες Live επιτρέπουν στους χρήστες να συνδεθούν

χρησιμοποιώντας το Live αναγνωριστικό τους, να προσπελαύνουν και να μοιράζονται επαφές , να τροφοδοτούν περιεχόμενο στο Windows Live κ.ο.κ .

Πίνακας 4-3 Περιπτώσεις χρήσης της πλατφόρμας Azure

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Παροχή εκδόσεων εφαρμογών λογισμικού ως υπηρεσία από τους πωλητές	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την πλατφόρμα Azure για να εμπλουτίσουν την λειτουργικότητα των υπαρχουσών εφαρμογών χωρίς να επενδύσουν σε εσωτερική υποδομή. Για παράδειγμα αντί να συνεχίζεται το υπάρχον μοντέλο ανάπτυξης ο κατασκευαστής μπορεί να αναπτύξει μια SaaS έκδοση του προϊόντος.	Windows Azure, .Net Υπηρεσίες, SQL υπηρεσίες
Ανάπτυξη εφαρμογών	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την πλατφόρμα Azure για να αναπτύξουν δικές τους εφαρμογές βασισμένες στο Windows Azure και τις συσχετιζόμενες υπηρεσίες χωρίς να επενδύσουν σε εσωτερική υποδομή.	Windows Azure, .Net Υπηρεσίες, SQL υπηρεσίες

4.1.7 Proofpoint (SaaS, IaaS)

Η Proofpoint προσφέρει υπηρεσίες SaaS και IaaS στο cloud που σχετίζονται με την ασφάλεια των εταιρικών ηλεκτρονικών μηνυμάτων, την αρχειοθέτηση, την κρυπτογράφηση, και την αποτροπή απώλειας δεδομένων. Η χρέωση που ακολουθεί η Proofpoint για τις υπηρεσίες της ακολουθεί το μοντέλο χρέωσης ανά χρήση, ή ανά έτος εξαρτάται από το προϊόν και τα χαρακτηριστικά που αυτό προσφέρει.

Η Proofpoint προσφέρει μια σειρά από SaaS και IaaS υπηρεσίες συμπεριλαμβανομένων των παρακάτω :

Enterprise

Το Enterprise είναι μια υπηρεσία που προσφέρει ασφάλεια αμφότερα στα εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου χωρίς την ανάγκη ύπαρξης λογισμικού και υλικού από την μεριά του χρήστη. Η τροποποιήσιμη υπηρεσία μπορεί να αναπτυχθεί με πληθώρα επιλογών συμπεριλαμβάνοντας ένα πακέτο προστασίας, (με προστασία ανεπιθύμητων μηνυμάτων, προστασία από ιούς, τοίχο προστασίας, και επιβολή πολιτικής μηνυμάτων ηλεκτρονικού ταχυδρομείου), ένα πακέτο ιδιωτικότητας (με χαρακτηριστικά προστασίας των δεδομένων που συμπεριλαμβάνει ανίχνευση ιδιωτικής ταυτότητας, ανίχνευση οικονομικών πληροφοριών, προ-ρυθμισμένων πολιτικών προστασίας των δεδομένων, και διαχείριση περιστατικών), και ένα πακέτο κρυπτογράφησης το οποίο προσθέτει χαρακτηριστικά κρυπτογράφησης του ηλεκτρονικού ταχυδρομείου βασισμένα στην πολιτική.

Shield

Η υπηρεσία Shield αμύνεται ενάντια σε κακόβουλα και ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, μειώνοντας τον όγκο τον εισερχόμενων ανεπιθύμητων μηνυμάτων και αποτρέποντας τις επιθέσεις άρνησης υπηρεσίας (DoS) και επιθέσεις σε καταλόγους για την συγκομιδή διευθύνσεων ηλεκτρονικού ταχυδρομείου.

Archive

Η υπηρεσία Archive παρέχεται κατά απαίτηση και δίνει λύση στην διαχείριση αποθήκευσης μηνυμάτων ηλεκτρονικού ταχυδρομείου, νομικής ανακάλυψης, και συμμόρφωσης στους κανονισμούς. Τεχνολογία κρυπτογράφησης χρησιμοποιείται για να διασφαλιστεί ότι τα μηνύματα είναι ασφαλή καθώς μεταφέρονται στα κέντρα δεδομένων της Proofpoint καθώς και όταν αποθηκεύονται στο αρχείο. Επιπλέον οι εξουσιοδοτημένοι χρήστες μπορούν να πραγματοποιήσουν αναζήτηση στα αρχειοθετημένα μηνύματα. Αυτή η υπηρεσία δίνει την δυνατότητα στις επιχειρήσεις να εντοπίζουν μηνύματα ηλεκτρονικού ταχυδρομείου που εμπλέκονται με νομικές υποθέσεις και στους τελικούς χρήστες την δυνατότητα πρόσβασης στο ιστορικό των μηνυμάτων τους.

Πίνακας 4-4 Περιπτώσεις χρήσης της Proofpoint

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Ασφάλεια εισερχόμενων μηνυμάτων	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την ασφάλεια μηνυμάτων ηλεκτρονικού ταχυδρομείου της Proofpoint για να μπλοκάρουν την ανεπιθύμητη αλληλογραφία, ιούς, επιθέσεις προσποίησης, και ακατάλληλου περιεχομένου στα εισερχόμενα μηνύματα, και να εφαρμόσουν την πολιτική του οργανισμού στα εξερχόμενα μηνύματα.	Enterprise
Προστασία απώλειας δεδομένων	Οι οργανισμοί μπορούν να προστατέψουν τα εμπιστευτικά δεδομένα από ακατάλληλη διανομή τους μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου	Enterprise
Συμμόρφωση με τους κανονισμούς προστασίας των δεδομένων	Οι οργανισμοί πρέπει να εξασφαλίζουν ότι προσωπικές πληροφορίες όπως οικονομικά δεδομένα πελατών, και προσωπικές πληροφορίες υγείας προστατεύονται ενάντια σε ακατάλληλη έκθεση τους. Τα εξερχόμενα μηνύματα και τα επισυναπτόμενα αρχεία τους σαρώνονται και είτε κρυπτογραφούνται αυτόματα είτε μπλοκάρεται η αποστολή τους ως ακατάλληλα για δημοσίευση.	Enterprise
Αρχειοθέτηση μηνυμάτων ηλεκτρονικού ταχυδρομείου	Οι οργανισμοί μπορούν να ενισχύσουν την πολιτική τους για την διατήρηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου , να ελαφρύνουν τους τοπικούς τους εξυπηρετητές από το βάρος της αποθήκευσης, και να επιτυγχάνουν γρήγορη αναζήτηση στο ιστορικό των μηνυμάτων τους.	Archive

4.1.8 RightScale (IaaS)

Η RightScale παρέχει υπηρεσίες IaaS στο Cloud που βοηθούν τους οργανισμούς να διαχειρίζονται εφαρμογές Cloud που παρέχονται από άλλους παρόχους, όπως η AWS, FlexiScale, και GoGrid. Η πλατφόρμα διαχείρισης Cloud της RightScale επιτρέπει στους οργανισμούς να διαχειρίζονται και να υποστηρίζουν τις δικές τους εφαρμογές Cloud μέσω μιας διαδικτυακής πλατφόρμας διαχείρισης, ενώ παράλληλα επωφελούνται από τα πλεονεκτήματα που προσφέρουν διαφορετικοί πάροχοι Cloud. Η RightScale χρεώνει τις υπηρεσίες τις με βάση τις διαφορετικές εκδόσεις που προσφέρει, τα χαρακτηριστικά αυτών των εκδόσεων και τον χρόνο χρήσης των εξυπηρετητών.

Η πλατφόρμα διαχείρισης Cloud της RightScale περιλαμβάνει τα παρακάτω :

Περιβάλλον διαχείρισης Cloud

Η πλατφόρμα διαχείρισης Cloud παρέχει έλεγχο, διαχείριση, και υποστήριξη στον κύκλο ανάπτυξης Cloud μέσω ενός πίνακα ελέγχου για διαχείριση σε πραγματικό χρόνο διαφορετικών υλοποιήσεων μεταξύ ενός ή περισσότερων cloud, συμπεριλαμβανόμενων δημόσιων και ιδιωτικών cloud. Ο πίνακας ελέγχου παρέχει διάφανη πρόσβαση και έλεγχο σε όλες τις πτυχές της ανάπτυξης cloud όπως παράμετροι εισόδου, επίβλεψη σε πραγματικό χρόνο, πρότυπες ρυθμίσεις εξυπηρετητή και αυτόματη ή χειροκίνητη απόκριση.

Πρότυπες ρυθμίσεις εξυπηρετητών Cloud

Οι πρότυπες ρυθμίσεις εξυπηρετητών και η βιβλιοθήκη Best Practice βοηθάν στην απλοποίηση της διαχείρισης της ανάπτυξης. Οι πρότυπες ρυθμίσεις εξυπηρετητών που αναπτύχθηκαν από την RightScale, ενσωματώνουν βασικές ρυθμίσεις για το cloud για κοινά συστατικά ανάπτυξης εφαρμογών όπως το επεκτάσιμο web, εφαρμογές εξυπηρετητών και βάσεις δεδομένων. Οι εταιρικές πρότυπες ρυθμίσεις που αναπτύχθηκαν από συνεργάτες της RightScale βοηθάει στο να ενσωματωθούν εργαλεία και συστατικά των συνεργατών της στις υλοποιήσεις. Οι πρότυπες ρυθμίσεις εξυπηρετητών των πελατών μπορούν να κλονοποιηθούν και να τροποποιηθούν για συγκεκριμένες ανάγκες, και έπειτα να αποθηκευτούν σε βιβλιοθήκες. Με το πέρασμα του χρόνου ένας οργανισμός μπορεί να δημιουργήσει μια αποθήκη με πρότυπα ρυθμίσεων εξυπηρετητών παρέχοντας πολύτιμη εταιρική γνώση για τον οργνισμό.

Προσαρμόσιμη μηχανή αυτοματισμού

Η προσαρμόσιμη μηχανή αυτοματισμού εκτελεί και διαχειρίζεται υλοποιήσεις που προσαρμόζονται στις συνθήκες κατόπιν απαίτησης του συστήματος, αποτυχίας του συστήματος ή άλλων συγκεκριμένων γεγονότων. Όταν απαιτούνται αλλαγές, εξυπηρετητές μπορούν να προστεθούν ή να παροπλιστούν. Όταν τα συστατικά αποτυγχάνουν , οι υπάρχοντες εξυπηρετητές μπορούν να υιοθετήσουν τον ρόλο

τους ή το σύστημα μπορεί να αναπτύξει νέους εξυπηρετητές. Όταν οι ουρές γεμίσουν ή αδειάσουν το δίκτυο μπορεί να αυξηθεί ή να μειωθεί αυτόματα.

Μηχανή πολλαπλών Cloud

Η μηχανή πολλαπλών Cloud αλληλεπιδρά με την διεπαφή προγραμματισμού εφαρμογών (API) και διαχειρίζεται τα ζητήματα διαφορετικών cloud. Αποτέλεσμα αυτού είναι οι οργανισμοί να μην εγκλωβίζονται σε κανένα cloud, απεναντίας είναι ελεύθεροι να επιλέγουν ανάμεσε σε διαφορετικούς παρόχους cloud, ή να μεταφέρουν μια εφαρμογή από το ένα cloud στο άλλο.

Πίνακας 4-5 Περιπτώσεις Χρήσης RightScale

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Περιπλοκότητα στην διαχείριση της υποδομής του Cloud	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την RightScale για να διαχειριστούν τις πολυπλοκότητες που προκύπτουν από την υλοποίηση υπηρεσιών υποδομής από έναν πάροχο. Αυτό επιφέρει αποδοτικότερη διαχείριση των υπηρεσιών και το χρόνου στην αγορά, καθώς ο οργανισμός μπορεί να επικεντρωθεί σε καίρια ζητήματα από το να μαθαίνει πώς να λειτουργεί μέσα στο περιβάλλον του παρόχου.	Πλατφόρμα διαχείρισης Cloud
Πλατφόρμα απλής διαχείρισης	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την RightScale για να διαχειριστούν και να συντηρούν υλοποιήσεις cloud μέσω μιας πλατφόρμας διαχείρισης. Αυτό επιφέρει αποδοτικότερη διαχείριση και μείωση του κόστους που σχετίζεται με το προσωπικό καθώς ο οργανισμός διευθύνει αποδοτικότερα τον αριθμό των απασχολούμενων στην διαχείριση της υλοποίησης cloud.	Πλατφόρμα διαχείρισης Cloud
Φορητότητα	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την RightScale για να διαχειριστούν τις διεπαφές προγραμματισμού εφαρμογών (API) και τα ιδιαίτερα ζητήματα κάθε cloud έτσι ώστε να επιλέγουν ελεύθερα ανάμεσα στην πληθώρα των παρόχων σύμφωνα με τις ανάγκες τους, να διαχειρίζονται και να μεταφέρουν εφαρμογές ανάμεσα σε διαφορετικά cloud (δημόσια ή ιδιωτικά) και να αποφεύγουν τον εγκλωβισμό τους.	Πλατφόρμα διαχείρισης Cloud

4.1.9 Salesforce.com (SaaS, PaaS)

Η Salesforce.com είναι πάροχος SaaS προϊόντων συστημάτων διαχείρισης πελατειακών σχέσεων (CRM) , επίσης προσφέρει και προϊόντα PaaS μέσω του Force.com. Το CRM της Salesforce.com διαιρείται σε διάφορες εφαρμογές και η χρέωση γίνεται ανα χρήστη.

Η Salesforce.com παρέχει υπηρεσίες PaaS μέσω του Force.com που επιτρέπει εξωτερικούς προγραμματιστές να δημιουργούν πρόσθετες εφαρμογές που ενοποιούνται μέσα στις βασικές εφαρμογές της Salesforce.com και φιλοξενούνται στις υποδομές της. Οι εφαρμογές δημιουργούνται με την γλώσσα

προγραμματισμού Apex, μια ιδιωτική γλώσσα για την πλατφόρμα του Force.com. Η χρέωση γίνεται ανά προγραμματιστή και υπάρχουν διάφορα πακέτα ανάλογα με το επίπεδο της αποθήκευσης, τις κλήσεις API κ.α. . Το AppExchange είναι ένας κατάλογος με εφαρμογές που δημιουργήθηκε για το Salesforce.com από τρίτους προγραμματιστές και οι χρήστες μπορούν να τις αγοράζουν και να τις προσθέτουν στα δικά τους περιβάλλοντα.

Πίνακας 4-6 Περιπτώσεις χρήσης της Salesforce.com

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Κατά απαίτηση CRM	Οι οργανισμοί μπορούν να χρησιμοποιήσουν το CRM της Salesforce.com για να διαχειριστούν να συγκεντρώσουν και να μοιραστούν αποδοτικά τις πληροφορίες των πελατών τους, χωρίς να επενδύσουν σε εσωτερική υποδομή.	CRM
Επέκταση της λειτουργικότητας στο CRM της Salesforce.com	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την Force.com για να αναπτύσσουν πρόσθετες εφαρμογές που επεκτείνουν την λειτουργικότητα του CRM της Salesforce.com ή να χρησιμοποιούν τον υπάρχον κατάλογο εφαρμογών του AppExchange χωρίς να επενδύσουν σε εσωτερική υποδομή.	Force.com, AppExchange
Ανάπτυξη Εφαρμογών	Οι οργανισμοί μπορούν να χρησιμοποιήσουν την πλατφόρμα της Force.com για να αναπτύξουν εφαρμογές που βασίζονται στο Force.com χωρίς να επενδύσουν σε εσωτερικές υποδομές.	Force.com

4.1.10 Ανοιχτή πλατφόρμα Cloud της Sun

Ως η εταιρεία που επινόησε την φράση “Το Δίκτυο είναι ο υπολογιστής” η Sun Microsystems οραματίζεται έναν κόσμο με πολλά cloud, δημόσια και ιδιωτικά που να είναι ανοιχτά και συμβατά μεταξύ τους. Σύμφωνα με την οπτική της Sun υπάρχουν πολλοί διαφορετικοί τύποι cloud και πολλές διαφορετικές εφαρμογές που μπορούν να αναπτυχθούν χρησιμοποιώντας τους. Το πλάνο της Sun είναι να προσφέρει ένα εκτεταμένο σύνολο προϊόντων (υλικού και λογισμικού) και υπηρεσιών κάτω από την ομπρέλα μιας “Ανοιχτής Πλατφόρμας Cloud” για να προωθήσει τις ανοιχτές κοινότητες και τα οικοσυστήματα των συνεργατών της. Σύμφωνα με την Sun η Ανοιχτή Πλατφόρμα Cloud είναι μια ανοιχτή αρχιτεκτονική (API, ανοιχτές τυποποιήσεις) και υποδομές που περιλαμβάνουν τεχνολογίες όπως Java, MySQL, OpenSolaris και ανοιχτό λογισμικό αποθήκευσης. Η Sun πιστεύει ότι η Ανοιχτή Πλατφόρμα Cloud που προσφέρει θα ενοποιήσει ένα οικοσύστημα συνεργατών, προγραμματιστών και άλλων γιατί το cloud computing μπορεί να είναι πετυχημένο μόνο αν μπορείς να πετύχεις την μέγιστη επαναχρησιμοποίηση άλλων τεχνολογιών και συστατικών.

Σύμφωνα με την Sun, η Ανοιχτή Πλατφόρμα Cloud προσφέρει όλα τα απαραίτητα συστατικά (υλικό, λογισμικό, και δυνατότητες διαχείρισης) για να βοηθήσει τους πελάτες και τους συνεργάτες της που σκοπεύουν να γίνουν πάροχοι οποιοδήποτε μοντέλου cloud (SaaS, PaaS, IaaS). Η Sun δουλεύει με παρόχους υπηρεσιών και

επιχειρήσεις που θέλουν να δημιουργήσουν το δικό τους Cloud για να εξυπηρετούν τους πελάτες και τους χρήστες τους.

Ένας από τους παράγοντες που οδηγούν το Cloud είναι η μεγάλη διαθεσιμότητα λογισμικού ανοιχτού κώδικα και συστατικών. Οι προγραμματιστές μπορούν γρήγορα να συνθέσουν εφαρμογές από συστατικά ανοιχτού κώδικα και να τις λειτουργούν στο Cloud. Η Sun έχει αναπτύξει θεμελιώδεις τεχνολογίες (υλικού και λογισμικού) για να υποστηρίξει τα τρία μοντέλα του Cloud : δημόσια, ιδιωτικά, υβριδικά .

Στις τεχνολογίες αυτές συμπεριλαμβάνονται τα : OpenSolaris, MySQL, ο ανοιχτού λογισμικού εξυπηρετητής εφαρμογών GlassFish, το Crossbow, ο xVM επόπτης της Sun(βασισμένος στο ανοιχτού λογισμικού Xen),το σύστημα αρχείων ZFS (Solaris Zeta files), το xVM VirtualBox της Sun, και το ολοκληρωμένο περιβάλλον ανάπτυξης NetBeans. Το χαρτοφυλάκιο υλικού της Sun περιλαμβάνει εξυπηρετητές βασισμένους στην οικογένεια X86, SPARC, UltraSPARC επεξεργστές, και ανοιχτή αποθήκευση.

Πίνακας 4-7 Περιπτώσεις χρήσης της Sun

Περίπτωση Χρήσης	**Περιγραφή**	**Υπηρεσία/ες**
Υψηλής απόδοσης Υπολογιστική	Οργανισμοί που έχουν απαιτήσεις υψηλής υπολογιστικής μπορούν να χρησιμοποιήσουν την ανοιχτή πλατφόρμα Cloud της Sun για να επεξεργαστούν μεγάλες ποσότητες δεδομένων.	Ανοιχτή Πλατφόρμα Cloud της Sun, υπηρεσίες ιδιωτικού Cloud
Ανάπτυξη και δοκιμές	Οργανισμοί, εταιρίες στο ξεκίνημα τους, προγραμματιστές κοινωνικών δικτύων και επιχειρήσεις μπορούν να χρησιμοποιήσουν της ανοιχτές δημόσιες υπηρεσίες cloud της Sun και τα ανοιχτά συστατικά για να αναπτύξουν εφαρμογές σε Java, Ruby, Python και MySQL.	Sun Cloud, Netbeans, VirtualBox

4.1.11 GoGrid (IaaS)

Η GoGrid είναι πάροχος υποδομής ως υπηρεσία στο Cloud. Η διαχείριση και διαμόρφωση της υποδομής στην GoGrid είναι παρόμοια με την διαχείριση της υποδομής σε ένα εταιρικό κέντρο δεδομένων ή έναν τοπικό πάροχο υπηρεσιών. Η υποδομή της GoGrid είναι προσβάσιμη και λειτουργική με την χρήση βασικών πρωτόκολλων δικτύου και διευθύνσεων IP μέσω του διαδικτύου, χωρίς να απαιτούνται νέες ικανότητες ή εξοπλισμός.

Με τις υπηρεσίες της GoGrid ο πελάτης μπορεί αυτόματα να τροφοδοτηθεί με υποδομές υλικού μέσω του διαδικτύου, χωρίς μακροχρόνιες δεσμεύσεις και με την ευελιξία να δημιουργεί φιλοξενούμενες υποδομές στο cloud σύμφωνα με τις ανάγκες του. Με την χρήση μιας διαδικτυακής διεπαφής ή ενός API μπορεί να εφοδιαστεί εικονικούς και φυσικούς εξυπηρετητές, αποθήκευση, εξισορρόπηση φόρτου εργασιών και ασφάλεια σε πραγματικό χρόνο και σε πολλαπλά κέντρα δεδομένων. Η χρέωση γίνεται με βάση τους πόρους που χρησιμοποιήθηκαν.

Η GoGrid υποστηρίζεται από τα πιο ισχυρά και λεπτομερή πιστοποιητικά SLA, και συμπεριλαμβάνει ένα πλούσιο οικοσύστημα συνεργατών που προσφέρουν προ-ρυθμισμένες και έτοιμες προς χρήση εμπορικές εφαρμογές. Επιπλέον η GoGrid παρέχει ευέλικτη υβριδική φιλοξενία, που επιτρέπει σε πραγματικό χρόνο την κάλυψη των αναγκών σε υποδομές. Έτσι επιταχύνει τον χρόνο εισόδου στην αγορά και μειώνει το κόστος της υποδομής χωρίς να κλειδώνει τους πελάτες της στις υπηρεσίες της.

4.2 Ανοιχτές Πλατφόρμες Cloud

Για τις ανάγκες της πτυχιακής εργασίας κρίθηκε απαραίτητη η υλοποίηση ενός Cloud εντός του δικτύου του Α-ΤΕΙΘ βασισμένο σε λογισμικό ανοιχτού κώδικα. Η επιλογή της κατάλληλης πλατφόρμας για την δεδομένη χρονική περίοδο έγινε ανάμεσα στους βασικότερους πρωταγωνιστές : Ubuntu Cloud , OpenNedula και Eucalyptus.

4.2.1 Ubuntu Cloud

Η Ubuntu προσφέρει εργαλεία και υπηρεσίες που καλύπτουν όλες τις ανάγκες για Cloud. Εύκολη και γρήγορη υλοποίηση ιδιωτικού cloud και δυνατότητα μεταφοράς του φόρτου εργασίας από το ιδιωτικό cloud στο δημόσιο όταν αυτό είναι απαραίτητο.

Μερικά από τα πλεονεκτήματα του Ubuntu Cloud είναι:

- Εξελιγμένα εργαλεία διαχείρισης βοηθούν στην υλοποίηση, και διαχείριση υπηρεσιών σε ελάχιστο χρόνο
- Συνεχές πρόγραμμα νέων εκδόσεων παρέχει διαρκώς τις πιο επίκαιρες και ενημερωμένες εφαρμογές και υπηρεσίες Cloud
- Στενή συνεργασία μεταξύ της Ubuntu και της OpenStack παρέχει στους χρήστες την δυνατότητα ανάπτυξης νέων υπηρεσιών εύκολα και γρήγορα
- Βασιζόμενο σε πρότυπα και ευρέως υποστηριζόμενο το Ubuntu Cloud δεν εγκλωβίζει σε έναν μόνο προμηθευτή

4.2.2 OpenNedula

Το OpenNedula είναι ένα ανοιχτού λογισμικού βιομηχανικό πρότυπο για εικονικά κέντρα δεδομένων και προσφέρει την πιο ευέλικτη και πλήρη σε χαρακτηριστικά λύση για την ολοκληρωμένη και πλήρη διαχείριση εικονικών κέντρων δεδομένων υλοποιώντας IaaS Cloud σε υπάρχουσες υποδομές. Η διαλειτουργικότητα του OpenNedula εξελίσσει τους υφιστάμενους πόρους προστατεύοντας τις επενδύσεις και αποφεύγοντας το κλείδωμα στους προμηθευτές.

Το OpenNedula μπορεί να χρησιμοποιηθεί πρωτίστως ως εργαλείο εικονικότητας για την διαχείριση εικονικών κέντρων δεδομένων ή cluster το όποιο αναφέρεται ως Ιδιωτικό Cloud. Το OpenNedula υποστηρίζει το Υβριδικό Cloud για να συνδυάσει τις τοπικές υποδομές με δημόσιες υποδομές Cloud παρέχοντας πολύ ευέλικτα

περιβάλλοντα φιλοξενίας. Το OpenNedula υποστηρίζει επίσης το δημόσιο Cloud παρέχοντας διεπαφές Cloud επεκτείνοντας την λειτουργικότητα του για εικονικές μηχανές, αποθήκευση και διαχείριση δικτύου.

4.2.3 Open Eucalyptus

Το Eucalyptus υλοποιεί ένα ιδιωτικό Cloud τύπου IaaS με τις υπάρχουσες υποδομές του οργανισμού το οποίο είναι προσβάσιμο μέσω μιας διεπαφής συμβατής με το Amazon EC2 και Amazon S3 . Αυτή η συμβατότητα επιτρέπει στο Eucalyptus να μετατραπεί σε υβριδικό cloud ικανό να αντλήσει υπολογιστικούς πόρους από ένα δημόσιο Cloud. Επιπλέον το Eucalyptus είναι συμβατό με μια πληθώρα εργαλείων και εφαρμογών που τηρούν τα πρότυπα του Amazon.

Μερικά από τα χαρακτηριστικά του Eucalyptus είναι :

Ανοιχτού κώδικά

> Το Eucalyptus είναι λογισμικό ανοιχτού κώδικα που επιτρέπει την τροποποίηση του, την αναδιανομή του, την ανοιχτή διαδικασία ανάπτυξης του και την αναφορά σφαλμάτων στην κοινότητα.

Διαρθωτό

> Τα συστατικά του Eucalyptus ακολουθούν έναν διαρθωτό σχεδιασμό μέσω αυστηρά καθορισμένων διεπαφών

Κατανεμημένο

> Το Eucalyptus επιτρέπει στα συστατικά του να εγκατασταθούν σύμφωνα με τους απαιτούμενος πόρους. Για παράδειγμα το Walrus μπορεί να εγκατασταθεί κοντά στο σύστημα αποθήκευσης ενώ ο ελεγκτής του cluster κοντά στο cluster που θα διαχειρίζεται.

Σχεδιασμένο να αποδίδει

> Το Eucalyptus έχει σχεδιαστεί από μηδενική βάση ώστε να μπορεί να επιτυγχάνει την βέλτιστη απόδοση σε διάφορα περιβάλλοντα.

Ευέλικτο

> Το Eucalyptus είναι ευέλικτο και μπορεί να εγκατασταθεί σε ένα σύστημα με ελάχιστες απαιτήσεις ή σε ένα σύστημα με εκατοντάδες πυρήνες και terabytes αποθηκευτικού χώρου.

Συμβατό

> Το Eucalyptus είναι συμβατό με συμβατό με τις πιο διαδεδομένες διεπαφές Cloud όπως το Amazon EC2 και το S3. Η σχεδίαση του Eucalyptus επιτρέπει οποιαδήποτε άλλη διεπαφή να υλοποιηθεί αλλά μέχρι σήμερα καμιά άλλη διεπαφή δεν είναι τόσο ολοκληρωμένη όσο του Amazon.

Ανεξάρτητο Επόπτη

Το Eucalyptus είναι σχεδιασμένο ώστε να υποστηρίζει τους περισσότερους διαθέσιμους επόπτες, παρέχει πλήρη υποστήριξη για τους επόπτες KVM και Xen και επιπλέον στην έκδοση Enterprise υποστηρίζει και τον ιδιόκτητο επόπτη VMware.

Υβριδικό Cloud

Όλα τα παραπάνω χαρακτηριστικά κάνουν το Eucalyptus ένα εύκολα υλοποιήσιμο υβριδικό Cloud. Ένα υβριδικό Cloud συνδυάζει πόρους από πολλαπλά Cloud συνήθως από ένα ιδιωτικό και ένα δημόσιο. Η συμβατότητα του Eucalyptus με το EC2 της Amazon επιτρέπει την υλοποίηση ενός υβριδικού Cloud με το μεγαλύτερο δημόσιο διαθέσιμο cloud.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό παρουσιάστηκαν οι μεγαλύτεροι πάροχοι cloud και οι υπηρεσίες τους, παρουσιάστηκαν επίσης πλατφόρμες cloud ανοιχτού κώδικα. Στο επόμενο κεφάλαιο θα υλοποιηθεί ένα cloud computing με τις υποδομές του Τμήματος Πληροφορικής.

ΚΕΦΑΛΑΙΟ 5

Πειραματική Υλοποίηση

5.1 Επιλογή πλατφόρμας Cloud και διαθέσιμη υποδομή

Η τελική επιλογή πλατφόρμας για την υλοποίηση του Cloud εντός του δικτύου του ΑΤΕΙΘ ήταν η πλατφόρμα Eucalyptus και το τμήμα Πληροφορικής διέθεσε δύο υπολογιστές για την υλοποίηση αυτή.

Ο ένας υπολογιστής ήταν τελευταίας γενεάς με τα εξής τεχνικά χαρακτηριστικά :

Computer

Processor 4x Intel(R) Core(TM) i5 CPU 750 @ 2.67GHz

Memory 4056MB (787MB used)

Operating System

Version Kernel Linux 2.6.32-5-amd64 (x86_64)

Compiled #1 SMP Wed Jan 12 05:14:59 UTC 2011

C Library GNU C Library version 2.11.2 (stable)

Default C Compiler Unknown

Distribution Debian GNU/Linux 6.0.1

Current Session

Computer Name Eucalyptus-Node1

Ενώ ο δεύτερος ήταν ένας παροπλισμένος υπολογιστής από τα εργαστήρια του τμήματος με τα εξής τεχνικά χαρακτηριστικά :

Computer

Processor 2x Intel(R) Pentium(R) 4 CPU 3.20GHz

Memory 514MB (281MB used)

Operating System

Version Kernel Linux 2.6.32-5-686 (i686)

Compiled #1 SMP Wed Jan 12 04:01:41 UTC 2011

C Library GNU C Library version 2.11.2 (stable)

Default C Compiler Unknown

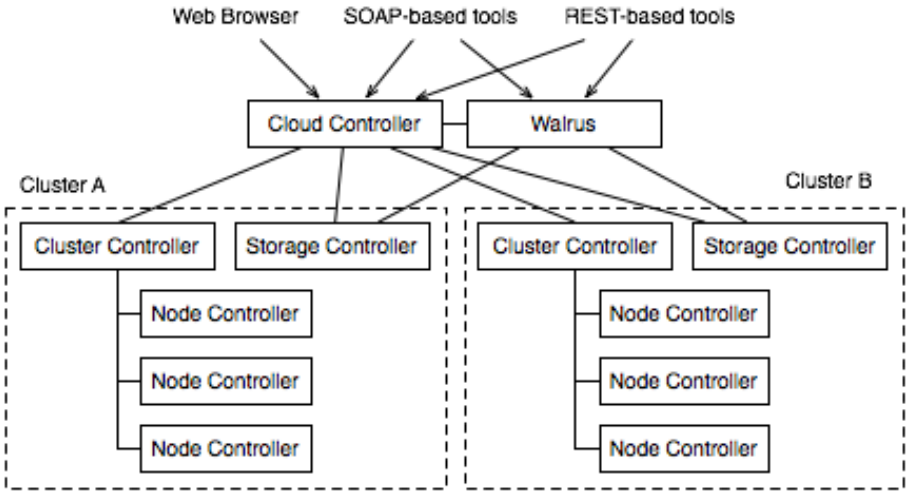
Distribution Debian GNU/Linux 6.0.1

Current Session

Computer Name Eucalyptus-Front-End

5.2 Εγκαθιστώντας το Eucalyptus

Εικόνα 5.1 δομή του Eucalyptus



Η εγκατάσταση του Eucalyptus αποτελείται από πέντε συστατικά μέρη. Ο Cloud Controller (CLC) – ελεγκτής του Cloud και ο “Walrus” είναι συστατικά υψηλού επιπέδου. Ο Cloud Controller είναι ένα πρόγραμμα γραμμένο σε Java που παρέχει διεπαφές SOAP και ερωτημάτων συμβατά κατά EC2 καθώς και μια διεπαφή Web μας τον έξω κόσμο. Επιπλέον για να χειριστεί εισερχόμενα αιτήματα ο Cloud Controller πραγματοποιεί υψηλού επιπέδου προγραμματισμό πόρων. Και ο Walrus είναι μας γραμμένος σε Java και είναι διαθέσιμος εντός και εκτός Cloud μέσω των διεπαφών SOAP και REST που είναι συμβατές με το S3 μας Amazon.

Τα συστατικά υψηλού επιπέδου μπορούν να συναθροίζουν πόρους από πολλά cluster, κάθε cluster χρειάζεται έναν cluster controller (CC), για προγραμματισμό σε επίπεδο cluster και έλεγχο δικτύου, καθώς και έναν Storage Controller (SC) για αποθήκευση. Οι δύο ελεγκτές επιπέδου cluster συνήθως αναπτύσσονται στον κεντρικό κόμβο μας cluster. Κάθε κόμβος με έναν επόπτη χρειάζεται έναν node controller (NC) για να ελέγχει τον επόπτη. Ο CC και ο NC είναι γραμμένοι με την γλώσσα C και έχουν αναπτυχθεί ως διαδικτυακή υπηρεσία μέσα στον Apache, ο SC είναι γραμμένος με Java. Η επικοινωνία μεταξύ αυτών των συστατικών λαμβάνει χώρα μέσω SOAP με WS ασφάλεια.

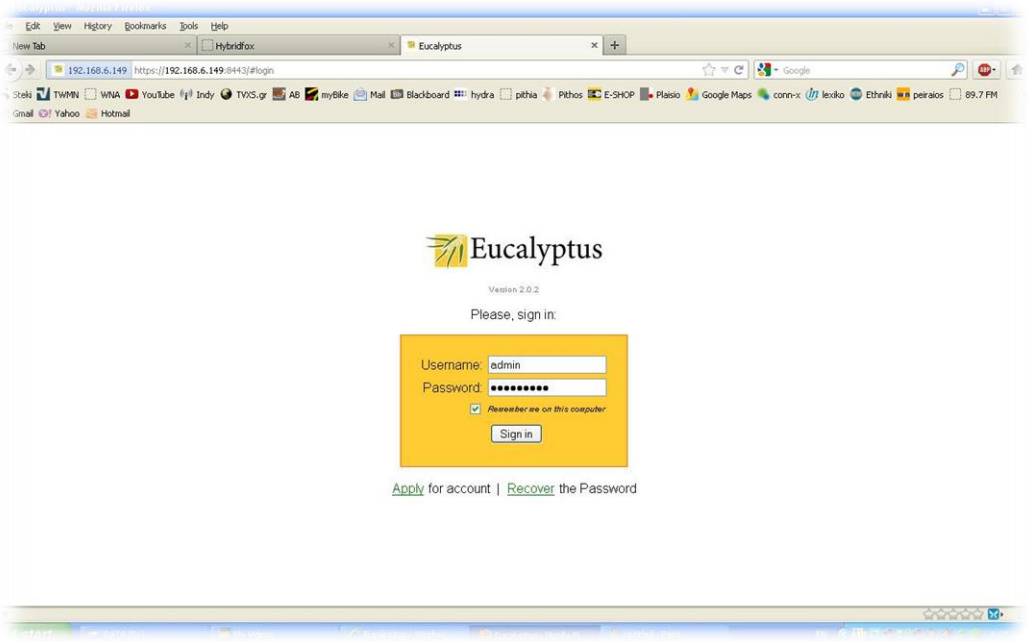
Η τυπική εγκατάσταση του Eucalyptus περιλαμβάνει εγκατάσταση μας απλού cluster όπου όλα τα συστατικά εκτός του NC τοποθετούνται σε ένα μηχάνημα που αναφέρεται ως Front-End. Όλα τα άλλα μηχανήματα τρέχουν μόνο τον NC και αναφέρονται ως nodes. Σε πιο προχωρημένες εγκαταστάσεις μας πχ με πολλαπλούς Cluster Controller ή με τον Walrus να αναπτύσσεται ξεχωριστά ως Front-End αναφέρεται μόνο το μηχάνημα που τρέχει τον Cloud Controller.

Για περαιτέρω τεχνικές λεπτομέρειες σχετικά με την εγκατάσταση του Eucalyptus ο αναγνώστης καλείται να επισκεφτεί την ιστοσελίδα http://open.eucalyptus.com/wiki/IntroducingEucalyptus_v2.0 καθώς οι λεπτομέρειες αυτές ξεφεύγουν από τον σκοπό μας παρούσας εργασίας.

5.2 Επιτυχής εγκατάσταση και δοκιμαστική λειτουργία

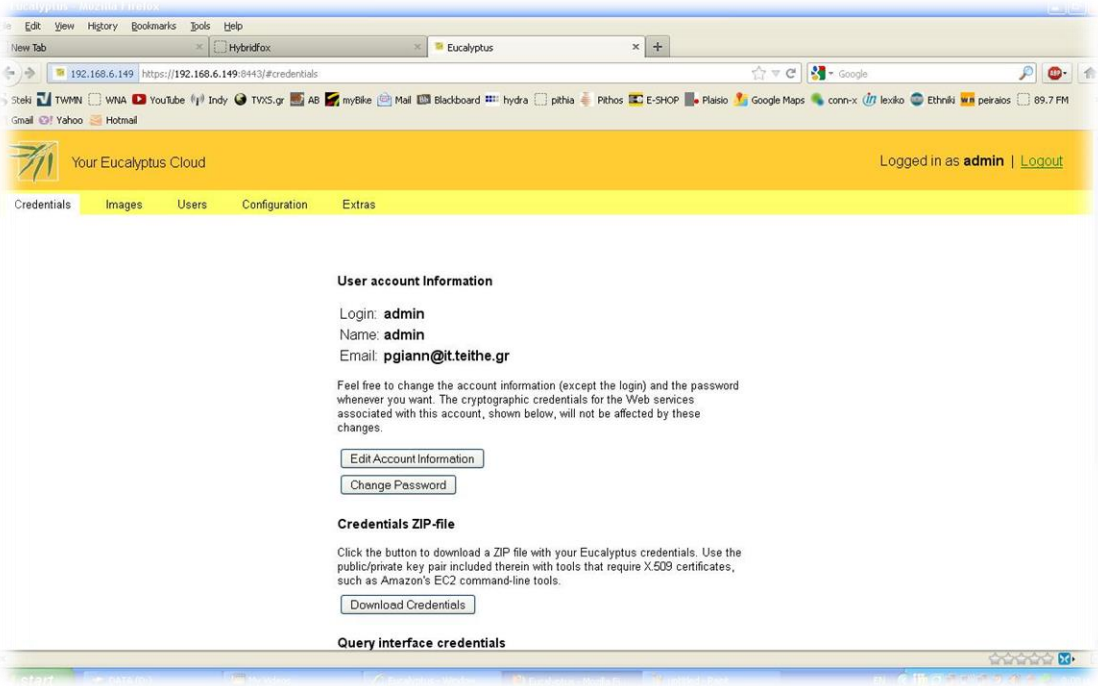
Σε αυτή την φάση το Eucalyptus έχει εγκατασταθεί με επιτυχία και η πρώτη επαφή θα γίνει μέσω μιας διεπαφής web που μας δίνει την δυνατότητα να ρυθμίσουμε διάφορες παραμέτρους του συστήματος καθώς και να δούμε πληροφορίες σχετικά με αυτό. Η διεπαφή αυτή είναι διαθέσιμη στην διεύθυνση https://ip-tou-FrontEnd-μηχανήματος:8443 όπου θα χρειαστεί να διαθέτουμε έναν ενεργό λογαριασμό χρήστη για να εισέλθουμε.

Εικόνα 5.2 διεπαφή web

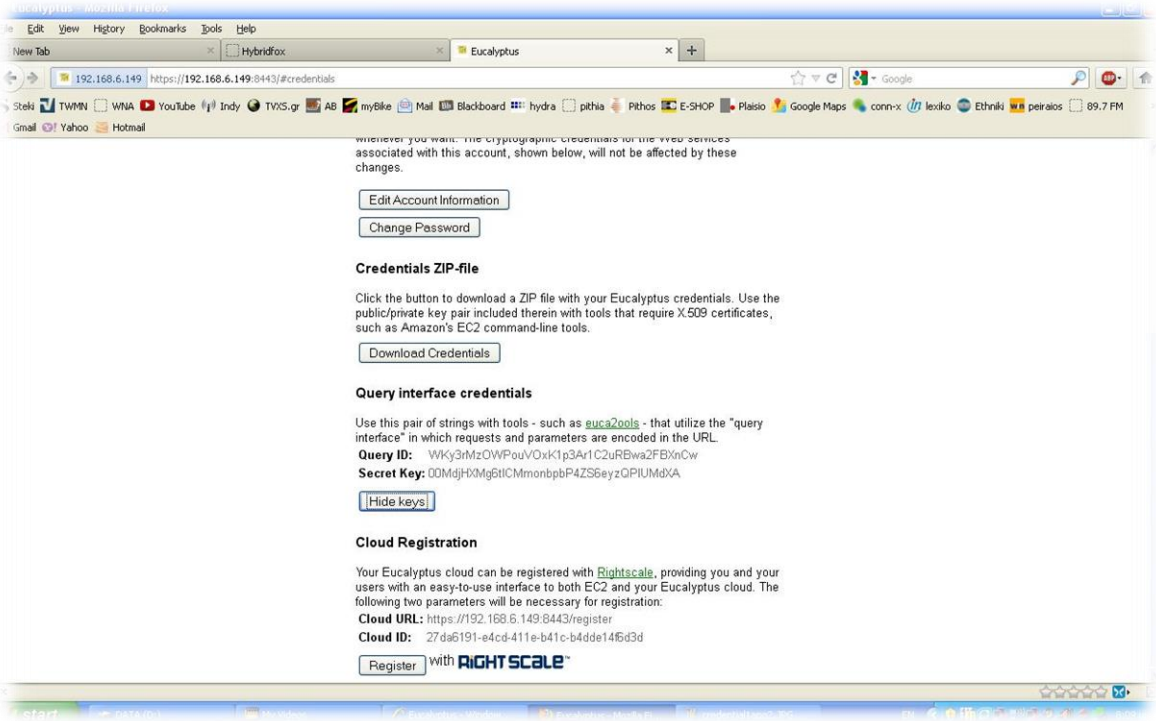


Μετα την επιτυχή εισαγωγή η πρώτη καρτέλα της διεπαφής μας ενημερώνει για τις πληροφορίες του λογαριασμού με τον οποίον έχουμε εισέλθει και για τα διαπιστευτήρια τα οποία είναι απαραίτητα σε ορισμένες λειτουργίες.

Εικόνα 5.3 Credentials

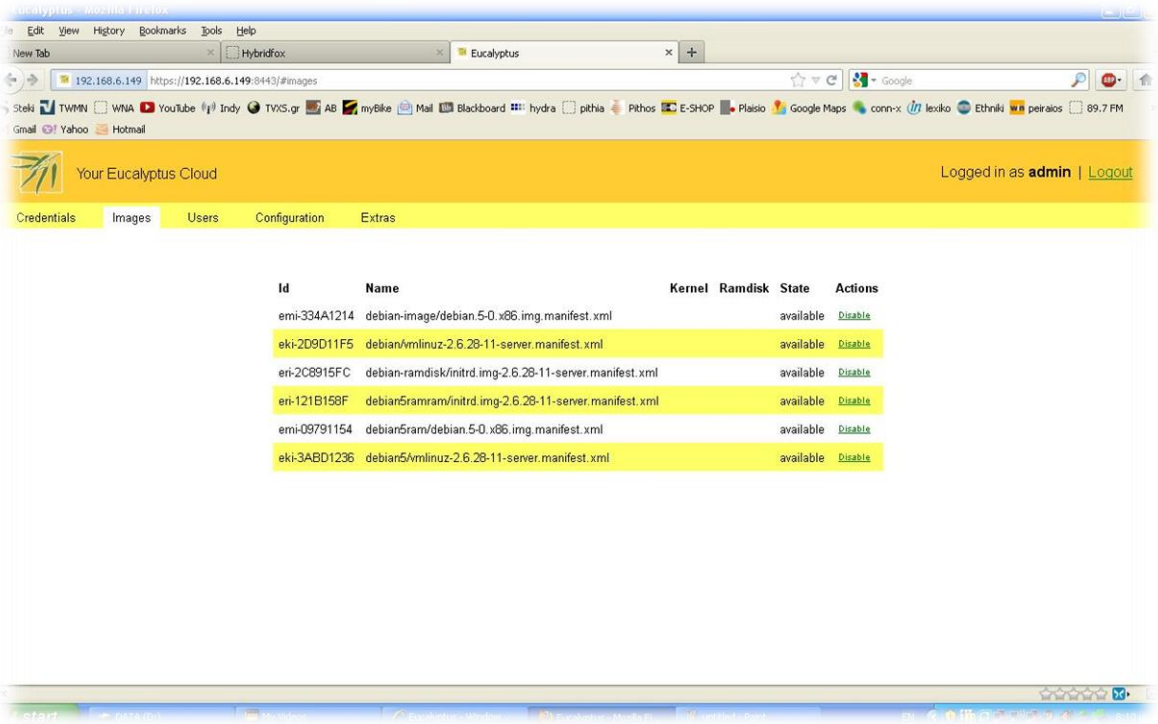


Εικόνα 5.4 Credentials



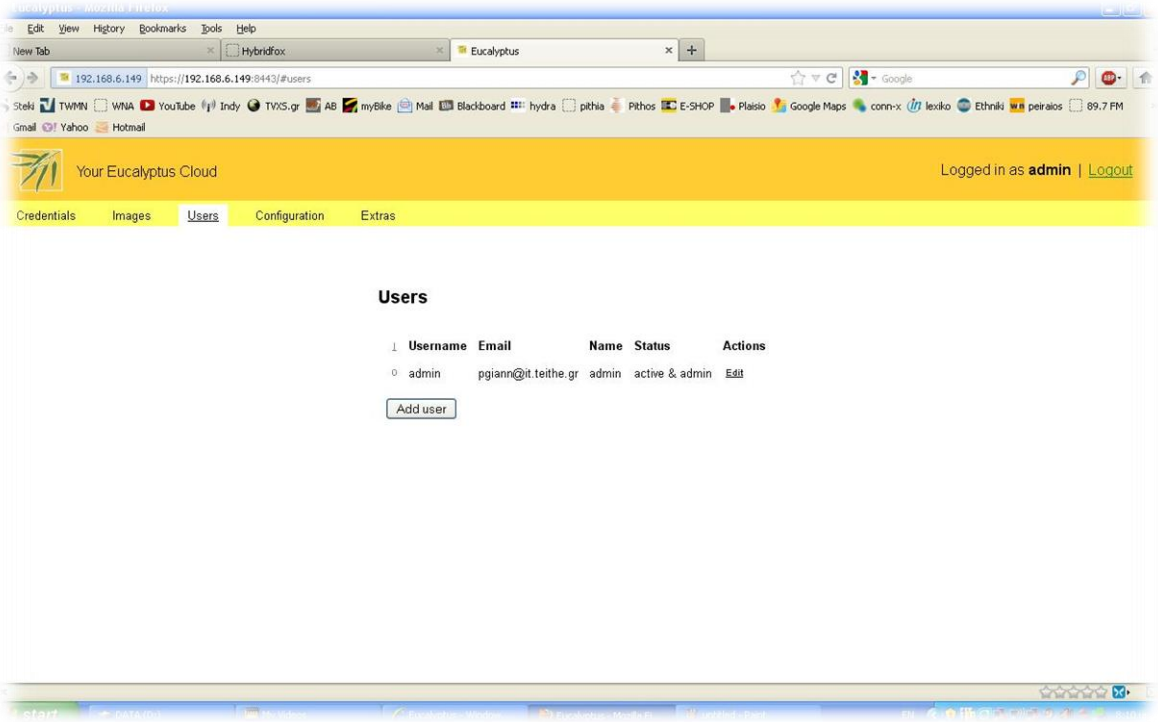
Στην επόμενη καρτέλα βλέπουμε πληροφορίες σχετικά με τα διαθέσιμα εικονικά συστήματα που υπάρχουν ήδη στο cloud μας ενώ δυνατότητα για εγγραφή νέων εικόνων δίνεται στους χρήστες ανάλογα με τον λογαριασμό που διαθέτουν.

Εικόνα 5.5 Images



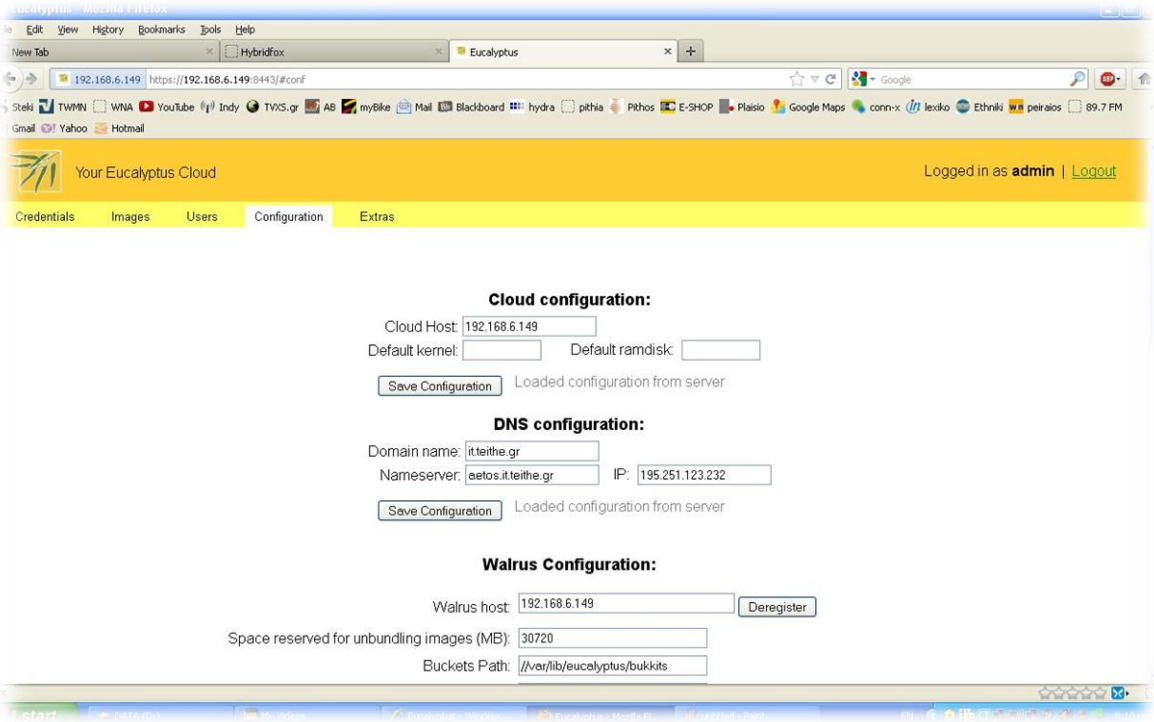
Στην επόμενη καρτέλα βλέπουμε πληροφορίες σχετικά με τους χρήστες που είναι εγγεγραμμένοι στο cloud και επίσης μπορούμε να επεξεργαστούμε τα στοιχειά των λογαριασμών.

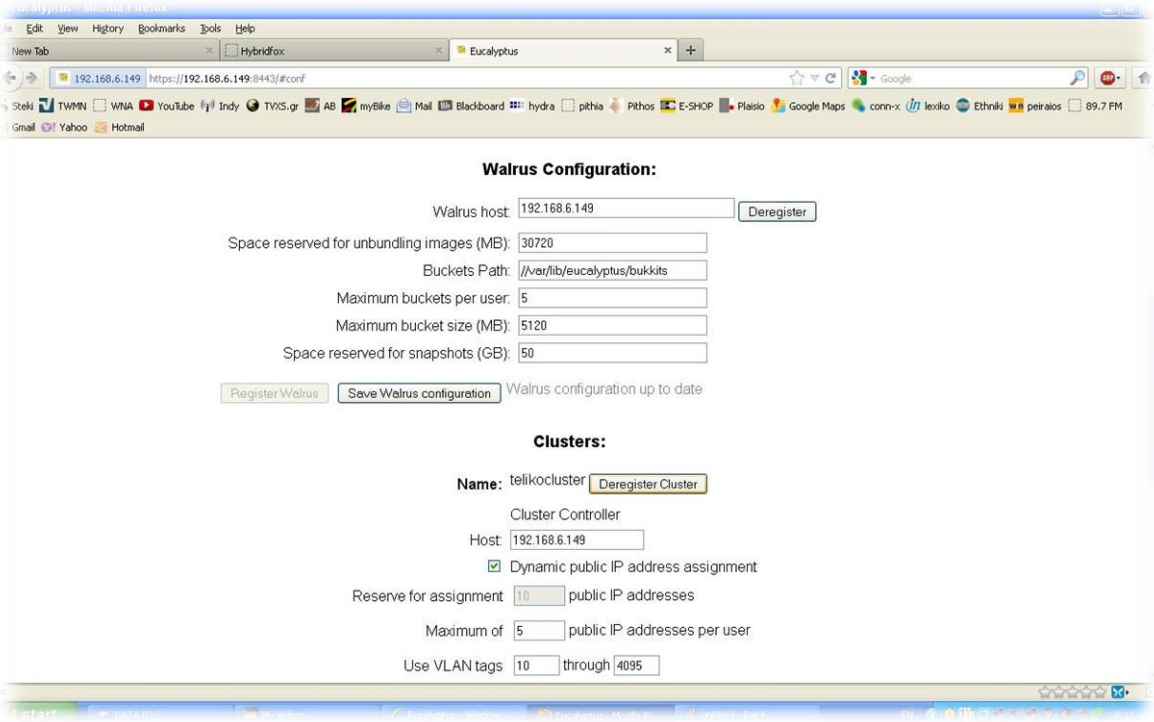
Εικόνα 5.6 Users

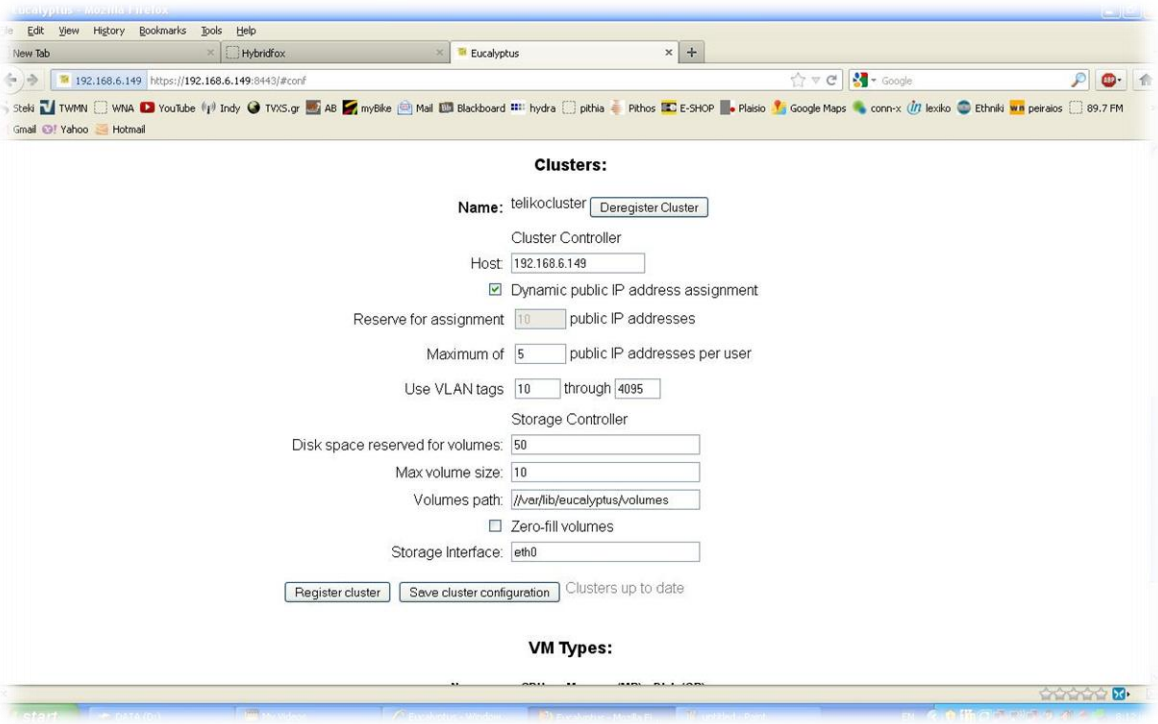


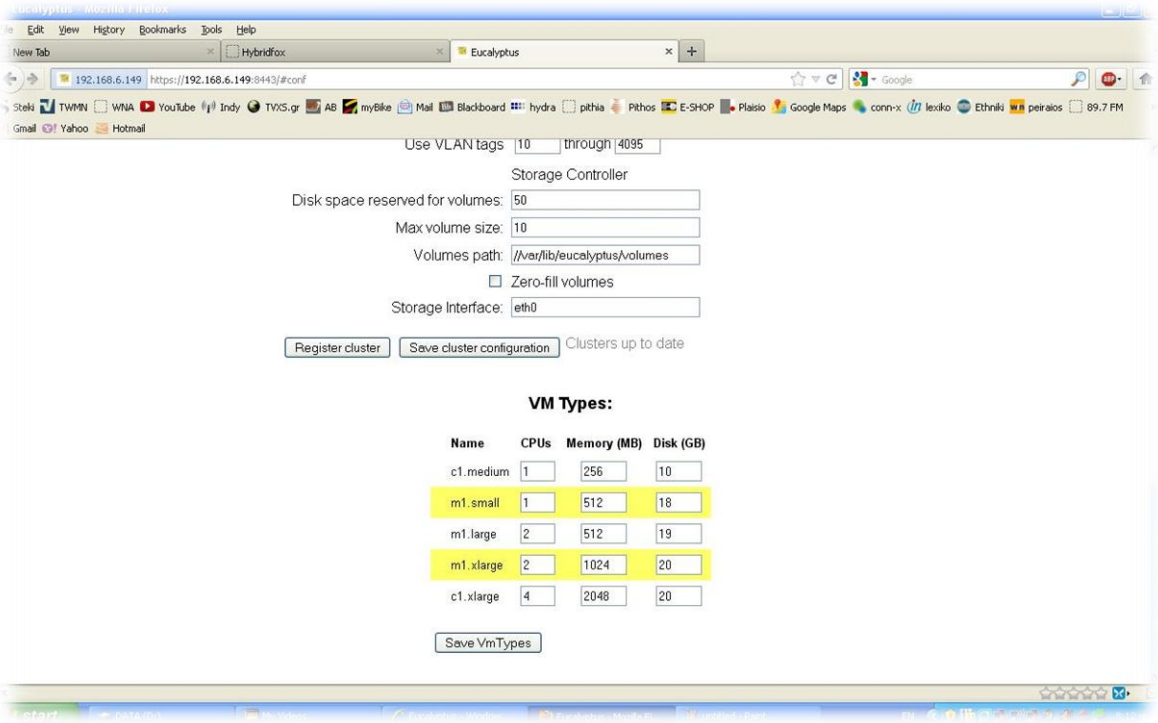
Η επόμενη καρτέλα μας δίνει πληροφορίες σχετικά με τις ρυθμίσεις του cloud μας και επιπλέον την δυνατότητα να αλλάξουμε αρκετές από αυτές μέσω της διαπεφής χωρίς να χρειαστεί να γίνει μέσω της γραμμής εντολών.

Εικόνα 5.7 Configuration



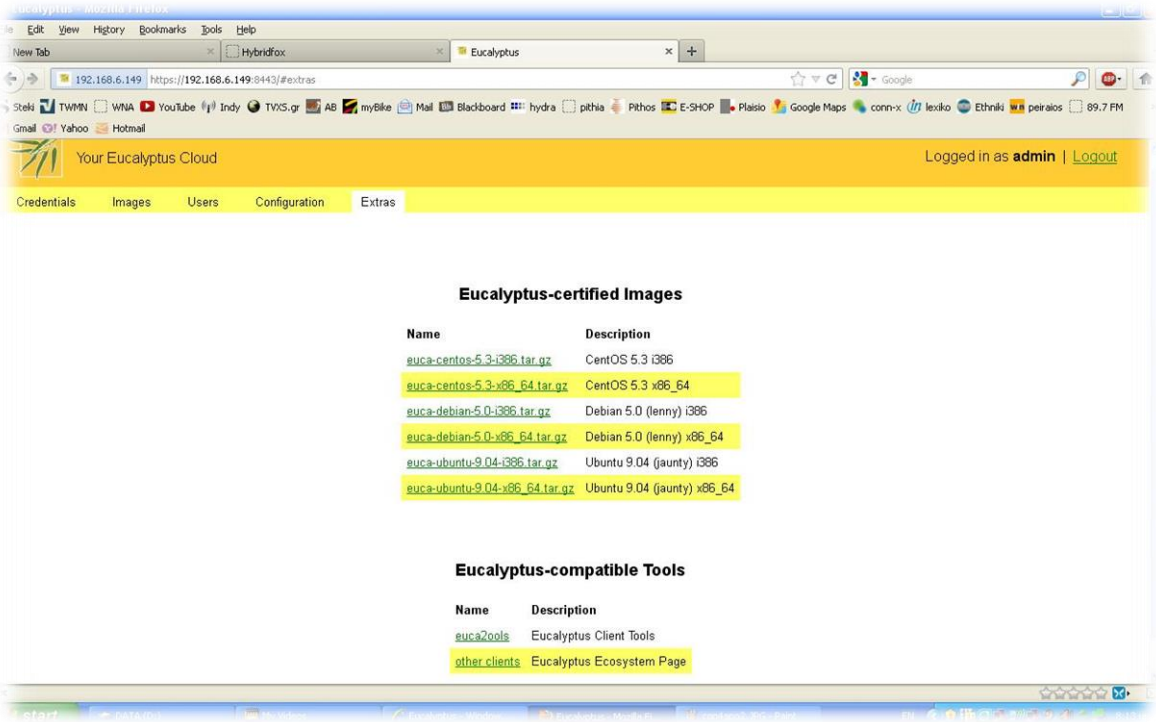






Τέλος η καρτέλα extras μας δίνει πληροφορίες σχετικά με τις έτοιμες εκδόσεις εικόνων που παρέχει το Eucalyptus καθώς και εργαλεία διαχείρισης συμβατά με αυτό.

Εικόνα 5.8 Extras

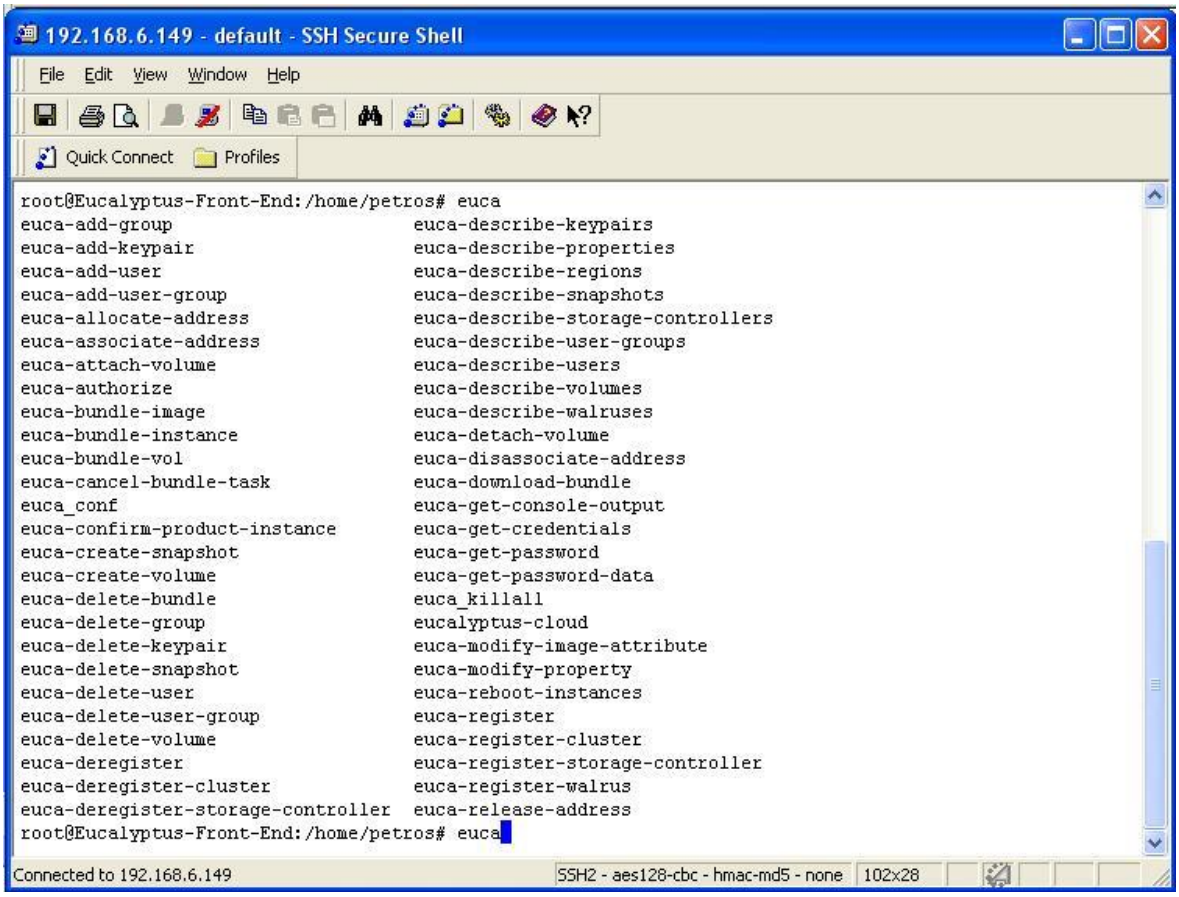


5.3 Euca2ools

Το μεγαλύτερο μέρος της διαχείρισης πραγματοποιείται μέσω της γραμμής εντολών και με την βοήθεια του Euca2ools. Από την διεπαφή web που αναλύθηκε πιο πάνω ο χρήστης πρέπει να κατεβάσει τα διαπιστευτήρια x509 και να τα προσθέσει στις μεταβλητές περιβάλλοντος του προκειμένου να έχει πρόσβαση στις εντολές του Euca2ools.

Το σύνολο των εντολών που μας παρέχει το Euca2ools φαίνεται στην παρακάτω εικόνα :

Εικόνα 5.9 Εντολές Euca2ools



Ωστόσο θα περιγραφούν μόνο οι βασικότερες εντολές για να ξεκινήσει κάποιος να λειτουργεί ένα εικονικό λειτουργικό. Για περαιτέρω μελέτη πάνω στο Euca2ools ο αναγνώστης παραπέμπεται στο http://open.eucalyptus.com/wiki/Euca2oolsGuide .

Ερωτήματα στο Σύστημα

Οι παρακάτω εντολές επιτρέπουν να λαμβάνουμε πληροφορίες από το σύστημα σχετικά με τα διαθέσιμα εικονικά λειτουργικά, τα στιγμιότυπα που τρέχουν, τις διαθέσιμες ζώνες και τα διαθέσιμα κλειδιά:

euca-describe-images
euca-describe-instances
euca-describe-availability-zones το αποτέλεσμα της εντολής στο δικά μας σύστημα βλέπουμε παρακάτω :

```
root@Eucalyptus-Front-End:/home/petros# euca-describe-availability-zones
verboseAVAILABILITYZONE        telikocluster   192.168.6.149

AVAILABILITYZONE        |- vm types     free / max     cpu   ram  disk
AVAILABILITYZONE        |- c1.medium   0004 / 0004   1    256    10
AVAILABILITYZONE        |- m1.small     0004 / 0004   1    512    18
AVAILABILITYZONE        |- m1.large     0002 / 0002   2    512    19
AVAILABILITYZONE        |- m1.xlarge    0002 / 0002   2   1024    20
```

AVAILABILITYZONE |- c1.xlarge 0001 / 0001 4 2048 20

euca-describe-keypairs

Δημιουργώντας κλειδιά

Τα ζευγάρια κλειδιών χρησιμοποιούνται στο Eucalytpus για να αυθεντικοποιήσουν την ταυτότητα ενός χρήστη. Πρώτου τρέξει ένα στιγμιότυπο θα πρέπει να έχει δημιουργηθεί ένα ζεύγος κλειδιών όπως φαίνεται στην παρακάτω εντολή :

euca-add-keypair mykey | tee mykey.private

Ένα ζεύγος δημιουργείται με το δημόσιο κλειδί να αποθηκεύεται στο Eucalyptus και ένα ιδιωτικό αποθηκεύεται στο mykey.private και εκτυπώνεται στην στάνταρ έξοδο. Ο ssh client απαιτεί αυστηρά δικαιώματα στο ιδιωτικό κλειδί :

chmod 0600 mykey.private

Θέτοντας σε λειτουργία ένα εικονικό σύστημα:

Έχοντας δημιουργήσει το ζεύγος κλειδιών μπορούμε να θέσουμε σε λειτουργία ένα από τα εικονικά συστήματα που μας παρέχονται από το cloud:

euca-run-instances -k mykey -n <number of instances to start> <emi-id>

Για να εισέρθουμε στο σύστημα που μόλις δημιουργήσαμε χρησιμοποιούμε την εντολή:

ssh -i mykey.private root@<accessible-instance-ip>

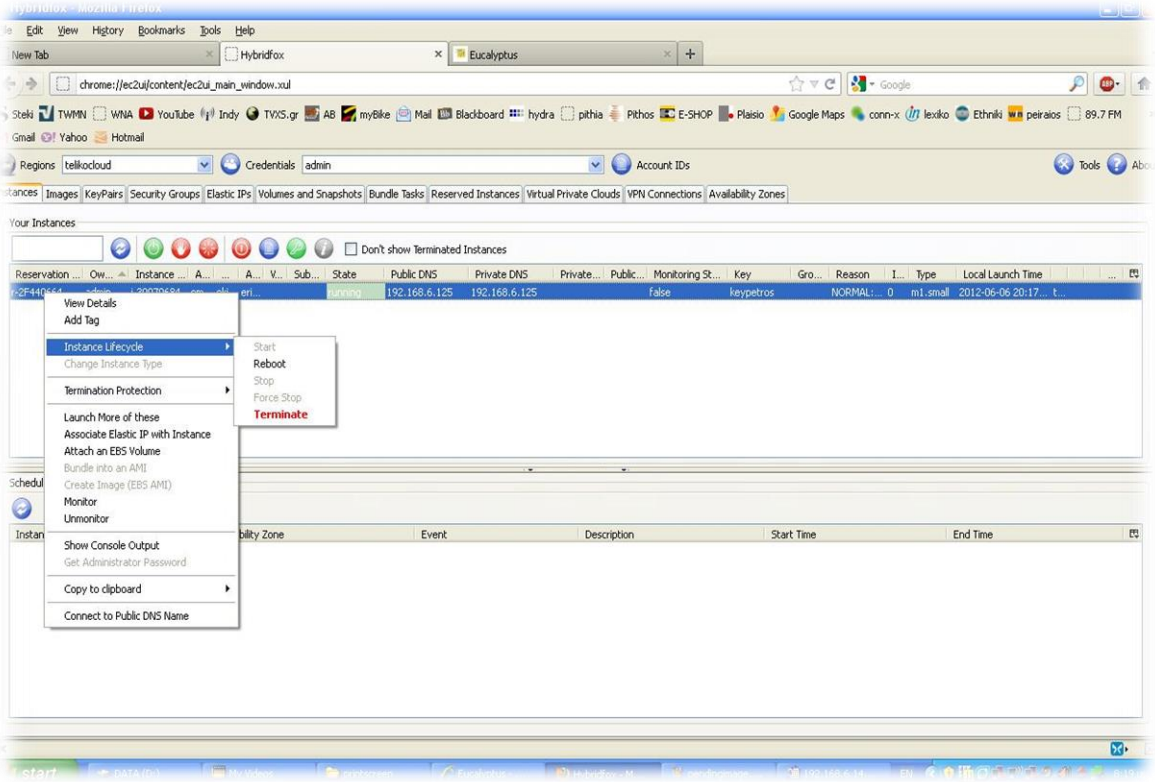
και για να τερματίσουμε κάποιο στιγμιότυπο :

euca-terminate-instances <instance-id1> <instance-id2>... <instance-idn>

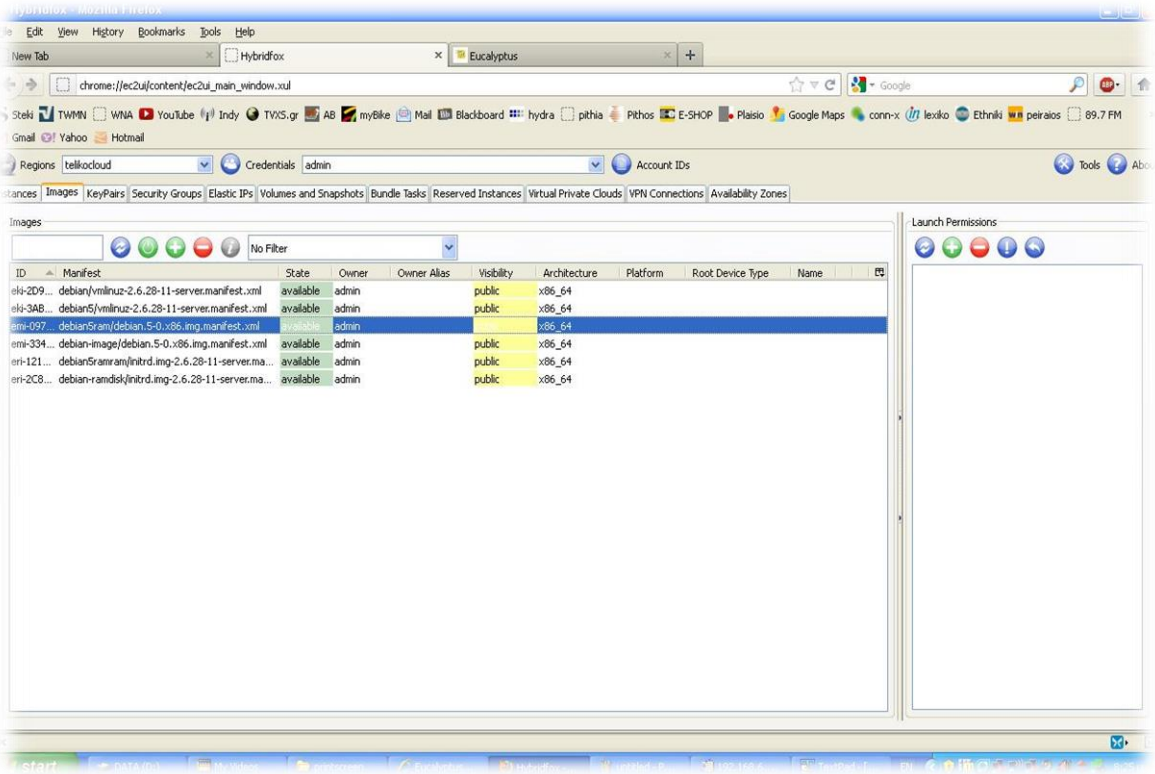
5.4 Hydrifox

Έχοντας εξοικειωθεί με τις εντολές του Euca2ools πολλές από τις βασικές λειτουργίες μπορούμε να τις πραγματοποιήσουμε μέσω του plug-in Hydrifox το οποίο μας προσφέρει μια διεπαφή μέσω του φυλλομετρητή μας.
Εγκαθιστούμε τον Hydrifox και του περνάμε τις παραμέτρους από τα πιστοποιητικά που μας δίνει το Eucalyptus έπειτα είμαστε έτοιμοι να συνδεθούμε και να λάβουμε πληροφορίες σχετικά με τα στιγμιότυπα που τρέχουν :

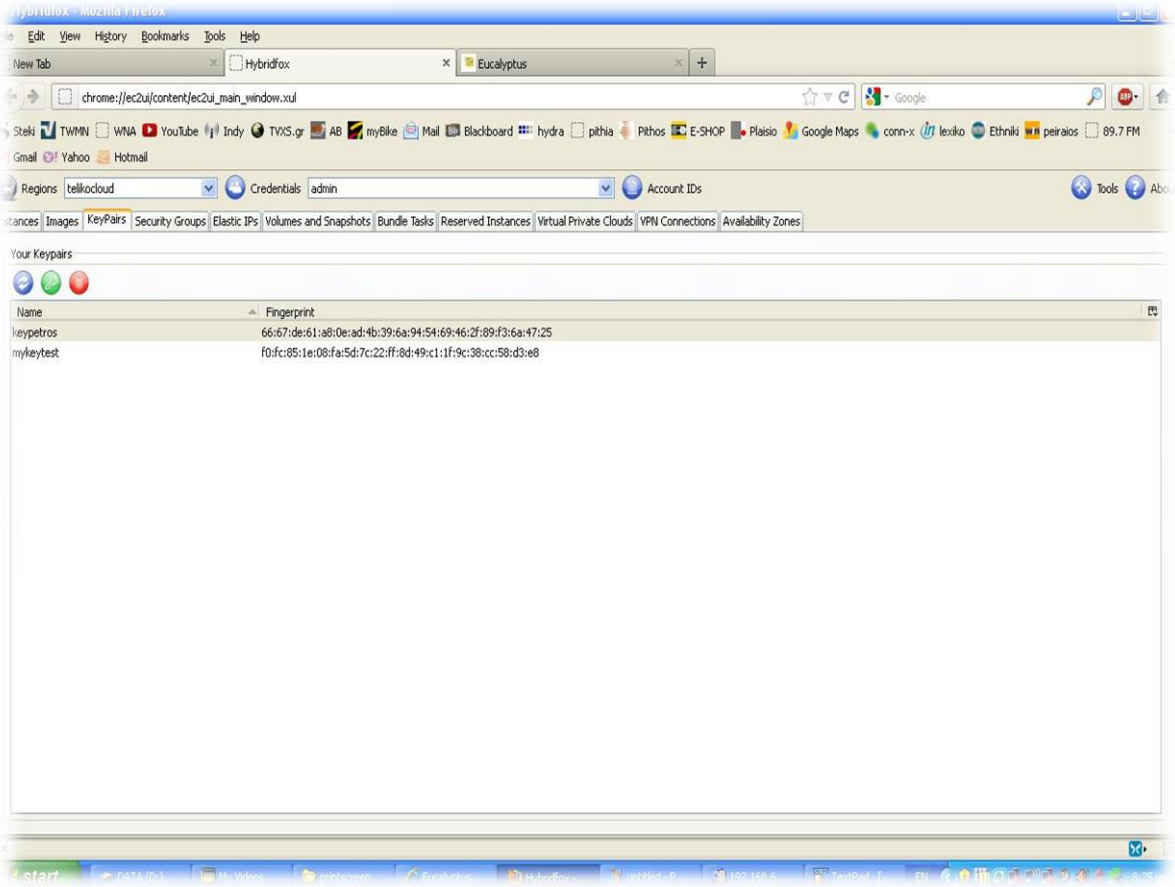
Εικόνα 5.10 Gydrifox



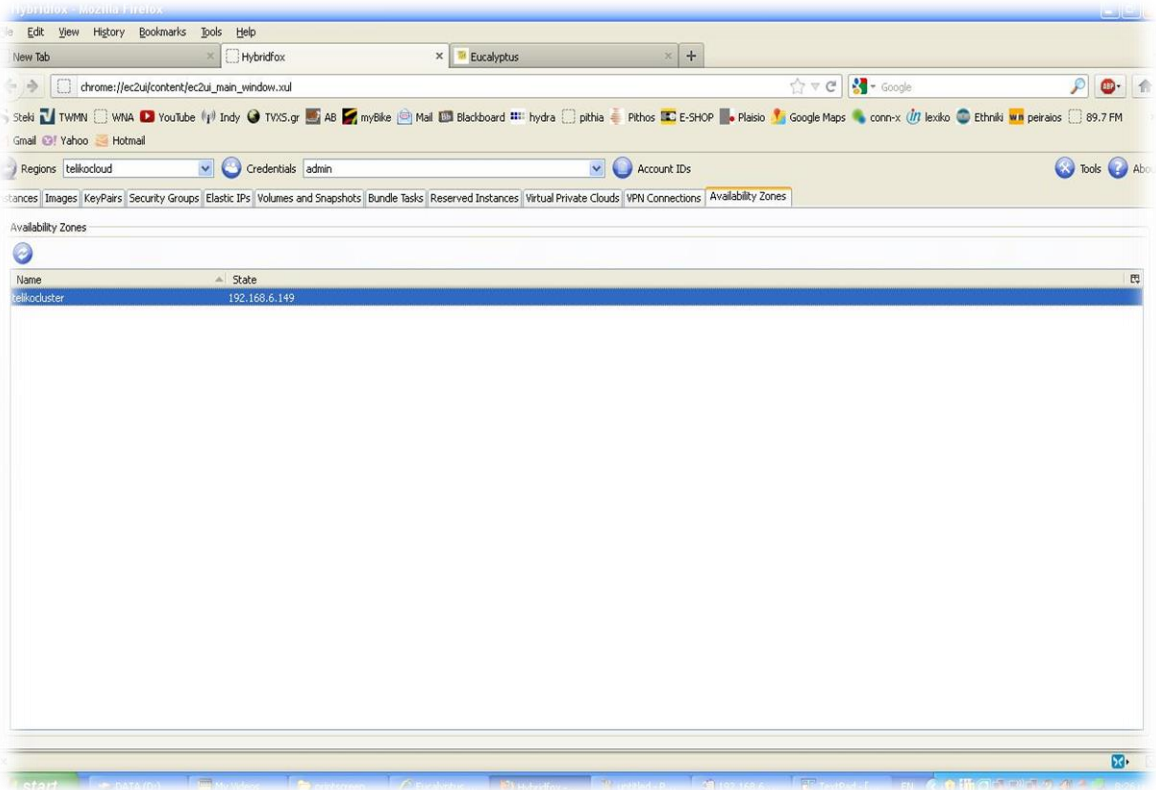
Τις διαθέσιμες εικόνες :



Τα κλειδιά που έχουμε δημιουργήσει :



Τις διαθέσιμες ζώνες :



Και πολλές άλλες πληροφορίες σχετικά με το cloud. Πλέον ο χρήστης είναι έτοιμος να συνδεθεί στο στιγμιότυπο του και να το λειτουργήσει χωρίς να τον απασχολεί τίποτα άλλο σχετικά με την αρχιτεκτονική και την υποδομή που βρίσκεται πίσω από αυτό.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό υλοποιήθηκε ένα cloud με την πλατφόρμα Eucalyptus. Παρουσιάστηκαν οι βασικές του λειτουργίες μέσω του euca2ools και του Hydrifox.

Κεφάλαιο 6 ΣΥΜΠΕΡΑΣΜΑΤΑ – Μελλοντικές Επεκτάσεις

Το μεγαλύτερο μέρος της πτυχιακής εργασίας αποτέλεσε η διαδικασία εγκατάστασης και παραμετροποίησης του Eucalyptus καθώς χρειάστηκαν αρκετές δοκιμές εγκαταστάσεων και ρυθμίσεων μέχρι το πρώτο εικονικό λειτουργικό να τεθεί σε λειτουργία.

Όταν άρχισα την έρευνα σχετικά με το cloud computing διάφορες ιδέες ‘έπεσαν’ στο τραπέζι πιστεύοντας ότι με το cloud θα μπορέσουμε να δώσουμε κάποιες πρακτικές λύσεις αξιοποιώντας τον διαθέσιμο εξοπλισμό του Τμήματος Πληροφορικής. Η ιδέα ήταν να χρησιμοποιηθούν πολλοί από τους παροπλισμένους μεν αλλά όχι τόσο παλιάς τεχνολογίας υπολογιστές που διαθέτει το τμήμα ώστε να στηθεί ένα cloud αρκετά δυνατό, ικανό να ικανοποιήσει τις ανάγκες σε υποδομή. Έμενε να δούμε αν αυτή η ιδέα μπορούσε να υλοποιηθεί.

Με αυτό το σενάριο και έχοντας στην διάθεση μου δύο υπολογιστές, έναν τελευταίας τεχνολογίας intel i core , και έναν από τους παροπλισμένους Pentium 4 αποφάσισα να αξιοποιήσω τον καινούργιο ως Front-End ώστε να τρέχουν γρήγορα οι βασικοί controller του cloud και σαν Node να χρησιμοποιηθεί ο παλιός υπολογιστής που θα μας έδινε τους πόρους σε μνήμη, επεξεργαστή και δίσκο ώστε να τρέχουν τα εικονικά λειτουργικά. Αυτό το σενάριο είχε την προοπτική ότι έχουμε στην διάθεση μας πολλούς παλιούς υπολογιστές ώστε να δημιουργήσουμε ένα μεγάλο δίκτυο υπολογιστών με αρκετά μεγάλη υπολογιστική ισχύ.

Δοκιμές επι δοκιμών καθώς το cloud δεν λειτουργούσε και η απάντηση ήρθε μέσω του KVM. Το KVM είναι ο επόπτης των εικονικών λειτουργικών συστημάτων και στις απαιτήσεις λειτουργίας του θέτει ως προϋπόθεση ο επεξεργαστής του συστήματος που τρέχει τον επόπτη να υποστηρίζει VT (virtualization technology), απαίτηση την οποία ο Pentium 4 δεν ικανοποιούσε.

Έτσι το αρχικό σενάριο δεν απέδωσε και το σύστημα έπρεπε να στηθεί από την αρχή αυτή την φορά με Front-End το παλιό μηχάνημα και Node το καινούργιο όπου πλέον το cloud λειτούργησε με επιτυχία.

Ο μόνος τρόπος για να υλοποιηθεί το αρχικό σενάριο θα ήταν αντί του KVM να επιλεχθεί ο επόπτης Xen ο οποίος υποστηρίζεται από το Eucalyptus αλλά απορρίφτηκε λόγω της πολυπλοκότητας στην διαδικασία εγκατάστασης αλλά και τις υποδεέστερης απόδοσης συγκριτικά με τον KVM.

Ένας ακόμα σημαντικός περιορισμός που καλείται να λάβει υπόψη του ο διαχειριστής του cloud κατά την εγκατάσταση είναι η μορφολογία του δικτύου του οργανισμού και το κατά πόσο υπάρχουν διαθέσιμες δημόσιες ip διευθύνσεις γιατί εκτός από τους υπολογιστικούς πόρους (μνήμη, επεξεργαστή και αποθήκευση) κάθε εικονικό σύστημα χρειάζεται μια τοπική και μια δημόσια ip για να είναι προσβάσιμο.

Τέλος ασκώντας κριτική σχετικά με την επιλογή του Eucalyptus ως πλατφόρμα υλοποίησης του cloud θα έλεγα ότι σε μια μελλοντική διαφορετική υλοποίηση δεν θα επέλεγα ξανά αυτήν την πλατφόρμα κυρίως για το ανεπαρκή υποστήριξη σε τεχνικό επίπεδο. Αυτό είχε ως αποτέλεσμα μικρά προβλήματα να απαιτούν μέρες για να λυθούν καθυστερώντας την συνολική υλοποίηση.

Σύμφωνα με τους αρχικούς στόχους μελετήθηκε και να ορίστηκε τι είναι το cloud computing καθώς και η αρχιτεκτονική δομή αυτού. Αναλύθηκε το μοντέλο διανομής του cloud (SaaS, IaaS , PaaS) και το μοντέλο εφαρμογής του cloud (Public, Private, Hydrid) . Αναλύθηκαν οι κυριότεροι λόγοι για την υιοθέτηση του cloud και της επίδρασης του στους οργανισμούς και τις επιχειρήσεις. Επίσης μελετηθηκαν τα ζήτημα της ασφάλειας στο cloud computing όπως αυτό παρουσιάζεται με βάση την αρχιτεκτονική δομή του cloud από την υποδομή μέχρι τον τελικό χρήστη και προταθήκαν τεχνολογικές λύσεις για την εξάλειψη των προβλημάτων ασφάλειας που προκύπτουν. Και τέλος υλοποιήθηκε μια πειραματική εφαρμογή λειτουργίας ενός cloud computing με υλική υποδομή του τμήματος Πληροφορικής.

Σε ότι αφορά την ασφάλεια του cloud από την μια η υπάρχουσα υποδομή και η αρχιτεκτονική του δικτύου δεν εισάγει νέες απαιτήσεις ασφάλειας, αλλά από την άλλη ειδικά το δημόσιο cloud θέτει νέες προϋποθέσεις και πτυχές ασφάλειας αλλάζοντας τις παραδοσιακή ζώνες και βαθμίδες με επίπεδα εμπιστευτικότητας. Επιπλέον για πρώτη φορά εισέρχεται η έννοια της ασφάλειας ως παρεχόμενη υπηρεσία και διασφαλίζεται μέσω συμβάσεων μεταξύ του πελάτη και του παρόχου. Μέσα από την τριβή μου με το cloud computing ως συμπέρασμα προκύπτει ότι είναι μια τεχνολογία που αξίζει να υιοθετηθεί και να επενδυθεί σε αυτήν προσπάθεια να διασφαλιστούν τα ζητήματα ασφάλειας που προκύπτουν καθώς της τεχνολογίας αυτής υπερνικούν τα όποια προβλήματα παρουσιάζει.

Έχοντας πλέον στην διάθεση μας ένα πλήρως λειτουργικό cloud ως πρόταση για μελλοντική έρευνα θα ήταν να δημιουργηθούν διάφοροι χρήστες μέσα στο τμήμα πληροφορικής οι οποίοι μέσω της χρήσης του cloud θα αναδείξουν τις όποιες αδυναμίες του συστήματος μας. Έτσι ο διαχειριστής θα κληθεί να λάβει τα απαραίτητα μέτρα για παράδειγμα σε περίπτωση διακοπής ρεύματος, ή λήψης αντιγράφων ασφάλειας των στιγμιότυπων καθώς και να στηθούν υπηρεσίες για τους τελικούς χρήστες όπως για παράδειγμα ένας cloud email client ή μια cloud σουίτα εφαρμογών γραφείου.

Το σημαντικότερο όμως επόμενο βήμα κατά την γνώμη μου θα ήταν να υλοποιηθεί ένα Σύνορο Εμπιστοσύνης και Διαχείριση Ταυτοποίησης και Πρόσβασης (IAM-Identity and Access Management) καθώς οι υπηρεσίες cloud που υποστηρίζουν IAM θα επιταχύνουν το πέρασμα από τα έμπιστα εταιρικά δίκτυα στο έμπιστο μοντέλο υπηρεσιών του cloud. Επιπλέον για τους χρήστες μια καλά υλοποιημένη

IAM θα βοηθήσει στην προστασία της εμπιστευτικότητας της ακεραιότητας και της διαχείρισης των πληροφοριών που αποθηκεύονται στο cloud.

Τα βασικότερα χαρακτηριστικά της IAM είναι :

Αυθεντικοποίηση

Αυθεντικοποίηση είναι η διαδικασία πιστοποίησης της ταυτότητας ενός χρήστη ή συστήματος (π.χ το Lightweight Directory Access Protocol – LDAP πιστοποιεί τα διαπιστευτήρια που παρουσιάζει ο χρήστης, όπου το αναγνωριστικό είναι ένα εταιρικό αναγνωριστικό χρήστη όπου είναι μοναδικό και εκχωρείται σε ένα υπάλληλο. Σε μερικές περιπτώσεις όπως αλληλεπίδραση μεταξύ υπηρεσιών η αυθεντικοποίηση εμπλέκεται πιστοποιώντας το δίκτυο της υπηρεσίας που ζητάει πρόσβαση σε πληροφορίες που βρίσκονται σε μια άλλη υπηρεσία (π.χ μια διαδικτυακή υπηρεσία συνδέεται σε μια υπηρεσία πιστωτικών καρτών για να πιστοποιήσει την πιστωτική κάρτα για λογαριασμό του πελάτη)

Εξουσιοδότηση

Εξουσιοδότηση είναι η διαδικασία με την οποία καθορίζονται τα προνόμια που δικαιούται ο χρήστης ή το συστήματα αφότου εξακριβωθεί η ταυτότητα του. Στον κόσμο των ψηφιακών υπηρεσιών η εξουσιοδότηση συνήθως ακολουθεί την αυθεντικοποίηση και χρησιμοποιείται για να καθορίσει πότε ένας χρήστης ή μια υπηρεσία έχει τα απαραίτητα προνόμια για να πραγματοποιήσει μια λειτουργία.

Έλεγχος

Στο πλαίσιο της IAM ο έλεγχος συνεπάγεται την διαδικασία της επανεξέτασης των καταγραφών της αυθεντικοποίησης και της εξουσιοδότησης και των ενεργειών που λαμβάνουν χώρα ώστε να προσδιοριστεί η επάρκεια του συστήματος ελέγχων της IAM. Επίσης πιστοποιείται η συμμόρφωση με την καθιερωμένη πολιτική ασφάλειας, εντοπίζονται παραβιάσεις στις υπηρεσίες ασφάλειας και προτείνονται οι όποιες απαραίτητες αλλαγές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Mather, T., Kumaraswamy, S., Latif, S. Cloud Computing and Privacy (2009), O'Reilly, Sebastol, USA

AWS signature version 1 is insecure, http://www.daemonology.net/blog/2008-12.html

GNU, http://www.gnu.org/licenses/licenses.html

Google Privacy Blunder, http://www.techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/

International Data Corporation, http://www.idc.com/getdoc.jsp?sessionId=&containerId=prMY21726709&sessionId=JC4TVLQ0F4XZICQJAFICFFAKBEAUMIWD

North American Networks Group (NANOG) (http://www.nanog.org/meetings/nanog36/presentations/boothe.pdf)

Open Source Initiave, http://www.opensource.org/docs/osd

OWASP, http://www/owasp.org/index.php/Top_10_2010