Τ.Ε.Ι. ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΣΤΟ CLOUD

ΓΑΛΙΑΤΣΑΤΟΥ ΑΓΛΑΪΑ ΜΑΡΓΑΡΙΤΑ
ΜΗΛΙΩΝΗ ΔΗΜΗΤΡΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΠΑΠΑΔΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ

ΠΑΤΡΑ – 2019

ΠΡΟΛΟΓΟΣ

Η ασφάλεια και η προστασία που παρέχεται από τις υπηρεσίες cloud αποτελεί μείζον ζήτημα του σύγχρονου computing. Για αυτό τον λόγο, οποιαδήποτε έρευνα ή μελέτη που αφορά την διερεύνηση της ασφάλειας που παρέχει το cloud, αποτελεί ένα σημαντικό εγχείρημα τόσο σε οικονομικό, όσο και σε διαδικτυακό επίπεδο. Το θέμα που επιλέγει για την ολοκλήρωση των σπουδών μου είναι η ασφάλεια και η προστασία στο Cloud. Η βασική επιδίωξη μέσα από την ανάπτυξη του θέματος είναι η διερεύνηση των θεμάτων ασφαλείας που προκύπτουν από την χρήση του cloud computing, τόσο μέσω της ανάπτυξης της υπάρχουσας βιβλιογραφίας όσο και μέσω της ποσοτικής μέτρησης των απόψεων των χρηστών σχετικά με την ασφάλεια και την προστασία που τους παρέχει το υπολογιστικό νέφος.

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο θα θέλαμε να ευχαριστήσουμε ιδιαίτερα των επιβλέποντα καθηγητή μας κ. Δημήτρη Παπαδόπουλο για την άψογη συνεργασία και επικοινωνία, καθώς και για τις χρήσιμες παρατηρήσεις και συμβουλές που μας έδωσε κατά την διάρκεια συγγραφής της παρούσας πτυχιακής εργασίας.

Έπειτα, θα θέλαμε να πούμε ένα μεγάλο ευχαριστώ στον κ. Αριστείδη Μπακάλη για την αμέριστη στήριξή του και πολύτιμή του βοήθειά στην επιλογή θέματος, αλλά και σε όλους τους καθηγητές μας, που με τις γνώσεις τους μας προσέφεραν σημαντικά εφόδια για την ατομική αλλά και επαγγελματική μας εξέλιξη.

Τέλος, οφείλουμε ένα τεράστιο ευχαριστώ στις οικογένειές μας, που πάντα μας στηρίζουν και μας ενθαρρύνουν στην εκπλήρωση των στόχων μας.

Σας ευχαριστούμε εκ βαθέων…

ΠΕΡΙΛΗΨΗ

Στην παρούσα πτυχιακή εργασία, γίνεται μία προσέγγιση του θέματος της ασφάλειας στο υπολογιστικό νέφος καθώς και των τρόπων με τους οποίους αυτή παρέχεται. Αρχικά γίνεται αναφορά στην ανάπτυξη του προβλήματος της ασφάλειας του cloud, μέσα από την ανάλυση της αρχιτεκτονικής του αλλά και των διαφόρων μοντέλων και υπηρεσιών που υπάρχουν. Στην συνέχεια αναλύονται οι παράγοντες που απειλούν την ασφάλεια του υπολογιστικού νέφους καθώς και την προστασία των δεδομένων των χρηστών και γίνεται αναφορά στον τρόπο με τον οποίο κατηγοριοποιούνται τα θέματα ασφαλείας στη νεφοϋπολογιστική. Έπειτα, ακολουθεί η ανάπτυξη της ερευνητικής μεθόδου που αναπτύχθηκε για την ποσοτική μέτρηση των απόψεων χρηστών του cloud, με την συμμετοχή επιχειρήσεων της Πάτρας και της Αθήνας, με ανάλυση και αξιολόγηση των αποτελεσμάτων. Τέλος, παρουσιάζονται τα συμπεράσματα που προκύπτουν από την ανάπτυξη της βιβλιογραφίας και από την ανάλυση των αποτελεσμάτων της έρευνα που διεξήχθη.

ABSTRACT

This thesis is an approach to the issue of security in cloud computing as well as the ways in which protection is provided. Initially, the development of the cloud security problem is analyzed, through the exploration of its architecture and the various models and services that exist. Next, there is an examination of the factors that threaten cloud computing security and the protection of the user data. Also reference is made to how security issues are categorized in the cloud computing. Following that, there is a presentation of the development of the research method that was developed regarding the quantitative measurement of cloud users' views, with the participation of business owners in Patras and Athens, followed by the analysis and the evaluation of the results. Finally, the conclusions from the development of the bibliography and the analysis of the results of the research carried out are presented.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Πριν από κάποιες δεκαετίες συνηθίζαμε να αποθηκεύουμε τα δεδομένα μας σε δισκέτες και δίσκους. Έπειτα, τους αντικαταστήσαμε με τα «φλασάκια» ή αλλιώς USB sticks. Πλέον, ήρθε η εποχή όπου έχουμε τη δυνατότητα να «σώσουμε» τα δεδομένα μας από όπου και βρισκόμαστε, χωρίς να χρειαζόμαστε κάποιο απτό αντικείμενο ως χώρο αποθήκευσης, αλλά μόνο μία ηλεκτρονική συσκευή (υπολογιστή, κινητό τηλέφωνο, tablet) και σύνδεση στο διαδίκτυο. Αυτή η τεχνολογία ονομάζεται cloud computing ή νεφοϋπολογιστική, στα ελληνικά.
Το Cloud computing έχει δημιουργήσει σημαντικό ενδιαφέρον τόσο για τον ακαδημαϊκό χώρο όσο και για τη βιομηχανία, εξακολουθώντας να είναι ένα εξελισσόμενο πρότυπο. Το υπολογιστικό νέφος προσφέρει πολλά πλεονεκτήματα όπως γρήγορη ανάπτυξη, επί πληρωμή χρήση, χαμηλότερο κόστος, δυνατότητα κλιμάκωσης, ταχεία παροχή, γρήγορη και μεγαλύτερη ελαστικότητα, πρόσβαση σε πανταχού παρούσα πρόσβαση στο δίκτυο, προστασία και ασφάλεια κατά των επιθέσεων δικτύου, χαμηλού κόστους αποκατάσταση καταστροφών και λύσεις αποθήκευσης δεδομένων, ανίχνευση σε πραγματικό χρόνο της παραβίασης του συστήματος και ταχεία ανασύσταση των υπηρεσιών.

Αν και το cloud computing στοχεύει στην καλύτερη αξιοποίηση των πόρων χρησιμοποιώντας τεχνολογίες εικονικοποίησης και στην ανάληψη μεγάλου μέρους του φορτίου εργασίας από τον πελάτη, είναι γεμάτο με κινδύνους ασφαλείας. Τόσο σε προσωπικό όσο και σε επιχειρησιακό επίπεδο, η προστασία και η ασφάλεια των προσωπικών πληροφοριών των πελατών, όσο και η ικανοποίηση των προσδοκιών των πελατών για τη χρήση των προσωπικών τους πληροφοριών, αποτελούν ένα από τα πιο βασικά ζητήματα σχετικά με την χρήση του cloud computing.

Τα τελευταία χρόνια, το cloud computing έχει εξελιχθεί από μια πολλά υποσχόμενη επιχειρηματική ιδέα σε ένα από τα ταχέως αναπτυσσόμενα τμήματα της βιομηχανίας πληροφορικής. Όμως, καθώς όλο και περισσότερες πληροφορίες σχετικά με άτομα και εταιρείες τοποθετούνται στο νέφος, αρχίζουν να αναπτύσσονται ανησυχίες σχετικά με το πόσο ασφαλές είναι το περιβάλλον τους. Παρά την όλη δημοσιότητα που περιβάλλει το cloud computing, οι εταιρικοί πελάτες εξακολουθούν να διστάζουν να αναπτύξουν την επιχείρησή τους στο σύννεφο. Η ασφάλεια είναι ένα από τα σημαντικότερα ζητήματα που μειώνει την ανάπτυξη του cloud computing και οι επιπλοκές με την ιδιωτική ζωή των δεδομένων και την προστασία των δεδομένων εξακολουθούν να μαστίζουν την αγορά.

Στα πλαίσια της παρούσας εργασίας, βασικός σκοπός είναι η διερεύνηση του φαινομένου των απειλών που δέχεται η ασφάλεια και η προστασία του υπολογιστικού νέφους, οι οποίες θέτουν σε κίνδυνο βασικά δεδομένα εκατομμυρίων χρηστών ανά τον κόσμο. Τα ερευνητικά ερωτήματα που θέτονται για την επίτευξη του στόχου της εργασίας είναι:

1. Ποιες είναι οι πιο σοβαρές απειλές του cloud computing;
2. Ποιο είναι το επίπεδο ικανοποίησης των χρηστών από τις υπηρεσίες cloud και πώς μετράνε την ποιότητα της ασφάλειας;

Για την διερεύνηση των ερευνητικών ερωτημάτων, γίνεται τόσο βιβλιογραφική όσο και ποσοτική έρευνα. Κατά την βιβλιογραφική έρευνα, γίνεται κριτική ανασκόπηση της υπάρχουσας βιβλιογραφίας για την κατανόηση των βαθύτερων παραγόντων που αποτελούν απειλή για την ασφάλεια στην νεφοϋπολογιστική.

Κατά το πρακτικό μέρος, διεξάγεται ποσοτική έρευνα, με συλλογή πρωτογενών στοιχείων, σε ένα συγκεκριμένο δείγμα πληθυσμού, με σκοπό την διερεύνηση των βασικών απόψεων του σχετικά με το κρίσιμο θέμα της ασφάλειας του υπολογιστικού νέφους και το μέτρο της προστασίας που τους παρέχεται από τους σχετικούς παρόχους νεφοϋπολογιστικής.

Μέσα από την παρούσα έρευνα δίνεται ιδιαίτερα προσοχή στη διερεύνηση και ερμηνεία του συνόλου των αιτιών του φαινομένου των απειλών που δέχεται η ασφάλεια του υπολογιστικού νέφους. Συγκεκριμένα, γίνεται προσπάθεια διερεύνησης των παραγόντων που προκαλούν τα κενά ασφαλείας στο νέφος, καθώς και το πώς αυτά επηρεάζουν τις απόψεις των χρηστών, ενισχύοντας την ήδη υπάρχουσα γνώση για το κοινωνικοοικονομικό φαινόμενο της απειλής της προστασίας στο cloud computing.

Η ανάπτυξη του θέματος γίνεται μέσα από πέντε κεφάλαια. Στο πρώτο κεφάλαιο γίνεται ανάπτυξη των διαθέσιμων μοντέλων υπηρεσιών, καθώς και αναφορά στα βασικά θέματα ασφαλείας και της απειλές που δέχεται η αρχιτεκτονική του cloud computing, ενώ παράλληλα, αναλύονται σημαντικές έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

Στο δεύτερο κεφάλαιο εξετάζονται οι διάφοροι τύποι επίθεσης που δέχεται το cloud computing και αναλύονται οι κίνδυνοι στην ασφάλεια, που σχετίζονται με την ανάπτυξη και χρήση κάθε μοντέλου υπηρεσιών του νέφους, εξετάζοντας ένα ευρύ φάσμα παραγόντων.
Στο τρίτο κεφάλαιο αναπτύσσονται προτάσεις σχετικά με την ασφάλεια στο cloud computing, ενώ παράλληλα γίνεται αναφορά σε αναδυόμενες τάσεις στην ασφάλεια και την ιδιωτικότητα κατά την χρήση του cloud computing.

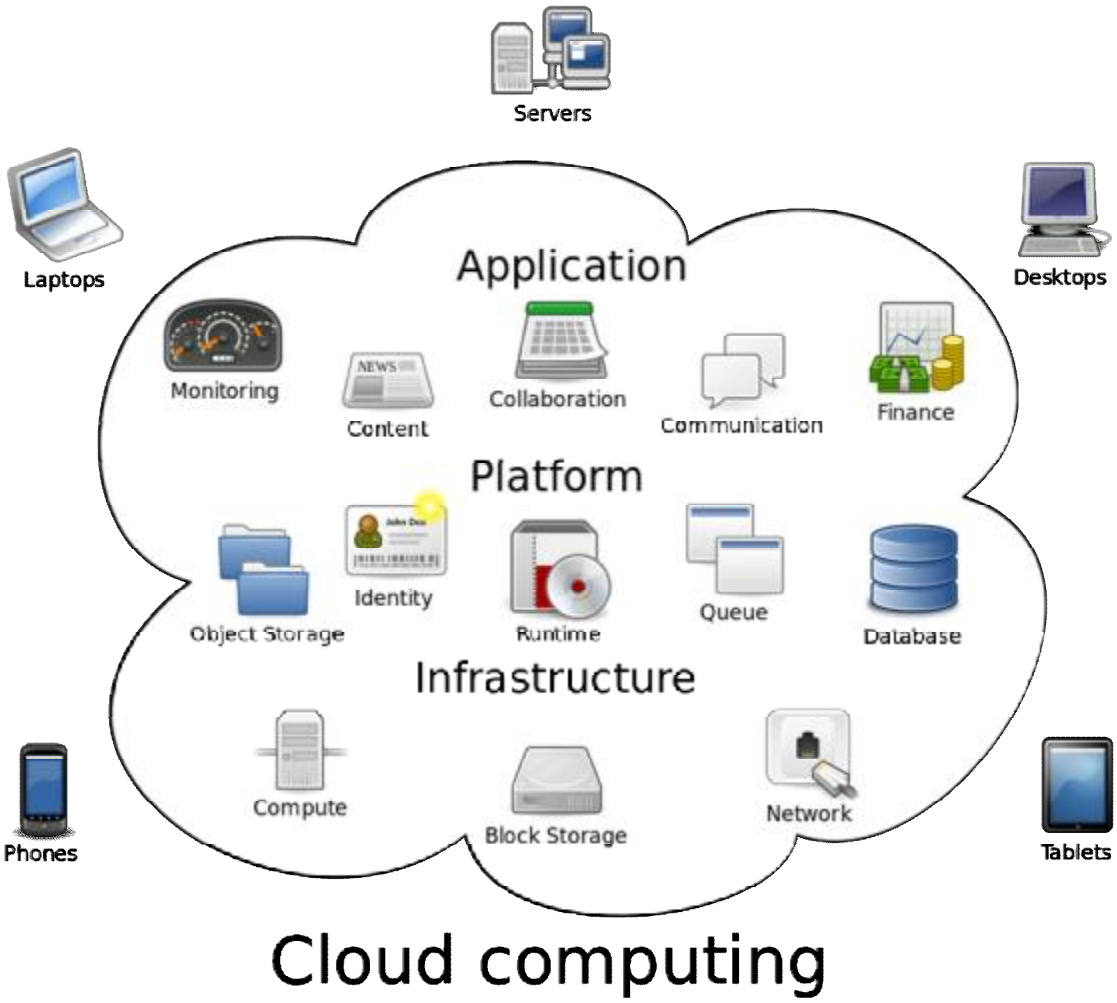
Στο τέταρτο κεφάλαιο αναπτύσσεται το ερευνητικό κομμάτι της εργασίας. Γίνεται αναφορά στην μεθοδολογία που ακολουθεί η έρευνα, ενώ διατυπώνονται οι στόχοι της έρευνας και παρουσιάζονται τα αποτελέσματα που προκύπτουν από την διεξαγωγή της.
Τέλος στο πέμπτο κεφάλαιο παρουσιάζονται τα αποτελέσματα του προκύπτουν από την ανασκόπηση της βιβλιογραφίας και από την διενέργεια της έρευνας.

ΚΕΦΑΛΑΙΟ 1

1.1 **ΓΕΝΙΚΑ ΓΙΑ ΤΟ** CLOUD COMPUTING

Σύμφωνα με τον ορισμό που δίνεται από το National Institute of Standards and Technology (NIST) το Cloud Computing:

«είναι ένα μοντέλο που καθιστά ικανή την πρακτική και κατά απαίτηση πρόσβαση σε μια πληθώρα παραμετροποιήσιμων υπολογιστικών πόρων (όπως δίκτυα, διακομιστές, αποθηκευτικοί χώροι, applications και υπηρεσίες), οι οποίοι μπορούν με ραγδαία ταχύτητα να εφοδιαστούν και να απελευθερωθούν χρησιμοποιώντας την ελάχιστη δυνατή προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών». (Badger, et al., 2011)



Εικόνα 1: Cloud Computing – Μεταφορικά: Μία ομάδα στοιχείων δικτύου σαν ένα άμορφο σύννεφο.
(Johnston, n.d.)

Ουσιαστικά, το cloud είναι απλά μία μεταφορά για το «Internet» και δεν έχει καμία σχέση με τον σκληρό δίσκο του υπολογιστή. Όταν η αποθήκευση δεδομένων ή η εκτέλεση προγραμμάτων γίνεται μέσω του σκληρού δίσκου, έχουμε να κάνουμε με την τοπική

αποθήκευση, αφού ότι χρειαζόμαστε είναι από φυσικής απόψεως κοντά μας, κάτι που διευκολύνει την πρόσβαση των δεδομένων από τον συγκεκριμένο υπολογιστή, καθώς και από τους υπόλοιπους υπολογιστές που ανήκουν στο ίδιο τοπικό δίκτυο.

Από την άλλη μεριά, το cloud computing κάνει δυνατή την αποθήκευση και διαχείριση δεδομένων ή προγραμμάτων μέσω του Internet. Γενικά, η νεφοϋπολογιστική και το local computing συνδέονται κατά πολύ και ορισμένες φορές ο διαχωρισμός τους γίνεται δύσκολος, αφού πλέον το cloud εμπλέκεται σχεδόν με όλες τις λειτουργίες του υπολογιστή. Ένα τοπικό μέρος κάποιου software μπορεί να αξιοποιεί κάποιας μορφής cloud computing (π.χ. το Microsoft Office χρησιμοποιεί το Microsoft OneDrive).

Το cloud computing αφορά τόσο τις εφαρμογές που παρέχονται ως υπηρεσίες μέσω του διαδικτύου, όσο το hardware και τα συστήματα λογισμικού στα κέντρα δεδομένων που παρέχουν αυτές τις υπηρεσίες. Όπως περιγράφεται από το NIST, υπάρχουν τέσσερα βασικά μοντέλα ανάπτυξης του νέφους, ανάλογα με το ποιος παρέχει τις υπηρεσίες (Badger et. al., 2011). Αυτά τα μοντέλα είναι:

	Διαχείριση Υποδομών[1]	**Ιδιοκτησία Υποδομών**[2]	**Τοποθεσία Υποδομών**[3]	**Προσβασιμότητα και Χρήση**[4]
Δημόσιο Νέφος	Τρίτος Πάροχος	Τρίτος Πάροχος	Εκτός Εγκαταστάσεων	Μη Αξιόπιστοι
Ιδιωτικό/Κοινοτικό Νέφος	Οργανισμός / Τρίτος Πάροχος	Οργανισμός / Τρίτος Πάροχος	Εκτός Εγκαταστάσεων / Εντός εγκαταστάσεων	Αξιόπιστοι
Υβριδικό Νέφος	Οργανισμός και Τρίτος Πάροχος	Οργανισμός και Τρίτος Πάροχος	Εκτός και Εντός Εγκαταστάσεων	Αξιόπιστοι και Μη Αξιόπιστοι

Πίνακας 1: Μοντέλα ανάπτυξης νέφους.

Δημόσιο Νέφος (Public Cloud): η υπηρεσία αυτή είναι διαθέσιμη για το κοινό. Οι πόροι παρέχονται στους χρήστες μέσω του Internet και οι υπηρεσίες είναι είτε δωρεάν, είτε επί πληρωμή, ανάλογα με τις δυνατότητες που προσφέρονται.

Όμως, η φύση του κοινόχρηστου περιβάλλοντος σε αυτό το μοντέλο ευνοεί hackers οι οποίοι αναζητούν αδυναμίες και μπορούν να αποκτήσουν παράνομη πρόσβαση ή να προκαλέσουν

[1] Η διαχείριση περιλαμβάνει την διακυβέρνηση, τις λειτουργίες, την ασφάλεια κλπ.
[2] Φυσικές υποδομές (π.χ. εγκαταστάσεις, υπολογιστικός, αποθηκευτικός και δικτυακός εξοπλισμός)
[3] Τοποθεσία τόσο των φυσικών εγκαταστάσεων όσο και της ιδιοκτησίας τους.
[4] Αξιόπιστοι Καταναλωτές: ανήκουν σε κάποιον τομέα του οργανισμού (εργαζόμενοι, εξωτερικοί συνεργάτες). Μη Αξιόπιστοι Καταναλωτές: εξουσιοδοτημένοι για χρήση μερικών ή όλων των υπηρεσιών, αλλά δεν ανήκουν νομικά στον οργανισμό.

αδυναμία πρόσβασης. Οι επιτιθέμενοι μπορούν επίσης να ενοικιάσουν χώρο στο cloud και να τον χρησιμοποιήσουν ως βάση επίθεσης για τους γειτονικούς πελάτες. Άλλες ανησυχίες είναι:

- η τοποθεσία και τα αντίγραφα ασφαλείας των δεδομένων,
- η αποκατάστασή τους,
- η φορητότητά τους
- και πόσο συχνά γίνεται έλεγχος ευπάθειας κλπ.

Ιδιωτικό Νέφος (Private Cloud): ανήκει σε μία εταιρεία, συνίσταται από πολλαπλούς καταναλωτές και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων. Το ιδιωτικό cloud αποτελείται από το δίκτυο, τον hardware διακομιστή (που συνήθως παρέχει τον εικονικό server), αποθηκευτικό χώρο και τα εργαλεία διαχείρισης. Συνήθως διοικείται εσωτερικά, αλλά μπορεί επίσης να «φιλοξενηθεί» και εξωτερικά από Παρόχους Διαχειριζόμενων Υπηρεσιών (MSP), όπου πλέον λέγεται Εικονικό Ιδιωτικό Νέφος (Virtual Private Cloud).

Η χρήση του ιδιωτικού cloud είναι πιο ασφαλής από αυτή του δημόσιου λόγω της αποκλειστικής εσωτερικής έκθεσης των δεδομένων. Μόνο η εταιρεία και οι ορισθέντες ενδιαφερόμενοι μπορούν να έχουν πρόσβαση στον χειρισμό κάποιου συγκεκριμένου ιδιωτικού νέφους. Η δομή του ιδιωτικού cloud αφαιρεί τα προβλήματα της έλλειψης διαφάνειας από την πλευρά του παρόχου υπηρεσιών.

Το περιβάλλον του νέφους διασπά τα τμηματικά σιλό και προσφέρει αυξημένη πρόσβαση, ειδικά σε μη εργαζόμενους της εταιρείας εάν τους δοθεί πρόσβαση στις on-demand υπολογιστικές πηγές. Όταν τα δεδομένα δεν κλειδώνονται σωστά δημιουργούνται προβλήματα που οδηγούν σε ανεπιθύμητες παραβιάσεις. Η προστασία των δεδομένων από διαρροές καθίσταται κρίσιμη στο περιβάλλον του νέφους.

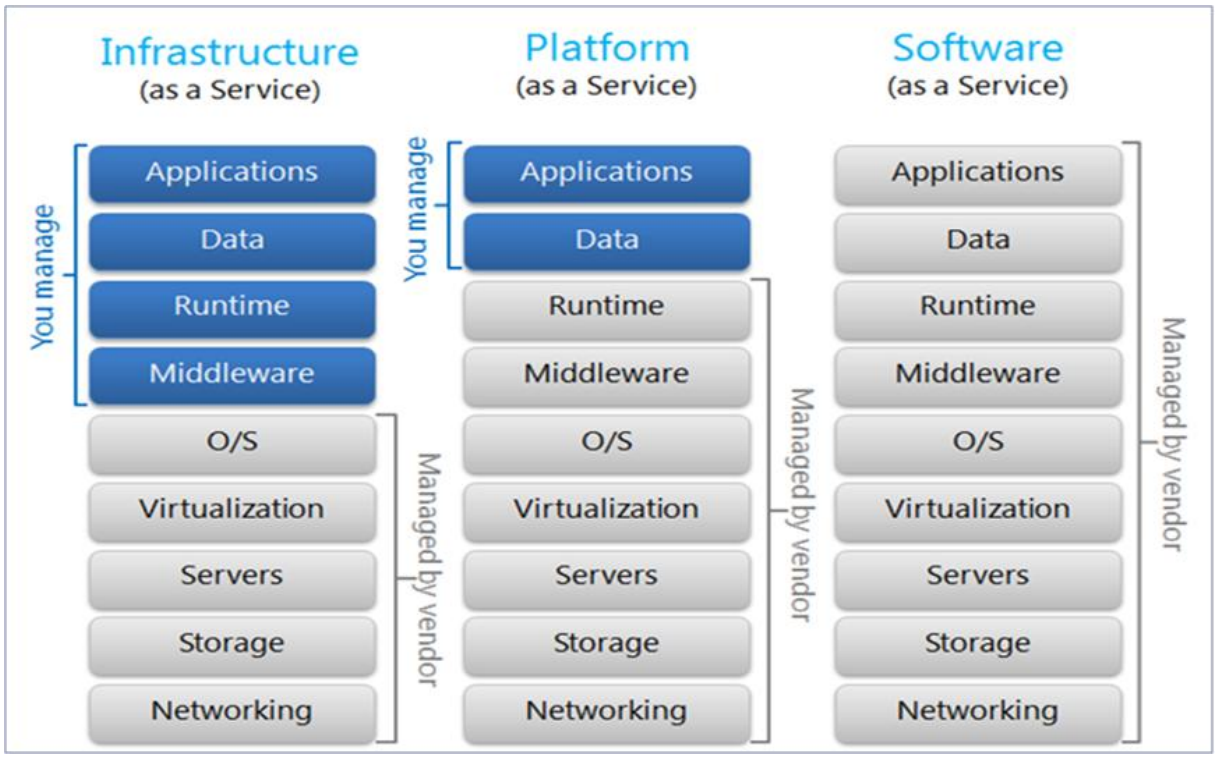
Υβριδικό Νέφος (Hybrid Cloud): Το μεγαλύτερο πλεονέκτημα της χρήσης του ιδιωτικού νέφους είναι η ελαστικότητα και η ασφάλεια, ενώ το δημόσιο νέφος προσφέρει επεκτασιμότητα και προσβασιμότητα. Και τα δύο είδη έχουν μοναδικά πλεονεκτήματα αλλά παράλληλα έχουν κοινά στοιχεία. Το υβριδικό νέφος ενώνει τα πλεονεκτήματα του ιδιωτικού και δημόσιου μοντέλου. Δηλαδή είναι ένας συνδυασμός του ιδιωτικού νέφους με τη χρήση των υπηρεσιών του δημόσιου νέφους και υπάρχουν ένα ή περισσότερα σημεία επαφής μεταξύ των περιβαλλόντων. Ο στόχος είναι ο συνδυασμός υπηρεσιών και δεδομένων από μία ποικιλία μοντέλων cloud, με σκοπό την δημιουργία ενός ενωμένου, αυτοματοποιημένου και ορθά διαχειρισμένου υπολογιστικού περιβάλλοντος (Hurwitz, et al., 2012).

Κοινοτικό Νέφος (Community Cloud): Το συγκεκριμένο νέφος παρέχεται για αποκλειστική χρήση σε κάποια συγκεκριμένη κοινότητα πελατών από οργανώσεις που έχουν κοινές ανησυχίες (π.χ. αποστολή, ανάγκες ασφαλείας, πολιτική, και παραμέτρους συμμόρφωσης). Μπορεί να αποτελεί αντικείμενο χρήσης και διαχείρισης από έναν ή περισσότερους οργανισμούς της κοινότητας, κάποιον εξωτερικό συνεργάτη, ή κάποιον συνδυασμό αυτών και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων (Pandith, 2014).

1.2 **ΜΟΝΤΕΛΑ ΥΠΗΡΕΣΙΩΝ**

Σύμφωνα με το National Institute of Standards and Technology (NIST) υπάρχουν τρεις βασικοί τύποι μοντέλων υπηρεσιών στο cloud:

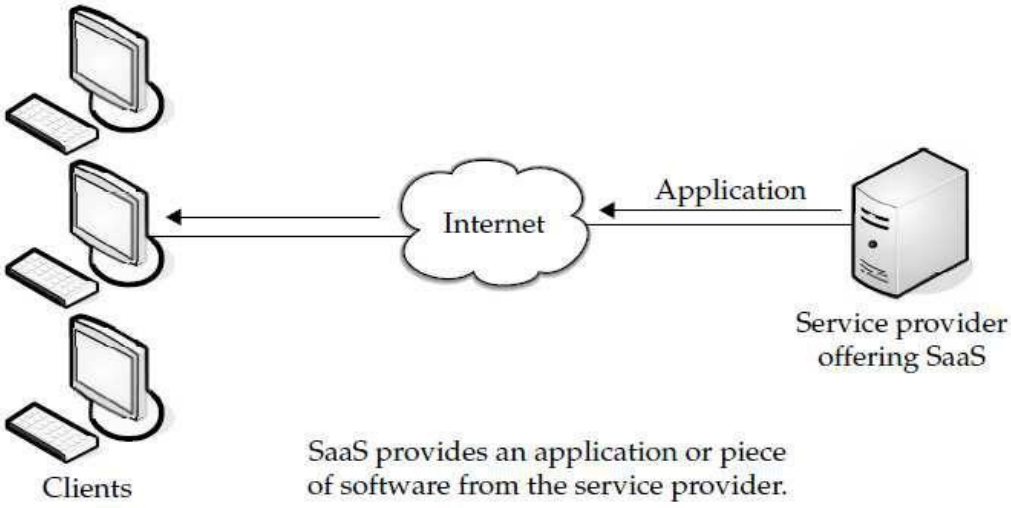
1. το Λογισμικό ως Υπηρεσία Νέφους (Applications/Software as a Service – SaaS),
2. η Πλατφόρμα ως Υπηρεσία Νέφους (Platform as a Service – PaaS) και
3. οι Υποδομές ως Υπηρεσία Νέφους (Infrastructure as a Service – IaaS).



Εικόνα 2: Μοντέλα υπηρεσιών (Anon., n.d.)

Αυτά τα τρία κλασσικά μοντέλα υπηρεσιών νέφους έχουν διαφορετικές ευθύνες απέναντι στην προστασία των προσωπικών δεδομένων. Οι κίνδυνοι και τα προτερήματα του κάθε μοντέλου διαφέρουν, ενώ κρίνεται αναγκαίο να καθοριστούν κατά περίπτωση και σε σχέση με την φύση των εν λόγω cloud υπηρεσιών.

1. Λογισμικό ως Υπηρεσία Νέφους (Applications/Software as a Service – SaaS):
   Η πρόσβαση στις εφαρμογές γίνεται μέσω διαδικτύου, όπως για παράδειγμα το Dropbox και το Microsoft Office 365. Οι SaaS εφαρμογές προσφέρονται δωρεάν ή με συνδρομή. Είναι προσβάσιμες από οποιονδήποτε ηλεκτρονικό υπολογιστή συνδεδεμένο στο διαδίκτυο, είτε μέσω ελαφριών πελατών διασύνδεσης, όπως περιηγητές διαδικτύου, είτε μέσω προγραμμάτων διασύνδεσης.



Εικόνα 3: Λογισμικό ως Υπηρεσία Νέφους (Pandith, 2014)

Θέματα Ασφαλείας στο SaaS:

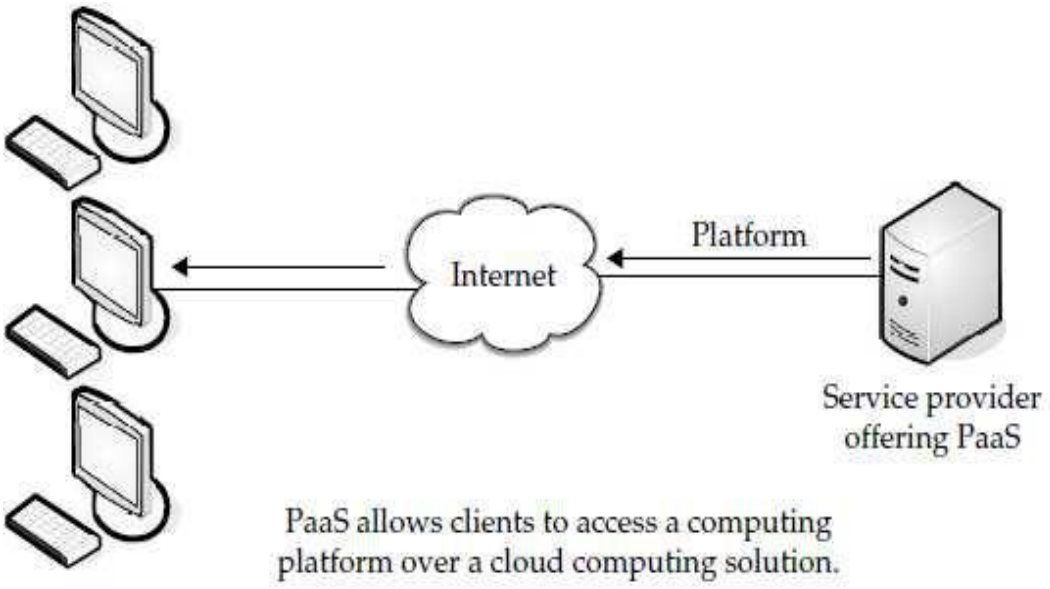
Τα μοντέλα SaaS προσφέρουν στους πελάτες πολλά πλεονεκτήματα, με τα πιο σημαντικά να είναι η βελτιωμένη λειτουργική αποτελεσματικότητα και το μειωμένο κόστος. Εξελίσσονται ραγδαία στο κυρίαρχο μοντέλο παροχής υπηρεσιών για την ικανοποίηση των αναγκών των επιχειρήσεων IT. Ωστόσο, στις περισσότερες επιχειρήσεις τα SaaS μοντέλα δεν είναι ευρέως διαδεδομένα εξαιτίας της έλλειψης διαφάνειας στην αποθήκευση και προστασία των δεδομένων. Σύμφωνα με την μελέτη του Forrester «The State of Enterprise Software: 2009», τα προβλήματα ασφαλείας είναι ο πιο σύνηθες λόγος που οι εταιρείες επικαλούνται αδιαφορία για τα SaaS (Lo, et al., 2009). Συνεπώς, η συζήτηση των ανησυχιών για την ασφάλεια των επιχειρήσεων έχει ανακηρυχθεί ως η μεγαλύτερη πρόκληση για την αποδοχή των εφαρμογών SaaS στο νέφος. Όμως, για να προσπεραστούν οι ανησυχίες των καταναλωτών για την ασφάλεια των εφαρμογών και των δεδομένων, οι πάροχοι πρέπει να αντιμετωπίσουν αυτά τα ζητήματα άμεσα.

Υπάρχει μία έντονη ανησυχία για τις εσωτερικές παραβιάσεις, καθώς και ευαισθησίες στις εφαρμογές και στη διαθεσιμότητα του συστήματος που μπορούν να οδηγήσουν σε απώλεια ευαίσθητων δεδομένων και χρημάτων. Τέτοιες προκλήσεις μπορούν να αποτρέψουν τις επιχειρήσεις να προτιμήσουν SaaS εφαρμογές μέσα στο cloud.

2. Πλατφόρμα ως Υπηρεσία Νέφους (Platform as a Service – PaaS):

Προσφέρει εργαλεία και περιβάλλον στους χρήστες για να δημιουργήσουν εφαρμογές cloud. Για παράδειγμα, η Google έχει ένα προϊόν που ονομάζεται App Engine, το οποίο επιτρέπει στον οποιοδήποτε να αναπτύξει και να τρέξει εφαρμογές πάνω στην υποδομή της Google. Οι App Engine εφαρμογές είναι εύκολες στην ανάπτυξη, στην συντήρηση και στις αλλαγές που χρειάζονται όταν μεγαλώνει ο όγκος της επισκεψιμότητας και των δεδομένων. Με την App Engine δεν υπάρχουν διακομιστές που χρειάζονται διατήρηση από τον δημιουργό της εφαρμογής. Ο πελάτης δεν διαχειρίζεται, ούτε ελέγχει την υποκείμενη cloud υποδομή, που εμπεριέχει δίκτυα, διακομιστές, λειτουργικά συστήματα, ή αποθηκευτικούς χώρους, αλλά έχει τον

έλεγχο των ανεπτυγμένων εφαρμογών και πιθανώς, των ρυθμίσεων παραμέτρων για το περιβάλλον που παρέχεται για την εφαρμογή.



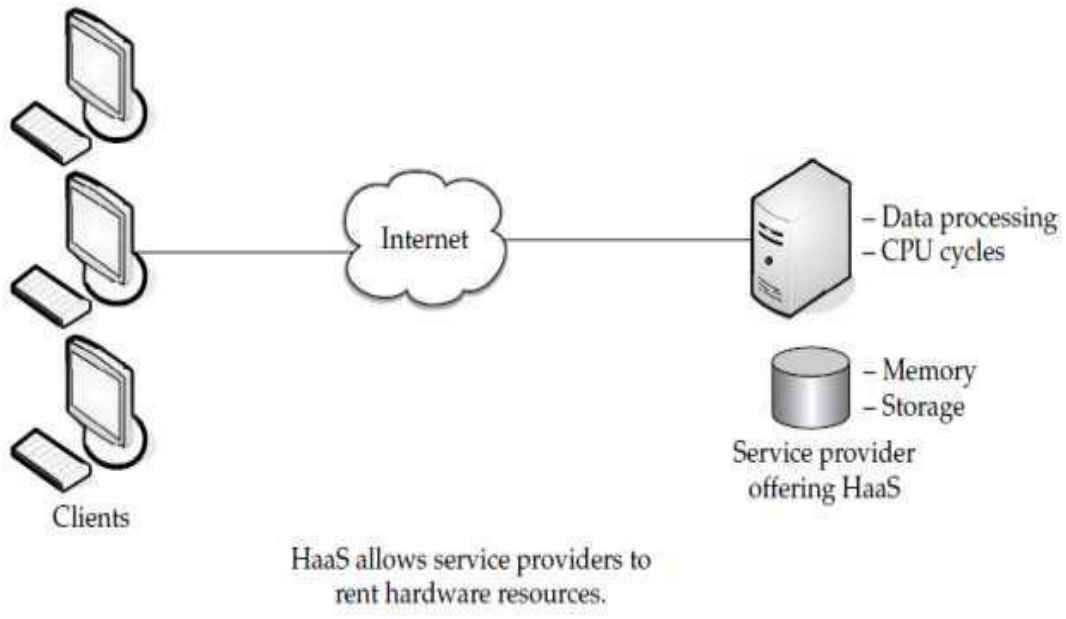
Εικόνα 4: Πλατφόρμα ως Υπηρεσία Νέφους (Pandith, 2014)

Θέματα ασφαλείας στο PaaS:

Προσφέρει στους προγραμματιστές πλήρης διαχείριση ανάπτυξης λογισμικού, καθ' όλο τον κύκλο ζωής της δημιουργημένης εφαρμογής, από την σχεδίαση και την ανάπτυξη των εφαρμογών ως την υλοποίηση, τις δοκιμές και την συντήρηση. Όλα τα υπόλοιπα είναι «κρυμμένα» από την θέα των προγραμματιστών. Αυτή η σκοτεινή πλευρά του PaaS, μπορεί να ευνοήσει hackers να μοχλεύσουν τις cloud υποδομές του PaaS, για επιβολή και έλεγχο κακόβουλου λογισμικού καθώς και την εισχώρηση σε IaaS εφαρμογές.

3. Υποδομή ως Υπηρεσία Νέφους (Infrastructure as a Service – IaaS):

Επιτρέπει στους χρήστες να τρέξουν οποιαδήποτε ήδη υπάρχουσα εφαρμογή στο hardware του παρόχου του cloud. Ο πελάτης δεν διαχειρίζεται ούτε ελέγχει τις υποκείμενες υποδομές του νέφους, αλλά έχει τον έλεγχο του λειτουργικού συστήματος, της αποθήκευσης και των ανεπτυγμένων εφαρμογών. Ίσως έχει και περιορισμένο έλεγχο κάποιων επιλεγμένων δικτυακών στοιχείων (όπως host-based firewalls).



Εικόνα 5: Υποδομή ως Υπηρεσία Νέφους (Pandith, 2014)

Θέματα ασφαλείας στο IaaS:

Το IaaS αλλάζει πλήρως τον τρόπο με τον οποίο οι προγραμματιστές προγραμματίζουν τις εφαρμογές τους. Αντί να σπαταλούν τεράστια χρηματικά ποσά στα δικά τους κέντρα δεδομένων, σε εταιρείες φιλοξενίας διαδικτυακών τόπων ή σε υπηρεσίες συνεγκατάστασης και έπειτα στην πρόσληψη προσωπικού για την συντήρηση της εφαρμογής, μπορούν να καταφύγουν στο Amazon Web Services ή σε κάποιον άλλο πάροχο IaaS, να αποκτήσουν έναν εικονικό server άμεσα και η χρέωσή τους να βασίζεται μόνο στους πόρους που χρησιμοποιούνται.
Με την ύπαρξη cloud μεσιτών όπως οι Rightscale, enStratus κλπ, είναι εύκολο για τους προγραμματιστές να «μεγαλώσουν» τις εφαρμογές τους, χωρίς να χρειάζεται να ανησυχούν για θέματα όπως το scaling και επιπρόσθετη ασφάλεια. Εν ολίγοις, το IaaS και οι υπόλοιπες σχετικές υπηρεσίες έχουν βοηθήσει startups και άλλες επιχειρήσεις να επικεντρωθούν στις βασικές ικανότητές τους, χωρίς να ανησυχούν ιδιαίτερα για την παροχή και την διαχείριση των υποδομών. Ουσιαστικά, το IaaS αφαιρεί τελείως το hardware μέρος και προσφέρει στον πελάτη την δυνατότητα να «καταναλώσει» την υποδομή ως υπηρεσία, δίχως να αναλώνεται τις υποκείμενες περιπλοκές. Το νέφος αποκτά μια ελκυστική προσφορά στην αξία από άποψη κόστους, αλλά το έτοιμο για χρήση IaaS παρέχει μόνο την βασική προστασία (περιμετρικό firewall, εξισορρόπηση φορτίου κ.ά.) και συνεπώς οι εφαρμογές που μεταφέρονται στο cloud χρειάζονται μεγαλύτερα επίπεδα ασφάλειας απ' ότι προσφέρονται. (Pandith, 2014)

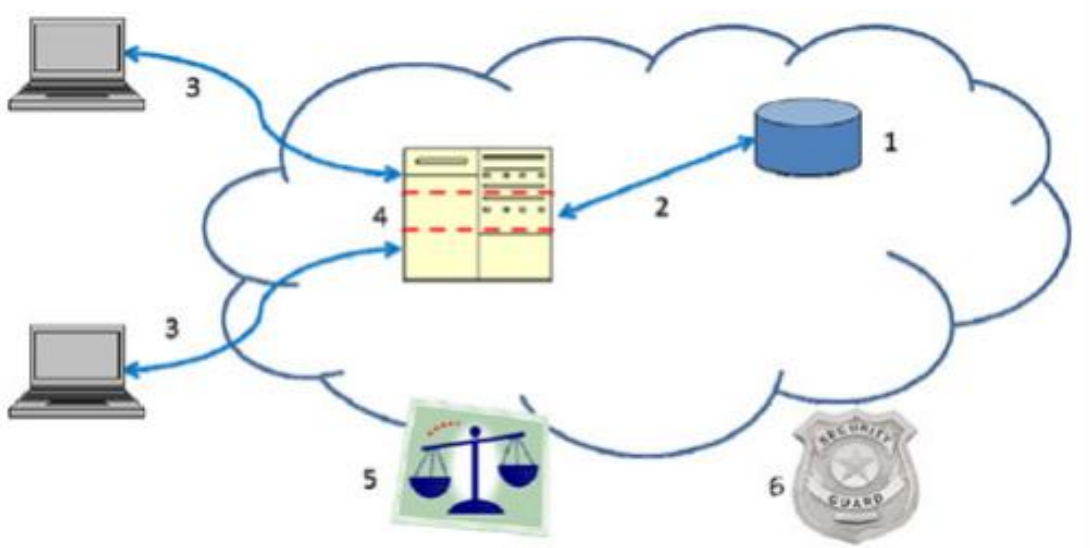
Η κατανόηση των σχέσεων και εξάρτησης μεταξύ αυτών των μοντέλων θεωρείται αποφασιστικής σημασίας. Το IaaS είναι η βάση όλων των υπηρεσιών νέφους. Το PaaS είναι «χτισμένο» πάνω στο IaaS, ενώ με τη σειρά του το SaaS πάνω στο PaaS. (Sen, 2013)

1.3 **ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ**

Λόγω του φθηνού κόστους και των νέων ευέλικτων επιχειρηματικών μοντέλων, το cloud computing υιοθετείται από πολλούς τομείς. Πιο συγκεκριμένα, η εικονικοποίηση και η συγκέντρωση των IT πόρων στο νέφος, επιτρέπει στους οργανισμούς να συνειδητοποιήσουν την σημαντική εξοικονόμηση κόστους, ενώ παράλληλα επιταχύνει την ανάπτυξη καινούριων εφαρμογών. Όμως, δεν μπορούμε να αναφερόμαστε στα μεγάλης βαρύτητας οφέλη για την επιχείρηση, χωρίς να θέσουμε επί τάπητος τις καινούριες προκλήσεις για την προστασία των δεδομένων που δημιουργούνται από την νεφοϋπολογιστική. Χωρίς αμφιβολία το cloud computing παρέχει πλεονεκτήματα στις επιχειρήσεις, αλλά υπάρχουν επίσης κάποιες ανησυχίες για την μεταφορά δεδομένων στο cloud. Η ασφάλεια και η παραμονή των δεδομένων είναι ο πρωταρχικός προβληματισμός. (Pandith, 2014)

Όπως φαίνεται και στην εικόνα παρακάτω, υπάρχουν έξι συγκεκριμένα τμήματα του cloud computing περιβάλλοντος, όπου ο εξοπλισμός και το software απαιτούν ουσιαστική προσοχή ως προς την ασφάλεια. Αυτά τα έξι τμήματα είναι τα εξής:

1. Ασφάλεια δεδομένων σε αδράνεια (data-at-rest).
2. Ασφάλεια δεδομένων κατά την διαβίβαση (data-in-transit).
3. Επαλήθευση χρηστών/ εφαρμογών/ διαδικασιών.
4. Ισχυρός διαχωρισμός μεταξύ δεδομένων που ανήκουν σε ξεχωριστούς πελάτες.
5. Νομικά και ρυθμιστικά θέματα του νέφους.
6. Διαχείριση προβλήματος.



Εικόνα 6: Περιοχές όπου παρουσιάζονται ανησυχίες σχετικά με την ασφάλεια του cloud computing: (1) δεδομένα σε κατάσταση αδράνειας, (2) δεδομένα υπό διακομισμό, (3) πιστοποίηση ταυτότητας, (4) διαχωρισμός μεταξύ πελατών, (5) νομικά και ρυθμιστικά θέματα νέφους και (6) αντιμετώπιση περιστατικών. (Sen, 2013)

Η κρυπτογράφηση των δεδομένων και η χρήση ενός μη ασφαλισμένου πρωτοκόλλου (π.χ. “vanilla” ή “straight” FTP ή HTTP) μπορούν να παρέχουν εχεμύθεια, αλλά δεν διασφαλίζεται η ακεραιότητα των δεδομένων (π.χ. με την χρήση συμμετρικών κρυπταλγορίθμων ροής). Γνωρίζουμε πώς να κρυπτογραφήσουμε δεδομένα κατά τη διαβίβαση (data-in-transit) και δεδομένα σε αδράνεια (data-at-rest). Μολονότι η κρυπτογράφηση δεδομένων σε αδράνεια φαίνεται προφανής, στην πραγματικότητα δεν είναι

τόσο απλό. Κατά τη χρήση μίας IaaS υπηρεσίας cloud (δημόσιο ή ιδιωτικό) για απλή αποθήκευση (π.χ. Amazon Simple Storage Service), η κρυπτογράφηση δεδομένων σε αδράνεια είναι δυνατή και συνίσταται. Αντιθέτως, η κρυπτογράφηση δεδομένων σε αδράνεια, που χρησιμοποιεί μία PaaS ή SaaS υπηρεσία cloud (π.χ. Google Apps, Salesforce.com) ως εξισορρόπηση ελέγχου, δεν είναι πάντα εφικτό.

Τα δεδομένα σε αδράνεια που χρησιμοποιούνται από μία εφαρμογή βασισμένη σε cloud γενικά δεν είναι κρυπτογραφημένα, καθώς η κρυπτογράφηση θα απέτρεπε την καταλογογράφηση ή την αναζήτηση αυτών των δεδομένων. Τα δεδομένα, των οποίων η επεξεργασία ή η αποθήκευση γίνεται σε cloud βασισμένη εφαρμογή, αναμειγνύονται με δεδομένα άλλων χρηστών, καθώς συνήθως αποθηκεύονται σε πελώριες αποθήκες δεδομένων (π.χ. Google BigTable). Παρόλο που οι εφαρμογές είναι συχνά σχεδιασμένες με λειτουργίες όπως ετικέτες δεδομένων για την πρόληψη μη εξουσιοδοτημένης πρόσβασης σε αναμειγμένα δεδομένα, η εξουσιοδοτημένη πρόσβαση είναι πιθανή με την εκμετάλλευση κάποιων αδυναμιών της εφαρμογής (π.χ. η διανομή μη εξουσιοδοτημένων δεδομένων μεταξύ των χρηστών των Documents και Spreadsheets της Google τον Μάρτιο του 2009). Ενώ κάποιοι πάροχοι νέφους παραθέτουν τις εφαρμογές τους για αξιολόγηση σε τρίτους φορείς ή επαληθεύονται από εργαλεία προστασίας εφαρμογών τρίτων φορέων, τα δεδομένα δεν βρίσκονται σε πλατφόρμα που ανήκει αποκλειστικά σε έναν οργανισμό.

Τα in-transit δεδομένα μίας οργάνωσης μπορεί να κρυπτογραφηθούν κατά τη διάρκεια της μεταφοράς τους από και προς σε κάποιον πάροχο cloud, και τα in-rest δεδομένα μπορούν να κρυπτογραφηθούν κατά την διάρκεια της απλής αποθήκευσης (π.χ. εάν δεν έχουν συνδεθεί με κάποια εφαρμογής προδιαγραφών). Σίγουρα τα δεδομένα μιας επιχείρησης δεν κρυπτογραφούνται κατά την επεξεργασία τους στο νέφος (δημόσιο ή ιδιωτικό). Για να επεξεργαστεί τα δεδομένα κάποια εφαρμογή, θα πρέπει τα δεδομένα αυτά να είναι κρυπτογραφημένα. Έως τον Ιούνιο του 2009 δεν υπήρχε γνώστη μέθοδος ολικής επεξεργασίας κρυπτογραφημένων δεδομένων. Επομένως, τα δεδομένα θα κρυπτογραφηθούν τουλάχιστον σε κάποιο μέρος του κύκλου ζωής τους κατά τη διάρκεια επεξεργασίας στο νέφος, εκτός εάν τα δεδομένα βρίσκονται στο cloud για απλή αποθήκευση.

Ακόμα και οι προσπάθειες επαρκούς διαχείρισης κρυπτογραφημένων δεδομένων είναι υπερβολικά περίπλοκες και προβληματικές εξαιτίας της τρέχουσας ανεπάρκειας των δυνατοτήτων των προϊόντων διαχείρισης κλειδιών (Key Management Products). Η διαχείριση κλειδιών στο ενδο-επιχειρησιακό πλαίσιο είναι από μόνη της αρκετά δύσκολη. Η επαρκής διαχείριση κλειδιών στο cloud είναι πέρα των σημερινών δυνατοτήτων και απαιτεί σημαντική εξέλιξη τόσο στην κρυπτογράφηση όσο και στην ίδια την διαχείριση κλειδιών.

Οι ανησυχίες για την ασφάλεια των δεδομένων δεν καταργούν τις δυνατότητες ή τα πλεονεκτήματα της αξιοποίησης της «αποθήκευσης ως υπηρεσία» στο νέφος, για μη ευαίσθητα ή μη ελεγχόμενα δεδομένα. Εάν οι πελάτες θέλουν απλά την αποθήκευση δεδομένων στο cloud, θα πρέπει να πάρουν ρητά μέτρα, ή τουλάχιστον να επαληθεύσουν ότι ο πάροχος θα παρέχει επαρκώς τις υπηρεσίες που χρειάζονται για την ασφαλή αποθήκευση των δεδομένων στο νέφος (Pandith, 2014).

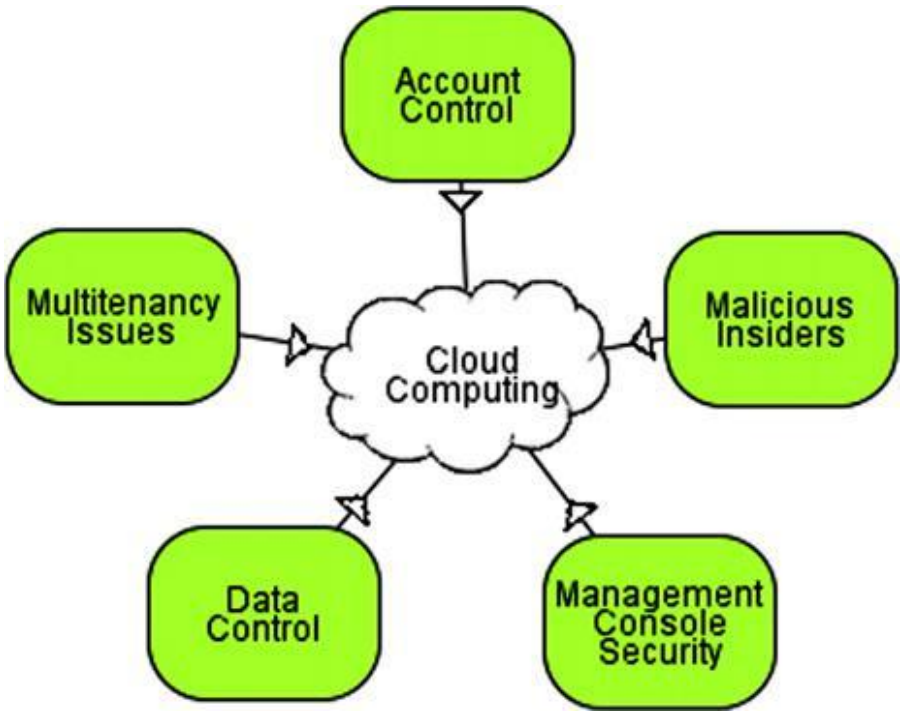
1.4 **ΑΝΗΣΥΧΙΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ**

Η ιδιωτικότητα έχει πολλές σημασίες για πολλούς ανθρώπους. Συνεπώς, αυτό το κοινωνικό φαινόμενο περιτριγυρίζεται από έντονες συζητήσεις ως προς τι στην ουσία είναι ιδιωτικότητα και τι ακριβώς σημαίνει; Οι ερωτήσεις ως προς αυτό το θέμα, έχουν ξεχωριστές απαντήσεις, αναλόγως τις διαφορετικές φιλοσοφικές προσεγγίσεις και τις θεωρητικές απόψεις του ορισμού των αξιών της ιδιωτικότητας μέσα στην κοινωνία. Η επικρατέστερη άποψη βασίζεται στην φιλελεύθερη πολιτική θεωρία, που υποστηρίζει πως μία φιλελεύθερη οντότητα εμπεριέχει την ικανότητα της ορθολογικής συζήτησης και επιλογής. Από την άλλη μεριά, η Anita Allen υποστηρίζει ότι η ιδιωτικότητα είναι η ύπαρξη θετικών ελευθεριών όπως για παράδειγμα ότι κάποιος είναι ελεύθερος να αποφύγει ανεπιθύμητες αποκαλύψεις, δημοσιότητα και την απώλεια ελέγχου της προσωπικότητάς του.

Από τις παραπάνω έννοιες, έχουν προκύψει πολλαπλές θεωρίες που επικεντρώνονται στην ιδιωτικότητα σε σχέση με την αυτονομία, την προσωπικότητα, την μυστικότητα, την ελευθερία κλπ.

Οι Warren και Brandeis στο επιδραστικό τους άρθρο «Το δικαίωμα στην ιδιωτικότητα» έθεσαν την ιδέα της ιδιωτικότητας ως το δικαίωμα των πολιτών σε μία ανενόχλητη και ήσυχη ιδιωτική ζωή.

Όλοι οι άνθρωποι ανεξαρτήτως ηλικίας ενδιαφέρονται για ερωτήματα που αφορούν την προστασία της ιδιωτικότητας, όπως: Ποιος διαχειρίζεται και έχει πρόσβαση στα δεδομένα; Πού αποθηκεύονται; Γνωρίζουμε πότε υπάρχει παραβίαση δεδομένων;



Εικόνα 7: Κατηγοριοποίηση ανησυχιών ιδιωτικότητας (Zissis & Lekkas, 2010)

Μερικές ανησυχίες για την προστασία του απορρήτου είναι εξής:

1. Ποιος διαχειρίζεται και έχει πρόσβαση στα δεδομένα; Τα δεδομένα θα παραμείνουν στο νέφος ακόμα και μετά από την διακοπή της υπηρεσίας;
   Σε αντίθεση με ένα κέντρο δεδομένων, του οποίου η διαχείριση γίνεται από το τμήμα πληροφορικής της ίδιας της επιχείρησης, το νέφος είναι μία εξωτερική - τρίτη υπηρεσία στην οποία οι χρήστες αναθέτουν την κάλυψη των αναγκών των δεδομένων τους. Συνεπώς, ο πάροχος γίνεται αυτόματα υπεύθυνος για όλες τις λειτουργίες, από τις ενημερώσεις και την συντήρηση έως και την διαχείριση της ασφάλειας. Αυτό, ουσιαστικά, σημαίνει ότι οι χρήστες εμπιστεύονται τα δικά τους δεδομένα σε κάποιον «ξένο», σύμφωνα με τα λόγια του Steve Santorelli, ενός πρώην μέλους της Scotland Yard και νυν υπεύθυνος πληροφοριών και ενίσχυσης της ερευνητικής ομάδας ασφάλειας διαδικτύου «Cymru».

   «Το μειονέκτημα είναι ότι ο χρήστης ανακαλεί την ευθύνη του για τα δεδομένα του. Κάποιος άλλος έχει πρόσβαση και την ευθύνη της ασφάλειάς τους.», αναφέρει ο Santorelli.

   Επίσης υποστηρίζει ότι παρότι οι πάροχοι νέφους μπορούν να διασφαλίσουν ασφάλεια, μερικοί δεν φροντίζουν πάντα τα συμφέροντα του χρήστη.

   «Καμία επιχείρηση δεν πρόκειται να είναι τόσο προσεκτική με την φύλαξη των δεδομένων σας όπως θα ήσασταν ή θα έπρεπε να είστε εσείς οι ίδιοι. Άλλωστε, ο μόνος στόχος τους είναι να κερδίζουν χρήματα από εσάς. Μερικές φορές η εξασφάλιση των δεδομένων σας γίνεται περισσότερο ένα μάρκετινγκ μάντρα παρά οτιδήποτε άλλο» συμπληρώνει.

   Ένας άλλος μεγάλος προβληματισμός είναι οι εσωτερικές παραβιάσεις ασφαλείας.
   «Η παραβίαση των δύο εκατομμυρίων αρχείων πελατών από την Vodafone ή η παραβίαση από τον Edward Snowden στην NSA είναι υπενθυμίσεις ότι οι σημαντικότερες παραβιάσεις γίνονται εσωτερικά » σημειώνει ο Eric Chiu, πρόεδρος και συνιδρυτής της εταιρείας ελέγχου υποδομών νεφοϋπολογιστικής HyTrust,
   Από την στιγμή που ένας εργαζόμενος αποκτήσει ο ίδιος ή δώσει σε κάποιον άλλον πρόσβαση στο cloud του χρήστη, οτιδήποτε βρίσκεται εκεί, από δεδομένα έως και απόρρητες πληροφορίες, είναι ευαίσθητο σε υποκλοπές.

   Σύμφωνα με τον Chiu, αυτό το πρόβλημα γίνεται δεκάδες φορές χειρότερο στο νέφος, καθώς η πρόσβαση στην πλατφόρμα διαχείρισης του cloud επιτρέπει την αντιγραφή και κλοπή οποιουδήποτε εικονικού μηχανήματος, χωρίς να γίνει αντιληπτό, ή ακόμα και να καταστρέψει ολόκληρο το περιβάλλον cloud μέσα σε λίγα λεπτά. (Angeles, 2013)

   Ενώ η ασφάλεια των δεδομένων συνήθως σχετίζεται με την προστασία και την διατήρηση του απορρήτου των δεδομένων, οφείλουμε να αναφέρουμε ότι και η διαγραφή τους είναι μία εξίσου σημαντική πτυχή της διαχείρισης και της προστασίας των ευαίσθητων πληροφοριών. Στην πραγματικότητα, είναι ένα βασικό στοιχείο στην διασφάλιση της εμπιστευτικότητας. Η ατελής διαγραφή δεδομένων μπορεί να οδηγήσει σε μία απροσδόκητη έκθεση των δεδομένων των χρηστών. Οι ασφαλείς μέθοδοι διαγραφής είναι διαφορετικές και έχουν διαφορετική συμπεριφορά. Η διαγραφή θεωρείται επιτυχής όταν κάποιος που έχει πρόσβαση στο σύστημα δεν είναι

πλέον σε θέση να ανακτήσει διαγεγραμμένα δεδομένα. (Ramokapane, et al., n.d.)

2. Τα νομικά και ρυθμιστικά ζητήματα είναι τόσο μεγάλης σημασίας στο Cloud Computing που προκαλούν επιπτώσεις στην ασφάλεια. Για να εξακριβωθεί ότι ένας πάροχος cloud έχει ισχυρές πολιτικές και πρακτικές για την αντιμετώπιση αυτών των ζητημάτων, ο εμπειρογνώμονας της κάθε εταιρείας θα πρέπει να ελέγχει τις πολιτικές και πρακτικές του παρόχου ώστε να διασφαλίζεται η αρτιότητα. Τα ζητήματα που ελέγχονται σε τέτοιες περιπτώσεις εμπεριέχουν την ασφάλεια και την εξαγωγή των δεδομένων, τη συμβατότητα, τον έλεγχο, τη φύλαξη και την καταστροφή των δεδομένων και τη νομική επισήμανση. Στον τομέα της φύλαξης και της καταστροφής των δεδομένων, η αξιόπιστη αποθήκευση και οι tpm [5] τεχνικές διαδραματίζουν σημαντικό ρόλο στην περιορισμένη πρόσβαση ευαίσθητων και μεγάλης σημασίας δεδομένων.

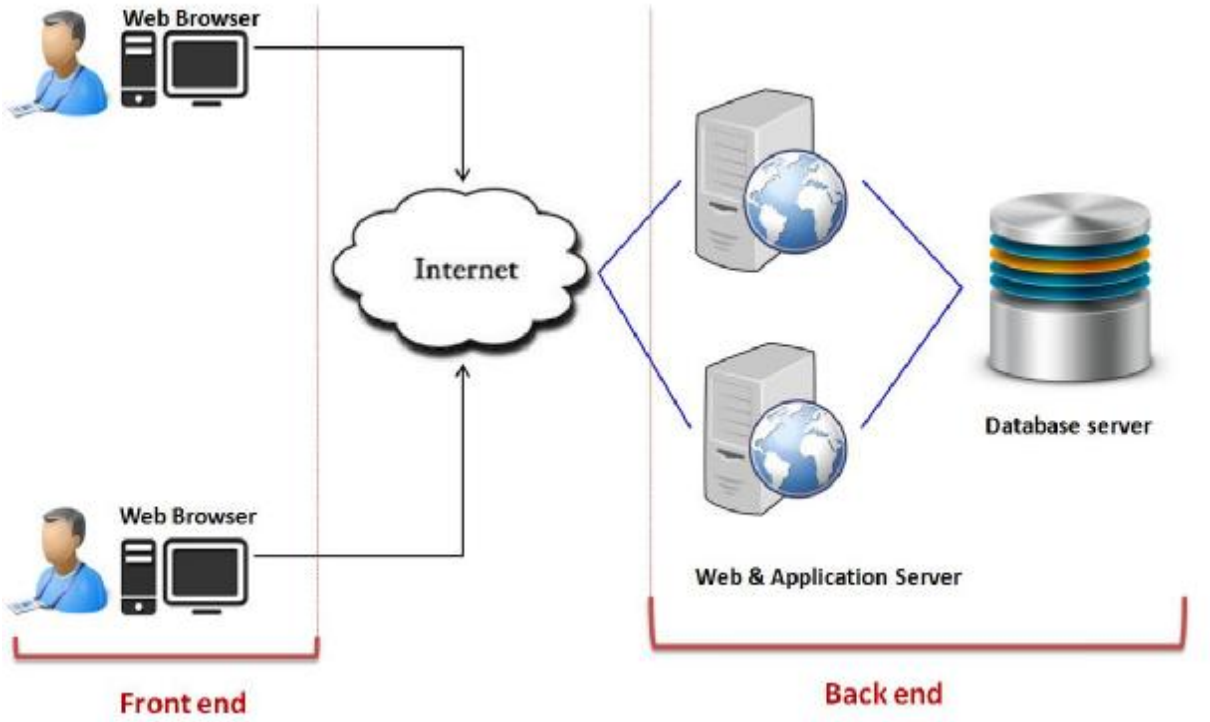
3. Πού αποθηκεύονται τα δεδομένα στο cloud; Ποια είναι η τοποθεσία του κέντρου δεδομένων;
   Οι νομοθεσίες απορρήτου σε πολλές χώρες ορίζει όρια στην ικανότητα των οργανισμών να μεταφέρουν μερικούς τύπους προσωπικών δεδομένων σε άλλες χώρες. Όταν τα δεδομένα αποθηκεύονται στο νέφος, η μεταφορά τέτοιου είδους μπορεί να πραγματοποιηθεί χωρίς να λάβει γνώση ο ίδιος ο οργανισμός, με επακόλουθο την δυνητική παράβαση της τοπικής νομοθεσίας.

4. Λαμβάνετε γνώση για την παραβίαση των δεδομένων; Πώς μπορεί κάποιος να βεβαιωθεί ότι ο πάροχος υπηρεσιών Νέφους ειδοποιεί τους πελάτες όταν γίνεται παραβίαση, και ποιος είναι υπεύθυνος για την διαχείριση της διαδικασίας ειδοποιήσεων παραβίασης, καθώς και των εξόδων που συνδέονται με την συγκεκριμένη διαδικασία; Εάν το συμβόλαιο εμπεριέχει ανάληψη ευθύνης για παραβίαση που προέρχεται από αμέλεια του παρόχου, πώς εφαρμόζεται το συμβόλαιο και πώς αποφασίζεται ο υπεύθυνος;

5. Τα δεδομένα θα παραμείνουν στο cloud και μετά την διαγραφής τους, καθώς οι πάροχοι cloud συνήθως δημιουργούν αντίγραφα δεδομένων σε πολλαπλά συστήματα και sites, εφόσον η αυξημένη διαθεσιμότητα είναι ένα από τα πλεονεκτήματα που προσφέρουν; Το προνόμιο γίνεται πρόκληση όταν ο οργανισμός προσπαθεί να καταστρέψει τα δεδομένα. Άρα είναι δυνατόν να καταστραφούν οι πληροφορίες από την στιγμή που βρίσκονται στο νέφος; (Pandith, 2014)

[5] Trusted Platform Modules (tpm): εξειδικευμένο chip σε μία endpoint συσκευή που αποθηκεύει RSA κλειδιά κρυπτογράφησης του κεντρικού υπολογιστή για τον έλεγχο ταυτότητας του hardware. (Rouse, 2014)

1.5 **ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ** CLOUD COMPUTING



Εικόνα 8: Αρχιτεκτονική νέφους (Anon., n.d.)

Το Cloud Computing βελτιώνει την συνεργασία, την ευκινησία, την κλίμακα και την διαθεσιμότητα και παρέχει τη δυνατότητα μείωσης κόστους μέσω της τελειοποίησης και αποτελεσματική υπολογιστική. Πιο συγκεκριμένα, το νέφος περιγράφεται από τη χρήση μίας συλλογής διανεμημένων υπηρεσιών, εφαρμογών, πληροφοριών και υποδομών που συγκροτούνται από ομάδες υπολογιστικών, δικτυακών, πληροφοριακών και αποθηκευτικών πηγών. Αυτά τα «συστατικά» μπορούν ραγδαία να συντονιστούν, να εφοδιαστούν, να εφαρμοστούν και να τεθούν εκτός λειτουργίας χρησιμοποιώντας ένα on-demand δικτυακό μοντέλο κατανομής και κατανάλωσης. Οι υπηρεσίες νέφους είναι συνήθως, αν και όχι πάντα, αξιοποιημένες σε συνδυασμό με ψηφιακές τεχνολογίες, ώστε να παρέχουν δυναμική ενσωμάτωση, εφοδιασμό, συντονισμό, κινητικότητα και κλίμακα.

Ενώ εξ ορισμού το νέφος υποδηλώνει τον διαχωρισμό των πηγών από την φυσική συνάφεια και τοποθεσία των υποδομών που τις διανέμει, πολλές περιγραφές του νέφους φτάνουν στο ένα άκρο ή στο άλλο, είτε υπερβάλλοντας είτε περιορίζοντας με τεχνάσματα πολλά χαρακτηριστικά του cloud. Αυτό συνήθως γίνεται εσκεμμένα σε μία προσπάθεια φουσκώματος ή περιθωριοποίησης του πεδίου του. Μερικά παραδείγματα περιλαμβάνουν την πρόταση ότι για να είναι η υπηρεσία βασισμένη στο νέφος, το Internet πρέπει να χρησιμοποιείται ως μέσο, ο web browser ως μέθοδος απεικόνισης πρόσβασης ή ότι οι πόροι πάντα μοιράζονται σε ένα πολλαπλά ενοικιαζόμενο περιβάλλον έξω από την «παράμετρο». Αυτό που λείπει από τους συγκεκριμένους ορισμούς είναι το ευρύτερο πλαίσιο.

Από αρχιτεκτονικής άποψης, δεδομένου αυτής της αφηρημένης τεχνολογικής εξέλιξης, υπάρχει μεγάλη σύγχυση γύρω από το πώς το cloud είναι ταυτόχρονα τόσο ίδιο αλλά και τόσο διαφορετικό από τα ήδη υπάρχοντα μοντέλα και πως αυτές οι ομοιότητες και διαφορές επηρεάζουν την οργανωτική, λειτουργική και τεχνολογική προσέγγιση στην αποδοχή του

νέφους, εφόσον συσχετίζεται με τα παραδοσιακά δίκτυα και τις τεχνικές ασφάλειας δεδομένων. Υπάρχουν αυτοί που ισχυρίζονται ότι το cloud είναι μία ριζική αλλαγή και μία τεχνική επαναστάτη, ενώ κάποιοι θεωρούν ότι είναι η φυσική εξέλιξη και η συνέπεια της συνένωσης τεχνολογίας, οικονομίας και κουλτούρας. Η αλήθεια βρίσκεται κάπου στη μέση.
Σήμερα υπάρχουν πολλά διαθέσιμα μοντέλα που προσπαθούν να αναλύσουν το Cloud από την ακαδημαϊκή, αρχιτεκτονική, μηχανική, προγραμματιστική, διαχειριστική, ακόμα και από την πελατειακή πλευρά. Εδώ θα επικεντρωθούμε στην πλευρά των IT δικτύων ανάπτυξης και παροχής υπηρεσιών.

Οι υπηρεσίες Cloud είναι βασισμένες πάνω σε πέντε βασικά χαρακτηριστικά που δείχνουν τις σχέσεις και τις διαφορές τους με τις παραδοσιακές πληροφοριακές προσεγγίσεις. Αυτά τα χαρακτηριστικά είναι τα εξής:

1. Αφαίρεση υποδομών: οι υπολογιστικές, δικτυακές και αποθηκευτικές υποδομές πόρων αφαιρούνται από την εφαρμογή και τις πηγές πληροφοριών ως συνάρτηση της παροχής υπηρεσιών. Το που και σε τι φυσικό πόρο γίνεται η επεξεργασία, μεταφορά και αποθήκευση των δεδομένων γίνεται θολό από την μεριά της εφαρμογής ή την δυνατότητα της υπηρεσίας να τα παρέχει. Οι υποδομές των πόρων γενικά μοιράζονται έτσι ώστε να παρέχεται η υπηρεσία ανεξάρτητα από το ενοικιασμένο μοντέλο που απασχολείται, κοινόχρηστο ή μη. Αυτή η αφαίρεση συνήθως γίνεται μέσω υψηλών επιπέδων εικονικοποίησης στο chipset[6] και στα επίπεδα λειτουργικών συστημάτων ή ενεργοποιείται στα υψηλοτέρα επίπεδα μέσω των προσαρμοσμένων συστημάτων αρχειοφακέλων, λειτουργικών συστημάτων ή πρωτοκόλλων επικοινωνίας.

2. Εκδημοκρατισμός πόρων: Η αφαίρεση των υποδομών δίνει προτεραιότητα στην ιδέα του εκδημοκρατισμού των πόρων (υποδομές, εφαρμογές ή πληροφορίες) και παρέχει την ικανότητα στους μοιρασμένους πόρους να γίνουν προσβάσιμοι στον οποιοδήποτε που είναι εξουσιοδοτημένος χρησιμοποιώντας τις απαραίτητες τυποποιημένες μεθόδους.

3. Αρχιτεκτονική υπηρεσιών: Όπως και η αφαίρεση υποδομών στις εφαρμογές και τις πληροφορίες δίνει προτεραιότητα στην σαφή και χαλαρή σύζευξη του εκδημοκρατισμού των πόρων, την ιδέα της χρήσης αυτών των συστατικών εξ ολοκλήρου ή μερικώς, σαν μονάδα ή σε συνεργασία, παρέχει μία αρχιτεκτονική υπηρεσιών όπου οι πόροι μπορούν να γίνουν προσβάσιμοι και να χρησιμοποιηθούν με έναν μέσο τρόπο. Σε αυτό το μοντέλο, το επίκεντρο είναι η παροχή της υπηρεσίας και όχι η διαχείριση των υποδομών.

4. Ελαστικότητα/Δυναμισμός: Το on-demand μοντέλο της παροχής νέφους μαζί με την υψηλού επιπέδου αυτοματοποίηση, την εικονικοποίηση, την ευρεία διάδοση, την αξιοπιστία και την υψηλής ταχύτητας συνδεσιμότητα δίνει τη δυνατότητα ραγδαίας επέκτασης ή συστολής καταμερισμού πόρων στην καθορισμένη υπηρεσία και στις καθορισμένες προδιαγραφές, χρησιμοποιώντας ένα μοντέλο αυτοεξυπηρέτησης που κλιμακώνεται στην χωρητικότητα σύμφωνα με τις ανάγκες.

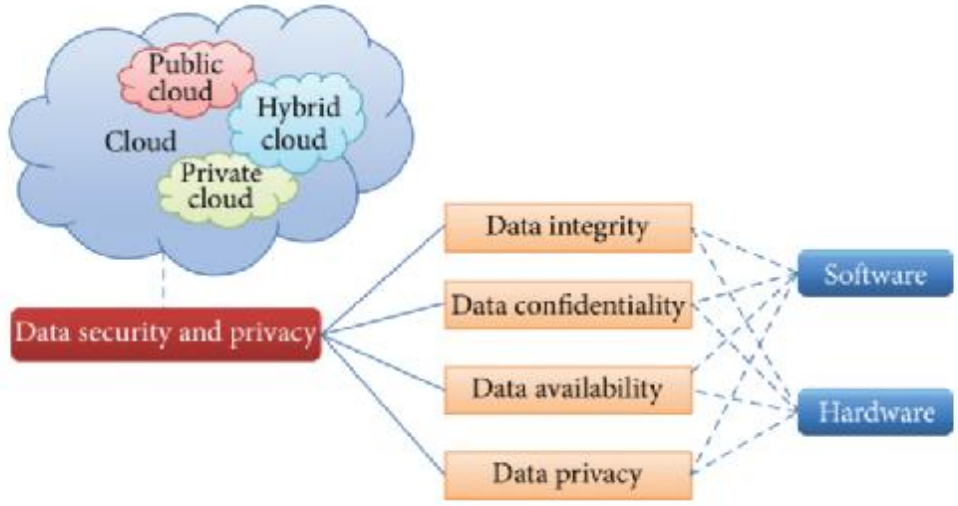
[6] Chipset: Σειρά εξειδικευμένων ολοκληρωμένων κυκλωμάτων πάνω στη μητρική πλακέτα του υπολογιστή. (Anon., 2003)

5. Υπόδειγμα Χρησιμότητας Κατανάλωσης και Καταμερισμού: Η αφηρημένη, εκδημοκρατισμένη, υπηρεσίο-κεντρική και ελαστική φύση του cloud σε συνδυασμό με την αυστηρή αυτοματοποίηση, ενορχήστρωση, τροφοδοσία και αυτοεξυπηρέτηση επιτρέπει τον δυναμικό καταμερισμό των πόρων, βασισμένο σε οποιοδήποτε αριθμό διακυβερνητικών εισερχόμενων παραμέτρων. Δεδομένου της ορατότητας σε ατομικό επίπεδο, η κατανάλωση των πόρων μπορεί έπειτα να χρησιμοποιηθεί για παροχή ενός διαιρούμενου κόστους χρήσης μοντέλου. Έτσι, διευκολύνεται ένα αποδοτικότερο, καλύτερα κλιμακούμενο, εύχρηστο και εύκολα προβλεπόμενο κόστος (Sen, 2013).

1.6 **ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ** CLOUD

Εικόνα 9: Απειλές ασφαλείας (Avatier, 2018)

*'*Όπως προαναφέραμε, οι απειλές δεν είναι πάντα ίδιες για τις πληροφορίες-δεδομένα που διαμένουν στο νέφος, αλλά διαφέρουν ανάλογα με το είδος των μοντέλων υπηρεσιών που έχει επιλεχθεί από τις επιχειρήσεις που χρησιμοποιούν υπηρεσίες cloud. Υπάρχουν αρκετά είδη απειλών ασφαλείας στην νεφοϋπολογιστική, τα οποία θα τα κατηγοριοποιήσουμε σύμφωνα με το μοντέλο ασφαλείας «Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα - CIA» και σε συνάρτηση με το κάθε μοντέλο υπηρεσιών.



Εικόνα 10: Οργάνωση ασφάλειας και ιδιωτικότητας των δεδομένων στο cloud computing (Sun, et al., 2014)

1.6.1 **Εμπιστευτικότητα** (Confidentiality)

Η εμπιστευτικότητα αναφέρεται στην είσοδο των προστατευμένων δεδομένων μόνο από τους εξουσιοδοτημένους συνεργάτες και συστήματα. Η απειλή της διακινδύνευσης των δεδομένων στο cloud πολλαπλασιάζεται, εξαιτίας του αυξημένου αριθμού συνεργατών, συσκευών και εφαρμογών που εμπλέκονται, καθώς όλα αυτά τα μέσα οδηγούν σε έναν μεγαλύτερο αριθμό σημείων πρόσβασης. Γενικά, η ανάθεση της προστασίας των δεδομένων στο νέφος, αντιθέτως οδηγεί σε αυξημένη διακινδύνευση πληροφοριών, είτε από εσωτερικούς παράγοντες, είτε από εξωτερικούς, πράγμα που είναι φυσικό όταν τα δεδομένα γίνονται προσβάσιμα από περισσότερες πλευρές. Κάποιες από τις ανησυχίες που αναδύονται είναι βασισμένες στις εσωτερικές απειλές από άμεσα εμπλεκομένους στην διαχείριση των πληροφοριών, στην ταυτόχρονη πολύ-μίσθωση και πολύ-προσβασιμότητα του χώρου στο νέφος, στα «υπολείμματα» διαγεγραμμένων δεδομένων, στην ασφάλεια των εφαρμογών και στην ιδιωτικότητα.

Εικόνα 11: Η εμπιστευτικότητα είναι μια από τις μεγαλύτερες ανησυχίες των χρηστών του cloud computing (Richardson, n.d.)

Άμεσα εμπλεκόμενοι με την διαχείριση πληροφοριών, όπως έχουμε ήδη αναφέρει, είναι ο πάροχος του νέφους, οι πελάτες-χρήστες του cloud και οι τρίτοι συνεργάτες από την μεριά του παρόχου υπηρεσιών ή από την μεριά του πελάτη. Όλοι οι παραπάνω θεωρούνται εν δυνάμει εσωτερικοί hacker. Η απειλή πρόσβασης δεδομένων πελατών, τα οποία βρίσκονται στο νέφος, από κάποιον εσωτερικό εισβολέα, είναι μεγαλύτερη καθώς κάθε μοντέλο υπηρεσιών έχει την δυνατότητα να παρουσιάσει την ανάγκη για πολλαπλούς εσωτερικούς χρήστες. Ειδικότερα, το μοντέλο SaaS αποτελείται από τον πελάτη του νέφους και τους διαχειριστές παροχών. Το μοντέλο PaaS αποτελείται από τους προγραμματιστές των εφαρμογών και τους υπεύθυνους διοίκησης περιβάλλοντος. Το μοντέλο IaaS αποτελείται από τους εξωτερικούς συμβούλους πλατφόρμας, οι οποίοι προσφέρουν υποστήριξη είτε στον πάροχο cloud είτε στις επιχειρήσεις-πελάτες.

Η ταυτόχρονη πολύ-μίσθωση βασίζεται στο χαρακτηριστικό της κοινής χρήσης των πόρων του cloud. Πολλές πλευρές των πληροφοριακών συστημάτων χρησιμοποιούνται από κοινού, όπως η μνήμη, τα προγράμματα, τα δίκτυα και τα δεδομένα. Η νεφοϋπολογιστική είναι δομημένη πάνω σε ένα επιχειρησιακό σχέδιο, όπου οι πόροι μοιράζονται -για παράδειγμα πολλαπλοί χρήστες χρησιμοποιούν τους ίδιους πόρους- στο δικτυακό επίπεδο, στο host επίπεδο, και στο επίπεδο της εφαρμογής. Παρόλο που οι χρήστες στο εικονικό πεδίο είναι απομονωμένοι, στον hardware τομέα όμως ουσιαστικά δεν είναι διαχωρισμένοι. Με αυτή την πολυ-μισθωτική αρχιτεκτονική, μία software εφαρμογή είναι σχεδιασμένη να διχοτομεί τα δεδομένα και τις παραμετρικές ρυθμίσεις, έτσι ώστε ο κάθε πελάτης να χειρίζεται μία εξατομικευμένη εικονικά περίπτωση εφαρμογής. Μπορούμε να πούμε ότι η πολύ-μίσθωση είναι συναφής με την πολυδιεργασία[7] στα λειτουργικά συστήματα, καθώς και στα δύο παρουσιάζεται ένας αριθμός από απειλές στην ιδιωτικότητα και στην εμπιστευτικότητα. Για παράδειγμα, η απειλή μίας εκτενής διαρροής δεδομένων από χρήστες που χρησιμοποιούν τον ίδιο πάροχο νέφους (οι οποίοι μπορούν κάλλιστα να είναι και ανταγωνιστές), είναι πιθανόν να προκληθεί είτε από ανθρώπινο λάθος, είτε από περίπτωση ελαττωματικού hardware, και θα έχει ως αποτέλεσμα την διαρροή σημαντικών πληροφοριών. Η επαναχρησιμοποίηση αντικειμένου είναι ένα σημαντικό χαρακτηριστικό των υποδομών του νέφους, όμως

[7] Πολυδιεργασία (Multitasking): Στην πληροφορική η πολυδιεργασία είναι μία μέθοδος με την οποία πολλαπλές διεργασίες μοιράζονται κοινούς πόρους επεξεργασίας, π.χ. CPU.

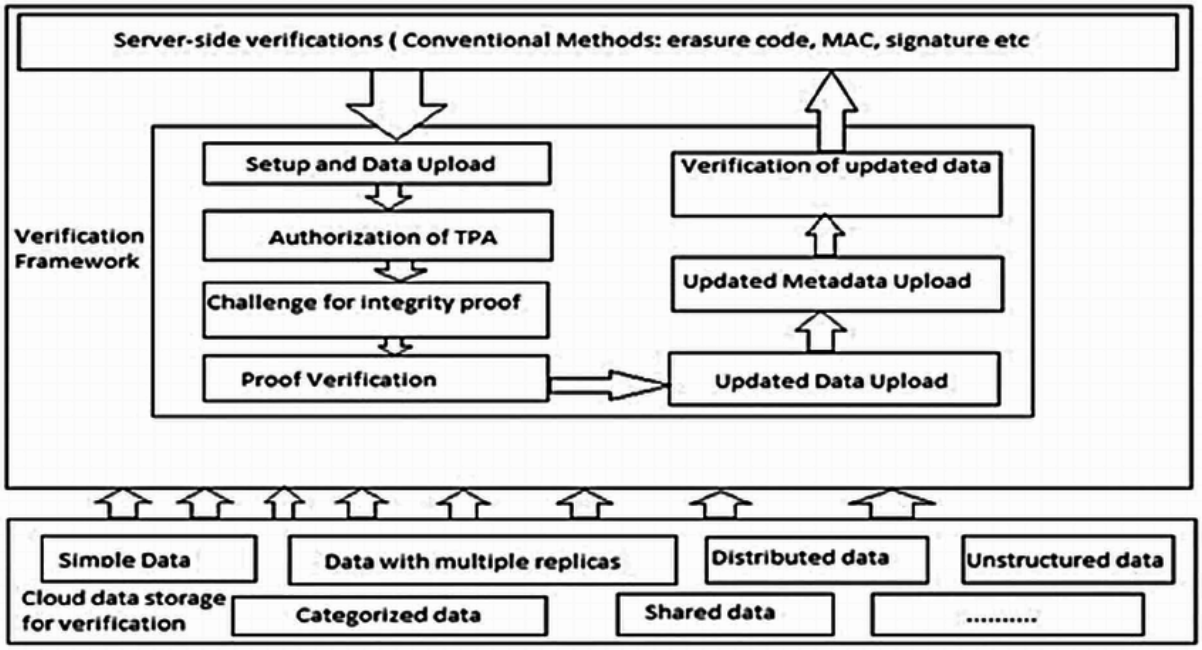
καθίσταται αναγκαίο τα επαναχρησιμοποιούμενα αντικείμενα να ελέγχονται προσεχτικά, προς αποφυγήν δημιουργίας σοβαρότερης αδυναμίας. Είναι πιθανόν η εμπιστευτικότητα των δεδομένων να παραβιαστεί εκ παραδρομής, εξαιτίας των «υπολειμμάτων». Τα «υπολείμματα» δεδομένων είναι η αναπαράσταση των εναπομεινασών δεδομένων, τα οποία είχαν εν μέρει διαγραφεί ή αφαιρεθεί πλασματικά. Ένεκα του εικονικού διαχωρισμού των λογικών drives και της έλλειψης διαχωρισμού του hardware μεταξύ πολλαπλών χρηστών σε μία μόνο υποδομή, τα υπολείμματα δεδομένων μπορούν να οδηγήσουν στην απρόθυμη κοινοποίηση των προσωπικών πληροφοριών.

Η εμπιστευτικότητα στο Software επίπεδο είναι τόσο σημαντική όσο η εμπιστευτικότητα των δεδομένων σε όλο το σύστημα ασφαλείας. Εμπιστευτικότητα στο Software ορίζεται ως η εμπιστοσύνη ότι συγκεκριμένες εφαρμογές ή διεργασίες διατηρούν και διαχειρίζονται τα προσωπικά δεδομένα των χρηστών με έναν ασφαλή τρόπο. Σε ένα περιβάλλον νέφους ο χρήστης είναι υποχρεωμένος να εναποθέσει «εμπιστοσύνη» στις εφαρμογές που παρέχονται από την επιχείρηση στην οποία ανήκουν οι υποδομές. Οι Software εφαρμογές οφείλουν να είναι πιστοποιημένα ασφαλείς, δηλαδή ότι δε θα παρουσιάσουν επιπρόσθετα ρίσκα στους τομείς της εμπιστευτικότητας και της ιδιωτικότητας. Η μη εξουσιοδοτημένη πρόσβαση μπορεί να γίνει πιθανή μέσω της εκμετάλλευσης μίας αδυναμίας της εφαρμογής ή την έλλειψη ισχυρής ταυτοποίησης, το οποίο μπορεί να επιφέρει θέματα στην εμπιστευτικότητα και την ιδιωτικότητα των δεδομένων. Εδώ οφείλουμε να τονίσουμε ότι τέτοιου είδους απειλές είναι περισσότερο πιθανές στο δημόσιο νέφος, όπου τα σημεία σύνδεσης των χρηστών μπορούν να γίνουν εύκολα στόχος. Οι πάροχοι cloud με μεγάλες αποθήκες δεδομένων, που εμπεριέχουν αριθμούς και πληροφορίες πιστωτικών καρτών, προσωπικά δεδομένα και ευαίσθητης φύσης κυβερνητική ή πνευματική ιδιοκτησία, μπορούν να γίνουν στόχος επιθέσεων από ομάδες με σημαντικούς πόρους, που έχουν ως σκοπό την ανάκτηση τέτοιου είδους δεδομένων. Αυτό εμπεριέχει και την απειλή hardware επίθεσης, κοινωνικής μηχανικής [8] και επίθεσης στα συστήματα διαχείρισης από «αφοσιωμένους» εισβολείς. Συνεπώς, ο πάροχος νέφους είναι υπεύθυνος για την παροχή ασφαλούς παρουσίας cloud, η οποία πρέπει να εξασφαλίζει ιδιωτικότητα στον χρήστη.

Ιδιωτικότητα είναι η επιθυμία ενός ατόμου να ελέγχει την δημοσιοποίηση των προσωπικών του πληροφοριών. Οι επιχειρήσεις που ασχολούνται με την διαχείριση των προσωπικών δεδομένων είναι απαραίτητο να ακολουθούν το νομικό πλαίσιο, που εξασφαλίζει την κατάλληλη ασφάλιση της ιδιωτικότητας και την εμπιστευτικότητας, της χώρας στην οποία βρίσκονται. Το νέφος παρουσιάζει ένα πλήθος νομικών προκλήσεων απέναντι στα θέματα ιδιωτικότητας που προέρχονται από το γεγονός ότι τα δεδομένα αποθηκεύονται σε πολλαπλές τοποθεσίες μέσα στο νέφος, κάτι που αυξάνει τον κίνδυνο παραβίασης της εμπιστευτικότητας και της ιδιωτικότητας. Αντί τα δεδομένα να αποθηκεύονται στους servers του χρήστη, αποθηκεύονται στους servers του παρόχου υπηρεσιών, οι οποίοι μπορεί να βρίσκονται στην Ασία, στην Ευρώπη ή οπουδήποτε αλλού. Αυτό το στοιχείο της νεφοϋπολογιστικής έρχεται σε σύγκρουση με διάφορες νομικές προϋποθέσεις, όπως για παράδειγμα με τους Ευρωπαϊκούς νόμους οι οποίοι προϋποθέτουν ότι οι επιχειρήσεις γνωρίζουν καθ' όλη τη διάρκεια που βρίσκονται τα δεδομένα που έχουν στην κατοχή τους.

[8] Η μέθοδος εξαπάτησης ενός χρήστη να δώσει πρόσβαση σε ευαίσθητες πληροφορίες παρακάμπτοντας με αυτόν τον τρόπο το μεγαλύτερο μέρος ή ακόμα και όλο το σύστημα προστασίας.

1.6.2 **Ακεραιότητα** (Integrity)



Εικόνα 12: Σύντομη περιγραφή της ακεραιότητας στο υπολογιστικό νέφος. (Shukla & Dixit, 2015)

Ένα βασικό στοιχείο της ασφάλειας των πληροφοριών είναι η ακεραιότητα. Η ακεραιότητα ορίζει ότι οι πληροφορίες τροποποιούνται μόνο από εξουσιοδοτημένους εμπλεκόμενους ή με εξουσιοδοτημένους τρόπους και αφορά τα δεδομένα, το software και το hardware.

Η ακεραιότητα δεδομένων αναφέρεται στην προστασία των δεδομένων από μη εξουσιοδοτημένη διαγραφή, τροποποίηση ή αναπαραγωγή. Η διαχείριση της άδειας εισόδου και των δικαιωμάτων σε συγκεκριμένες επιχειρησιακές πληροφορίες εξασφαλίζει ότι τα πολύτιμα δεδομένα και υπηρεσίες δεν καταχρώνται, υπεξαιρούνται ή υποκλέπτονται. Η παρεμπόδιση της μη εξουσιοδοτημένης πρόσβασης επιτυγχάνει μεγαλύτερη εμπιστοσύνη στην ακεραιότητα των δεδομένων και του συστήματος. Επιπροσθέτως, ένας τέτοιος μηχανισμός προσφέρει σπουδαιότερη ορατότητα στον καθορισμό του ποιος ή τι έχει τροποποιήσει δεδομένα ή πληροφορίες, αφού μία τέτοια τροποποίηση ενδεχομένως να επηρεάσει την αξιοπιστία-ακεραιότητα. Η εξουσιοδότηση είναι ο μηχανισμός με τον οποίο ένα σύστημα καθορίζει το επίπεδο πρόσβασης που ένας συγκεκριμένος εξουσιοδοτημένος χρήστης μπορεί να έχει στους ασφαλισμένους πόρους που ελέγχονται από το σύστημα. Εξαιτίας του αυξημένου αριθμού οντοτήτων και σημείων πρόσβασης στο περιβάλλον του νέφους, η εξουσιοδότηση καθίσταται κρίσιμη για την εξασφάλιση αλληλεπίδρασης των δεδομένων αυστηρά μόνο με εξουσιοδοτημένες οντότητες.

Ένας πάροχος νεφοϋπολογιστικού περιβάλλοντος θεωρείτε αρκετά αξιόπιστος να διατηρήσει ακεραιότητα και ορθότητα δεδομένων. Το μοντέλο του νέφους παρουσιάζει έναν αριθμό απειλών, όπως για παράδειγμα σύνθετες εσωτερικές επιθέσεις εναντίον των συγκεκριμένων χαρακτηριστικών των δεδομένων.

Η ακεραιότητα Software αναφέρεται στην προστασία του software από μη εξουσιοδοτημένη διαγραφή, τροποποίηση, υποκλοπή ή αναπαραγωγή. Η διαγραφή, η τροποποίηση και η αναπαραγωγή μπορεί να γίνουν σκόπιμα ή ακούσια. Λόγου χάρη, ένας δυσαρεστημένος εργαζόμενος είναι πιθανόν να τροποποιήσει εσκεμμένα ένα πρόγραμμα ώστε να παρουσιάσει

ελαττώματα σε συγκεκριμένες συνθήκες ή συγκεκριμένο χρόνο. Οι πάροχοι cloud εφαρμόζουν ένα σύνολο από software διασυνδέσεις ή APIs[9] που χρησιμοποιούν οι πελάτες για να επικοινωνούν με τις υπηρεσίες του νέφους. Αυτή η απειλή της μείωσης της ποιότητας των δεδομένων αυξάνεται με την συγκρότηση δεδομένων πολλών χρηστών. Η εμφάνιση ενός ελλαττωματικού ή δυσλειτουργικού δομικού στοιχείου, που είναι απαραίτητο από κάποιον άλλον χρήστη, ενδεχομένως να επηρεάσει την ακεραιότητα των δεδομένων και για άλλους χρήστες που μοιράζονται τις ίδιες υποδομές. Εκτός από τις προαναφερθείς απειλές, η ασφάλεια στις υπηρεσίες του νέφους βασίζεται σε μεγάλο βαθμό στην ασφάλεια των ίδιων των περιβαλλόντων εργασίας καθώς ένας μη εξουσιοδοτημένος χρήστης που αποκτήσει τη δυνατότητα ελέγχου των δεδομένων, είναι εύκολο να τα διαγράψει, να τα τροποποιήσει ή και να τα διαρρεύσει. Στο cloud η ευθύνη της προστασίας της ακεραιότητας του software μεταφέρεται στον ιδιοκτήτη του software ή στον διαχειριστή. Η ακεραιότητα του δικτύου και του hardware είναι ένα άλλο θέμα που είναι απαραίτητο να ρυθμιστεί από τον πάροχο του νέφους, εφόσον εκεί πέφτει το βάρος της προστασίας του βασικού hardware από κλοπή, διαρροή και τροποποίηση.

1.6.3 **Διαθεσιμότητα** (Availability)

Η διαθεσιμότητα αναφέρεται στην ιδιότητα ενός συστήματος να είναι προσβάσιμο και έτοιμο για χρήση κατόπιν ζήτησης από μία εξουσιοδοτημένη οντότητα. Η διαθεσιμότητα του συστήματος συμπεριλαμβάνει την δυνατότητα του συστήματος να διεξάγει λειτουργίες ακόμα και όταν κάποια εξουσιοδότηση ενεργεί ανάρμοστα. Το σύστημα οφείλει να έχει τη δυνατότητα να συνεχίσει τις διεργασίες ακόμα και κατά τη διάρκεια ενδεχόμενης παραβίασης ασφαλείας. Πιο συγκεκριμένα, αφορά την δυνατότητα των δεδομένων, του software, αλλά επίσης και του hardware να είναι διαθέσιμα on demand στους εξουσιοδοτημένους χρήστες. Η μόχλευση των χρηστών μέσω των απαιτήσεων των υποδομών του hardware, δημιουργεί μία εκτεταμένη εξάρτηση στην πανταχού παρούσα διαθεσιμότητα του δικτύου, κάτι που προκαλεί μεγάλο φόρτο στο δίκτυο, καθώς ανακτά και επεξεργάζεται τα δεδομένα. Ο ιδιοκτήτης του νέφους οφείλει να εξασφαλίσει ότι η επεξεργασία των δεδομένων καθώς και τα ίδια τα δεδομένα είναι διαθέσιμα στους πελάτες μόλις ζητηθούν.

[9] API: ορίζεται ως «συμβόλαιο κλήσης» μεταξύ καλούντος και καλούμενου, διαχωρίζοντας όμως την προγραμματιστική υλοποίηση από την χρήση των υπηρεσιών. (Μουρίκη, 2014)

Εικόνα 13: Οι διαθέσιμοι υπολογιστικοί πόροι της Amazon παγκοσμίως. (Viswav, 2017)

Η κατανόηση και η ξεκάθαρη καταγραφή συγκεκριμένων απαιτήσεων του χρήστη κρίνεται επιτακτική στην σχεδίαση μίας λύσης για την εξασφάλιση των παραπάνω αναγκαιοτήτων. Η επαλήθευση ταυτοτήτων, εκ των οποίων πολλές μοιράζονται κοινές βασικές απαιτήσεις ασφαλείας, και ο καθορισμός συγκεκριμένων αναγκών για προστασία των δεδομένων και ασφάλεια πληροφοριών, ίσως είναι ένα από τα πιο πολύπλοκα στοιχεία της σχεδίασης των πληροφοριακών συστημάτων. Το πολυχρηστικό περιβάλλον εμφανίζει πολλές μοναδικές προκλήσεις ασφαλείας, που εξαρτώνται από το επίπεδο στο οποίο λειτουργούν (επίπεδο εφαρμογής, εικονικό επίπεδο, φυσικό επίπεδο).

1. Επίπεδο Εφαρμογής:
   Σε αυτό το επίπεδο ανήκουν οι SaaS υπηρεσίες και τελικός πελάτης θεωρείται το άτομο ή η επιχείρηση η οποία γίνεται συνδρομής μίας υπηρεσίας που προσφέρεται από κάποιον πάροχο cloud και θεωρείται υπόλογος της χρήσης αυτής της υπηρεσίας. Στο συγκεκριμένο επίπεδο απαιτείται ιδιωτικότητα στα περιβάλλοντα πολύ-μίσθωσης, προστασία των κατάλοιπων δεδομένων, επαρκής έλεγχος πρόσβασης, προστασία επικοινωνίας, ασφάλεια software και διαθεσιμότητα υπηρεσίας. Επίσης, κάποιοι από τους κινδύνους που βρίσκονται στο επίπεδο της εφαρμογής είναι η απειλή υποκλοπής, η τροποποίηση δεδομένων που βρίσκονται είτε στο στάδιο της διαβίβασης είτε στο στάδιο της αδράνειας, η παρέμβαση-διαγραφή δεδομένων, η παραβίαση της ιδιωτικότητας, η αντιποίηση της ταυτότητας χρήστη καθώς και η αποκάλυψη του δικτύου.

2. Εικονικό Επίπεδο:
   Στο δεύτερο επίπεδο ανήκουν οι PaaS και οι IaaS υπηρεσίες. Προγραμματιστής και συντονιστής θεωρείται το άτομο ή η επιχείρηση που αναπτύσσει το software σε κάποια cloud υποδομή. Όπως και στο επιπέδο εφαρμογής, έτσι και εδώ απαιτείται επαρκής έλεγχος πρόσβασης και προστασία επικοινωνίας. Επιπρόσθετα, απαιτείται η ασφάλεια της εφαρμογής και των δεδομένων (in transit και at rest), έλεγχος ασφαλείας της διαχείρισης του νέφους, λογισμικά ασφαλείας και προστασία εικονικού νέφους. Οι απειλές που συναντάμε σε αυτό το επίπεδο είναι λάθος στον

προγραμματισμό, τροποποίηση software, παρέμβαση-διαγραφή software, αντιποίηση ταυτότητας, αποκάλυψη δικτύου, επίθεση DDoS[10] καθώς και διακοπή επικοινωνίας.

3. Φυσικό Επίπεδο:
   Στο τελευταίο επίπεδο είναι το φυσικό κέντρο δεδομένων (datacenter). Ο χρήστης του συγκεκριμένου επιπέδου είναι ο ιδιοκτήτης που κατέχει την υποδομή, πάνω στην οποία αναπτύσσονται τα νέφοι. Σε αυτό το επίπεδο είναι απαραίτητο να γίνεται νόμιμη και όχι καταχρηστική χρήση της νεφοϋπολογιστικής, να υπάρχει ασφάλεια και αξιοπιστία του hardware και προστασία τόσο των πόρων του δικτύου, όσο και προστασία στο ίδιο το δίκτυο. Οι κίνδυνοι που παραμονεύουν στο φυσικό επίπεδο είναι οι επιθέσεις δικτύου και DDoS επιθέσεις, παρέμβαση, κλοπή και τροποποίηση του hardware, κατάχρηση της υποδομής και τέλος φυσικές καταστροφές.

1.7 **ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ**

Οι στόχοι ασφαλείας εντός ενός κατανεμημένου συστήματος ουσιαστικώς είναι:

- Η εξασφάλιση της διαθεσιμότητας των πληροφοριών που στέλνονται μεταξύ ή κρατούνται μέσα στα συμμετέχοντα συστήματα.
- Η διατήρηση της ακεραιότητας των πληροφοριών που στέλνονται μεταξύ ή κρατούνται μέσα στα συμμετέχοντα συστήματα, π.χ. η αποτροπή του απώλειας ή τροποποίησης των πληροφοριών λόγω μη εξουσιοδοτημένης πρόσβασης, συστηματικής αστοχίας ή κάποιου άλλου λάθους.
- Η διατήρηση της ακεραιότητας των υπηρεσιών που προσφέρονται, π.χ. εμπιστευτικότητα και ορθή λειτουργία.
- Η παροχή ελέγχου της πρόσβασης στις υπηρεσίες ή σε μέρη τους ώστε να εξασφαλιστεί ότι οι χρήστες μπορούν να εισέρχονται σε υπηρεσίες για τις οποίες είναι εξουσιοδοτημένοι.
- Η πιστοποίηση της ταυτότητας των συμμετεχόντων (διομότιμες οντότητες) και όπου κρίνεται απαραίτητο (π.χ. για τραπεζικές συναλλαγές) η εξασφάλιση της μη άρνησης αναγνώρισης της προέλευσης και διανομή των δεδομένων.
- Ανάλογα με την περίπτωση, η παροχή ασφαλούς διαλειτουργικότητας με τα μη ανοικτά συστήματα.
- Η εξασφάλιση της εμπιστευτικότητας των πληροφοριών που κρατούνται στα συστήματα που συμμετέχουν.
- Ο καθαρός διαχωρισμός των δεδομένων και των διεργασιών στο εικονικό επίπεδο του νέφους, για την εξασφάλιση μηδενικής διαρροής δεδομένων μεταξύ των διαφορετικών εφαρμογών.
- Και τέλος η διατήρηση του ίδιου επιπέδου ασφαλείας όταν υπάρχει προσθήκη ή αφαίρεση πόρων στο φυσικό επίπεδο. (Zissis & Lekkas, 2010)

[10] DDoS (Distributed Denial-of-Service) – Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας: είναι τύπος επίθεσης κατά την οποία μεγάλος όγκος κλήσεων από πολλαπλές πηγές προκαλεί υπερφόρτωση δικτύου με αποτέλεσμα τη μη διαθεσιμότητα μίας online υπηρεσίας.

1.8 **ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ** CLOUD

Οι σημερινοί πάροχοι υπηρεσιών cloud λειτουργούν πολύ μεγάλα συστήματα. Έχουν εξελιγμένες διαδικασίες και προσωπικό εμπειρογνωμόνων για τη διατήρηση των συστημάτων τους, τις οποίες οι μικρές επιχειρήσεις δεν έχουν πρόσβαση. Ως αποτέλεσμα, υπάρχουν πολλά πλεονεκτήματα άμεσης και έμμεσης ασφάλειας για τους χρήστες του cloud. Στην συνέχεια, ακολουθούν μερικά από τα βασικά πλεονεκτήματα ασφάλειας ενός περιβάλλοντος υπολογιστικού νέφους:

Κεντρική διαχείριση δεδομένων: Σε ένα περιβάλλον νέφους, ο πάροχος υπηρεσιών φροντίζει για θέματα αποθήκευσης, με αποτέλεσμα, οι μικρές επιχειρήσεις να μην χρειάζεται να ξοδεύουν πολλά χρήματα σε συσκευές φυσικής αποθήκευσης. Επίσης, η αποθήκευση που βασίζεται στο cloud, παρέχει έναν πιο γρήγορο και ενδεχομένως, φθηνότερο τρόπο για τη συγκέντρωση των δεδομένων. Αυτό είναι ιδιαίτερα χρήσιμο για τις μικρές επιχειρήσεις, οι οποίες δεν μπορούν να ξοδέψουν επιπλέον χρήματα στους επαγγελματίες της ασφάλειας για την παρακολούθηση των δεδομένων.

Άμεση αντίδραση σε περίπτωση εμφάνισης προβλήματος: Οι πάροχοι υπηρεσιών IaaS μπορούν να δημιουργήσουν έναν ειδικό ιατροδικαστικό διακομιστή, ο οποίος μπορεί να χρησιμοποιηθεί βάσει της ζήτησης. Κάθε φορά που λαμβάνει χώρα μια παραβίαση ασφαλείας, ο διακομιστής μπορεί να μεταφερθεί στο διαδίκτυο. Σε ορισμένες περιπτώσεις έρευνας, ένα αντίγραφο ασφαλείας του περιβάλλοντος μπορεί εύκολα να γίνει και να τοποθετηθεί στο σύννεφο χωρίς να επηρεαστεί η φυσιολογική πορεία των εργασιών.

Χρόνος επαλήθευσης της εγκληματολογικής εικόνας: Ορισμένες εφαρμογές αποθήκευσης στο νέφος εκθέτουν ένα κρυπτογραφικό ποσό ελέγχου ή ένα hash. Για παράδειγμα, το Amazon S3 δημιουργεί αυτόματα το hash MD5 (αλγόριθμος υποβολής μηνυμάτων 5) όταν αποθηκεύετε ένα αντικείμενο. Ως εκ τούτου, θεωρητικά, η ανάγκη για τη δημιουργία χρονοβόρων MD5 αθροισμάτων ελέγχου με τη χρήση εξωτερικών εργαλείων εξαλείφεται.

Καταγραφή: Σε ένα παραδοσιακό παράδειγμα υπολογιστικής, η καταγραφή είναι συχνά μια δεύτερη σκέψη. Σε γενικές γραμμές, ο ανεπαρκής χώρος στο δίσκο είναι κατανεμημένος που καθιστά την καταγραφή είτε ανύπαρκτη είτε ελάχιστη. Ωστόσο, σε ένα cloud, η ανάγκη αποθήκευσης για τυπικά αρχεία καταγραφής λύεται αυτόματα.

ΚΕΦΑΛΑΙΟ 2

2.1 **ΤΥΠΟΙ ΕΠΙΤΗΘΕΜΕΝΩΝ ΣΤΟ** CLOUD COMPUTING

Το cloud computing περιβάλλον είναι πλέον ο αγαπημένος στόχος των εγκληματιών του διαδικτύου, και αναμένεται στο μέλλον να συναντήσουμε πιο σύνθετες επιθέσεις. Θα μπορούσαμε να πούμε ότι το συγκεκριμένο περιβάλλον ελκύει διαδικτυακούς εγκληματίες όπως οι τράπεζες ληστές. Μία βάση δεδομένων που βρίσκεται στο νέφος είναι κάτι παρόμοιο με μία τράπεζα πληροφοριών με πολλούς πελάτες, και ο συγκεκριμένος τύπος εγκληματία ενδιαφέρεται ιδιαίτερα να χρησιμοποιήσει αυτές τις πληροφορίες είτε κακόβουλα είτε με μη εξουσιοδοτημένους τρόπους.

Συνεπώς, εκθέτει το νέφος σε μία άλλη μορφή απειλών και προκλήσεων. Το προσωπικό ασφαλείας του κάθε παρόχου πρέπει να είναι σε θέση να καταλάβει το είδος και την πηγή της κάθε επίθεσης.

Πολλές από τις απειλές και τις προκλήσεις ασφαλείας στο cloud computing είναι γνωστές στις επιχειρήσεις που διαχειρίζονται εσωτερικές υποδομές και σε αυτές που εμπλέκονται με παραδοσιακά μοντέλα αναθέσεων σε εξωτερικούς συνεργάτες. Οι απειλές στο κάθε μοντέλο παροχής υπηρεσιών του cloud computing προέρχονται από τους επιτιθέμενους, οι οποίοι μπορούν να χωριστούν σε δύο κατηγορίες.

Στην πρώτη κατηγορία εντάσσονται οι εσωτερικοί hackers. Αυτού του είδους οι επιτιθέμενοι έχουν προσληφθεί από τον πάροχο υπηρεσιών νέφους, ή από τον πελάτη ή από κάποια άλλη τρίτη επιχείρηση παροχής που αναλαμβάνει την λειτουργία μίας υπηρεσίας cloud. Οι συγκεκριμένοι, ανάλογα με τον επιχειρησιακό ρόλο τους, μπορούν να έχουν ήδη εξουσιοδοτημένη πρόσβαση στις υπηρεσίες, στα δεδομένα του πελάτη ή στις φέρουσες υποδομές και τις εφαρμογές. Οι εσωτερικοί hackers χρησιμοποιούν ήδη υφιστάμενα προνόμια ώστε να αποκτήσουν περαιτέρω πρόσβαση ή να βοηθήσουν τρίτους να εκτελέσουν επιθέσεις εναντίων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών μέσα στην υπηρεσία νέφους.

Σύμφωνα με την έρευνα CyberSecurity Watch Survey 2011 που διεξήχθη σε 607 επιχειρήσεις, κυβερνητικά στελέχη, επαγγελματίες και συμβούλους, το 21% των επιθέσεων στον κυβερνοχώρο προκλήθηκαν από εσωτερικά άτομα. Το 33% των ερωτηθέντων θεωρούσε ότι οι επιθέσεις από τους εμπλεκόμενους φορείς ήταν πιο δαπανηρές και επιζήμιες για τους οργανισμούς (CERT, 2011). Οι πιο συνηθισμένες εσωτερικές επιθέσεις ήταν η μη εξουσιοδοτημένη πρόσβαση και η χρήση εταιρικών πληροφοριών (63%), η ακούσια έκθεση ιδιωτικών ή ευαίσθητων δεδομένων (57%), ιοί, σκουλήκια ή άλλοι κακόβουλοι κωδικοί (37%) και κλοπή πνευματικής ιδιοκτησίας.

Οι αδυναμίες που παρουσιάζει το cloud computing και το καθιστά ευάλωτο στους εσωτερικούς hackers είναι (Catteddu, 2010):

- οι ασαφείς ρόλοι και οι ευθύνες,
- η κακή εφαρμογή των ορισμών των ρόλων,
- η μη εφαρμογή της αρχής της ανάγκης για γνώση,

- τα τρωτά σημεία του συστήματος ή των λειτουργικών συστημάτων,
- οι ανεπαρκείς διαδικασίες φυσικής ασφάλειας,
- η αδυναμία επεξεργασίας δεδομένων σε κρυπτογραφημένη μορφή,
- ευπάθειες εφαρμογής ή κακή διαχείριση των διορθώσεων.
-

Στην δεύτερη κατηγορία εντάσσονται οι εξωτερικοί hackers. Σε αντίθεση με τους εσωτερικούς hackers, οι εξωτερικοί δεν εργάζονται για τον πάροχο υπηρεσιών, τον πελάτη ή για κάποια άλλη τρίτη επιχείρηση παροχής που αναλαμβάνει την λειτουργία μίας υπηρεσίας cloud. Επίσης, δεν έχουν καμία εξουσιοδοτημένη πρόσβαση στις υπηρεσίες του νέφους, στα δεδομένα του πελάτη ή στις υποστηριζόμενες υποδομές και εφαρμογές. Αυτό που κάνουν είναι να εκμεταλλεύονται τις τεχνικές, λειτουργικές και διαδικαστικές αδυναμίες για να επιτεθούν σε κάποιον πάροχο υπηρεσιών νέφους, πελάτη ή τρίτη επιχείρηση υποστήριξης, ώστε να αποκτήσουν πρόσβαση για εξάπλωση επιθέσεων εναντίων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των εσωτερικών πληροφοριών (Chou, 2013).

Εικόνα 14: Περιγραφή ενός computer worm[11] (Rastogi, et al., 2015)

Το ποσοστό των εξωτερικών απειλών για έναν οργανισμό είναι πολύ υψηλό. Περιλαμβάνει καλά χρηματοδοτούμενους hackers, ομάδες οργανωμένου εγκλήματος και κυβερνητικές οντότητες. Οι επιθέσεις μπορεί να είναι είτε ενεργές είτε παθητικές. Μια ενεργή επίθεση δημιουργεί πακέτα ή συμμετέχει στο δίκτυο ενώ μια παθητική επίθεση παρακολουθεί το δίκτυο ή παρακολουθεί τους χρήστες. Κύριο κίνητρο για τέτοιου είδους επιθέσεις στον κυβερνοχώρο είναι η κυβερνητική κατασκοπεία, ο πολεμικός κυβερνοχώρος και ο πειραματισμός. Αυτοί οι εισβολείς είναι επίμονοι και είναι σημαντικό να γνωρίζετε τις μεθόδους που χρησιμοποιούν οι hackers. Αυτό αποτελεί σημαντικό βήμα για την υπεράσπιση ευαίσθητων δεδομένων της εταιρείας. Το κόστος για μια εταιρεία θα μπορούσε να είναι εκατομμύρια δολάρια, όταν ένας hacker εκθέτει ευαίσθητα δεδομένα στο κοινό.

Αν και ο εσωτερικοί και εξωτερικοί hackers διαχωρίζονται με σαφήνεια στην θεωρία, αυτό που τους διαχωρίζει ουσιαστικά ως απειλή τόσο στους πελάτες όσο και στους προμηθευτές, είναι η ικανότητά τους να εκτελέσουν επιτυχημένες επιθέσεις. Σύμφωνα με την έρευνα του CyberSecurity Survey το 2011, τα συμβάντα ηλεκτρονικού εγκλήματος προήλθαν από 58%

[11] Computer worm/ Σκουλήκι υπολογιστή: Είναι ένας τύπος κακόβουλου λογισμικού, που στέλνει αντίγραφα του εαυτού του από υπολογιστή σε υπολογιστή. Αναπαράγεται μόνο του και δεν χρειάζεται να προσκολληθεί σε κάποιο software πρόγραμμα για να προκαλέσει ζημιά. (Anon., n.d.)

εξωτερικούς hackers, 21% εσωτερικούς και ένα ποσοστό της τάξης του 21% προήλθε από άγνωστη πηγή.

Στο περιβάλλον του νέφους, οι εισβολείς μπορούν να κατηγοριοποιηθούν σε τέσσερις τύπους: τυχαίος, αδύναμος, δυνατός και σημαντικός (Center for the Protection of National Infrastructure, CPNI, 2010). Κάθε κατηγορία είναι βασισμένη στην ικανότητα να επιφέρει μία επιτυχημένη επίθεση και όχι τόσο στον τύπο απειλής που παρουσιάζουν (για παράδειγμα εγκληματική, κατασκοπία ή τρομοκρατία).

1. Τυχαίος: ο πιο συχνός τύπος εισβολέα χρησιμοποιεί απλά εργαλεία και τεχνικές. Ο επιτιθέμενος μπορεί να σκανάρει τυχαία το Διαδίκτυο ψάχνοντας ευάλωτα στοιχεία. Έπειτα, θα αξιοποιήσουν διαδεδομένα εργαλεία και τεχνικές, που είναι εύκολα ανιχνεύσιμα.
2. Αδύναμος: Οι μέτρια επιδέξιοι εισβολείς στοχεύουν συγκεκριμένους servers/παρόχους νέφους, προσαρμόζοντας ήδη υπάρχοντα και δημόσια διαθέσιμα εργαλεία ή συγκεκριμένους στόχους. Οι μέθοδοί τους είναι πιο ανεπτυγμένοι καθώς προσπαθούν να εξατομικεύσουν τις επιθέσεις τους χρησιμοποιώντας ήδη διαθέσιμα εκμεταλλευόμενα εργαλεία.
3. Δυνατός: Αυτή η κατηγορία αποτελείται από οργανωμένες, επαρκώς χρηματοδοτούμενες και επιδέξιες ομάδες εισβολέων, που χαρακτηρίζονται από εσωτερική ιεραρχία και ειδικεύονται στη στοχοποίηση συγκεκριμένων εφαρμογών και χρηστών στο cloud. Γενικά σε αυτή την κατηγορία ανήκουν ομάδες οργανωμένου εγκλήματος που ειδικεύονται σε μεγάλης κλίμακας επίθεσης.
4. Σημαντικός: Εδώ ανήκουν οι δυνατοί και με κίνητρο hackers, οι οποίοι δεν είναι εύκολα ανιχνεύσιμοι από τις επιχειρήσεις που δέχονται την επίθεση, ή ακόμα και από τις οργανώσεις που ειδικεύονται στην σχετική επιβολή νόμου και έρευνας των ηλεκτρονικών εγκλημάτων ή της κυβερνο-ασφάλειας. Η άμβλυνση αυτής της απειλής απαιτεί μεγαλύτερο βαθμό γνώσης πάνω στις επιθέσεις και εξειδικευμένους πόρους κατόπιν τον εντοπισμό κάποιου περιστατικού ή κάποιας επίθεσης. (Sen, 2013)

Οφείλουμε να αναφέρουμε σε αυτό το σημείο, ότι η ανάθεση της προστασίας του cloud συστήματος πρέπει να γίνεται σε κάποιον που κατέχει εμπειρία στην προστασία των επιχειρησιακών δικτύων. Είναι απαραίτητο να κατέχει την δυνατότητα να ρυθμίζει και να σχεδιάζει συστήματα ασφαλείας. Οι πιστοποιήσεις από Microsoft, Cisco, Cloud Security Alliance, SANS κλπ βοηθούν πολύ στην απόκτηση γνώσης και εμπειρίας μέσω εργαστηριακών και θεωρητικών μαθημάτων. Σε γενικές γραμμές οι συγκεκριμένες πιστοποιήσεις παρέχουν σε ικανοποιητικό βαθμό κατανόηση για το πώς δουλεύουν τα ποικίλα συστήματα ασφαλείας και οι μηχανισμοί κοινών επιθέσεων, αλλά και τρόπους προστασίας κατά αυτών. Αυτές οι γνώσεις μπορούν να εφαρμοστούν με ασφάλεια σε πολλά συστήματα και αργότερα να εξελιχθούν κιόλας, καθώς η τεχνολογία αναπτύσσεται περεταίρω. Κάποιος ενδιαφερόμενος μπορεί να ενημερώνεται για τις καινούριες απειλές είτε από διάφορα blogs, εκθέσεις ή άλλους οργανισμούς. Κάθε μέρα παρέχονται όλο και περισσότερες λεπτομέρειες και έτσι η γνώση μας για την εξέλιξη αυτών των απειλών γίνεται βαθύτερη.

Μπορεί το προσωπικό ασφαλείας να έχει επαρκής γνώσεις για τον τρόπο λειτουργίας και ασφάλειας του συστήματος, αλλά τις ίδιες γνώσεις μπορεί να τις κατέχει κάλλιστα και ο επιτιθέμενος. Μαζί με την τεχνολογία προστασίας εξελίσσονται οι τεχνικές και οι γνώσεις

για της αντίθετης πλευράς, της κακόβουλης. Η ετερογένεια των συστημάτων και τα software που τη συνδέουν θα συμβάλλει στην αύξηση των πεδίων απειλών. (Rastogi, et al., 2015)

2.2 **ΚΙΝΔΥΝΟΙ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ** CLOUD

Οι κίνδυνοι στην ασφάλεια, που σχετίζονται με το κάθε μοντέλο υπηρεσιών του νέφους, διαφέρουν και βασίζονται σε ένα ευρύ φάσμα παραγόντων, στο οποίο περιλαμβάνονται τα πληροφοριακά στοιχεία, η αρχιτεκτονική του cloud και οι έλεγχοι ασφαλείας που γίνονται σε κάθε cloud περιβάλλον ξεχωριστά. Οι κίνδυνοι στους οποίους θα αναφερθούμε είναι: η προνομιακή πρόσβαση χρηστών, η τοποθεσία και ο διαχωρισμός των δεδομένων, η διάθεση των δεδομένων, οι ηλεκτρονικές έρευνες και παρακολούθηση της προστασίας και η διασφάλιση της ασφάλειας του νέφους.

2.2.1 **Προνομιακή Πρόσβαση Χρηστών**

Από την στιγμή που τα δεδομένα αποθηκεύονται στο νέφος, ο πάροχος υπηρεσιών όχι μόνο έχει πρόσβαση στα συγκεκριμένα δεδομένα, αλλά επίσης ελέγχει την πρόσβαση άλλων οντοτήτων σε αυτά (μεταξύ άλλων χρήστες του νέφους και άλλους εξωτερικούς παρόχους). Η διατήρηση της εμπιστευτικότητας των δεδομένων στο Cloud και ο περιορισμός της προνομιακής πρόσβασης χρήστη είναι δυνατόν να επιτευχθεί τουλάχιστον με τη μία από τις δύο προσεγγίσεις που μπορεί να επιλέξει ο ιδιοκτήτης των δεδομένων· πρώτον, με την κρυπτογράφηση των δεδομένων πριν την εισαγωγή τους για τη διαχώριση της δυνατότητας αποθήκευσης των δεδομένων από τη δυνατότητα της χρήσης τους, και δεύτερον με την νόμιμη επιβολή των απαιτούμενων για τις παροχές cloud μέσω συμβατικών υποχρεώσεων και μηχανισμών διασφάλισης για την εξασφάλιση των επιπέδων της εμπιστευτικότητας των δεδομένων στις απαιτούμενες προδιαγραφές. Ο πάροχος νέφους οφείλει να έχε αποδείξιμες πολιτικές ελέγχου ασφαλούς πρόσβασης και ενεστωτικές τεχνικές λύσεις, οι οποίες αποτρέπουν τη δυνατότητα τροποποίησης των προνομίων μίας διεργασίας από κάποιον τυπικό χρήστη, καθιστούν δυνατόν τον έλεγχο των ενεργειών των χρηστών, και ενισχύουν τον διαχωρισμό των καθηκόντων των προνομιούχων χρηστών για να αποτραπεί και να ανιχνευτεί κακόβουλη εσωτερική δραστηριότητα.

Η κρυπτογράφηση των δεδομένων, πριν την είσοδό τους στο νέφος, δημιουργεί δύο προκλήσεις. Για να θεωρηθεί η κρυπτογράφηση ένας αποτελεσματικός τρόπος διατήρησης της εμπιστευτικότητας, είναι απαραίτητο τα κλειδιά αποκρυπτογράφησης να είναι ασφαλώς απομονωμένα από το περιβάλλον του νέφους ώστε να εξασφαλιστεί ότι μόνο ένα εξουσιοδοτημένο μέρος μπορεί να αποκρυπτογραφήσει δεδομένα. Αυτό μπορεί να επιτευχθεί με την αποθήκευση κλειδιών σε απομονωμένα συστήματα εσωτερικός στην εταιρεία ή με την αποθήκευση κλειδιών σε έναν δεύτερο πάροχο.

Μία επιπρόσθετη πρόκληση της κρυπτογράφησης στο νέφος είναι η αποφυγή παραποίησης κρυπτογραφημένων δεδομένων έτσι ώστε απλό κείμενο, ή οποιαδήποτε άλλα βαρυσήμαντα δεδομένα, μπορούν να ανακτηθούν και να χρησιμοποιηθούν για να «σπαστεί» η κρυπτογράφηση. Αυτός ο περιορισμός στην τεχνολογία της κρυπτογράφησης φανερώνει ότι οι πάροχοι νέφους δεν πρέπει να διαθέτουν απεριόριστη δυνατότητα αποθήκευσης και αρχειοθέτησης των κρυπτογραφημένων δεδομένων. Εάν η εταιρεία-χρήστης cloud επιτρέπει στον πάροχο υπηρεσιών την διαχείριση των μη κρυπτογραφημένων δεδομένων, τότε ο πάροχος υπηρεσιών νέφους οφείλει να διασφαλίσει ότι τα δεδομένα θα προστατευτούν από μη εξουσιοδοτημένη πρόσβαση, τόσο εσωτερική όσο και εξωτερική. Μέσα στο νέφος, η παραγωγή και η χρήση των κρυπτογραφικών κλειδιών για τον κάθε cloud χρήστη μπορεί να

χρησιμοποιηθεί ως παροχή ενός επιπλέον επιπέδου προστασίας πέρα από τους ελέγχους διαχωρισμού των δεδομένων. Παρόλα αυτά, οι πάροχοι χρειάζονται ισχυρές επί τόπου διαδικασίες διαχείρισης κλειδιών και έπειτα η απόκτηση ασφαλείας κατά τη διαδικασία αυτή γίνεται η πρόκληση για τους πελάτες.

Ένας σημαντικά δυνατός εισβολέας είναι πιθανόν να εκμεταλλευτεί αδύναμες πολιτικές κρυπτογράφησης, και την προνομιακή πρόσβαση διαχείρισης του cloud παρόχου, με σκοπό την ανάκτηση δεδομένων των πελατών, χρησιμοποιώντας μία πολύπλοκη software ή hardware επίθεση σε συσκευές τελικού σημείου (endpoint devices) του χρήστη ή σε συσκευές υποδομών cloud. Αυτή η επίθεση μπορεί να επιφέρει μακροπρόθεσμη έκθεση της εφοδιαστικής αλυσίδας του παρόχου νέφους, ή κοινωνική μηχανική[12] ενός συγκεκριμένου πελάτη-χρήστη.

Η χρήση της τεχνολογίας κρυπτογράφησης μπορεί επίσης να υπόκειται σε περιορισμούς ή σε συγκεκριμένες απαιτήσεις εξαρτώμενες από την δικαιοδοσία με την οποία ο πάροχος νέφους θα αποθηκεύει τα δεδομένα των cloud πελατών. Για παράδειγμα, σε κάποιες χώρες, η χρήση της τεχνολογίας της κρυπτογράφησης είναι περιορισμένη βασιζόμενη στον τύπο της κρυπτογράφησης ή τον σκοπό της δραστηριότητας. Οι πελάτες του νέφους οφείλουν να επανεξετάσουν κατά πόσο η εφαρμογή της κρυπτογράφησης, όπως ορίζεται από τους τοπικούς αρμόδιους του παρόχου cloud, είναι αποδεκτή και δεν ενισχύει τους κινδύνους για τα δεδομένα τους. Παραδείγματος χάριν, στο Ηνωμένο Βασίλειο, ο νόμος της Ρύθμισης των Εξουσιών Έρευνας (Regulatory Investigatory Powers Act – RIPA) δύναται να επιβάλλει νομική υποχρέωση κοινοποίησης των κλειδιών αποκρυπτογράφησης για διευκόλυνση πρόσβασης στα δεδομένα από τις υπηρεσίες ασφαλείας και τις αστυνομικές αρχές. Οι πελάτες του νέφους πρέπει να σιγουρευτούν ότι καταλαβαίνουν τις υποχρεώσεις τους εντός όλης της δικαιοδοσίας του παρόχου cloud, και έχουν πρέπουσες πολιτικές και διαδικασίες για την αντιμετώπιση συγκεκριμένων εξωτερικών προβλημάτων, που σέβονται τα κρυπτογραφημένα δεδομένα.

2.2.2 **Τοποθεσία και Διαχωρισμός Δεδομένων**

Η τοποθεσία των δεδομένων και ο διαχωρισμός τους είναι ιδιαίτερης σημασίας στο cloud, δεδομένου της ανομοιογενής φυσικής τοποθεσίας των δεδομένων και των κοινόχρηστων πληροφοριακών πόρων. Οι χρήστες του νέφους μπορεί να βρίσκονται κάτω από νομικές και συμβατικές υποχρεώσεις, για την διασφάλιση ότι τα δεδομένα κρατούνται, επεξεργάζονται και διαχειρίζονται με ένα συγκεκριμένο τρόπο. Σε αυτή την περίπτωση υπάρχουν κάποιοι συνακόλουθοι κίνδυνοι ασφαλείας:

- Ο πάροχος νέφους εξαναγκάζεται να κοινοποιήσει δεδομένα, και ενδεχομένως κλειδιά κρυπτογράφησης, ή να παραδώσει φυσικά μέσα σε κάποιο τρίτο πρόσωπο ή σε νομική αρχή.
- Αναπτύσσονται υποχρεώσεις για πληρωμές φόρων σε τοπικές αρχές, σαν αποτέλεσμα των πωλήσεων και άλλων συναλλαγών που γίνονται εντός της δικιάς τους δικαιοδοσίας.
- Οι περιβαλλοντικοί κίνδυνοι όπως οι σεισμοί, οι πλημύρες και οι ακραίες καιρικές συνθήκες επηρεάζουν την ασφάλεια των δεδομένων των πελατών.

[12] Κοινωνική μηχανική είναι η πράξη της προφορικής χειραγώγησης με σκοπό την απόσπαση εμπιστευτικών πληροφοριών, απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα. (Γκιούρδας, 2001)

- Και τέλος, οι μακροοικονομικοί κίνδυνοι, όπως ο υπερπληθωρισμός ή η παρατεταμένη οικονομική ύφεση επηρεάζουν τις υπηρεσίες των παρόχων και τις συνθήκες του προσωπικού.

Η διάταξη της κεντρικής αποθήκευσης στη νεφοϋπολογιστική εφοδιάζει τους εισβολείς με έναν πολύ πλουσιότερο στόχο πληροφοριών. Με μία μόνο επίθεση, οι εισβολείς πιθανότατα να αποκτήσουν πρόσβαση σε απόρρητες πληροφορίες που ανήκουν σε διάφορες επιχειρήσεις – πελάτες. Εάν δεν εφαρμόζεται επαρκής διαχωρισμός στα δεδομένα πολλοί πελάτες είναι πιθανόν να υποστούν κάποια διαρροή ασφαλείας εξαιτίας κάποιου περιστατικού το οποίο θα έπρεπε να ήταν περιορισμένο μόνο σε έναν πελάτη.

Η εικονικοποίηση είναι μία από τις πολλές βασικές τεχνολογίες της νεφοϋπολογιστικής, και χαρακτηρίζεται σαν μία run-time μέθοδος διαχωρισμού των επεξεργαζόμενων δεδομένων. Πολλές από τις ανησυχίες και τα ζητήματα ασφαλείας που συνδέονται με την εικονικοποίηση είναι σημαντικά στην νεφοϋπολογιστική, ανεξάρτητα από το αν ο πάροχος υπηρεσιών νέφους αξιοποιεί τεχνολογίες εικονικοποίησης. Η ασφάλεια των δεδομένων βασίζεται στους επαρκείς ελέγχους ασφαλείας σε κάθε επίπεδο του εικονικοποιημένου περιβάλλοντος. Επιπροσθέτως, είναι απαραίτητη η ασφαλής εξάλειψη μνήμης και χώρου, ώστε να προληφθεί η απώλεια δεδομένων σε ένα πολλαπλά ενοικιαζόμενο περιβάλλον όπου τα συστήματα ανακυκλώνονται.
Το hypervisor επίπεδο[13] που βρίσκεται ανάμεσα στο hardware και στα virtual machines επιτρέπει προνομιακή πρόσβαση στα πιο πάνω επίπεδα. Επίσης έχει αρκετά μεγάλη δυνατότητα ελέγχου στο hardware, μία δυνατότητα που αυξάνεται όλο και περισσότερο καθώς οι κατασκευαστές hardware εγκαθιστούν hypervisor λειτουργίες απευθείας στα chipsets και στις κεντρικές μονάδες επεξεργασίας (CPU). Επομένως, οι χρήστες του cloud είναι απαραίτητο να εκτιμήσουν την χρήση και λειτουργία της τεχνολογίας εικονικοποίησης από τους παρόχους υπηρεσιών νέφους και κατά πόσο οι κίνδυνοι αξίζουν να αγνοηθούν.

2.2.3 **Διάθεση των Δεδομένων**

Οι υπηρεσίες cloud που προσφέρουν λειτουργίες αποθήκευσης δεδομένων συνήθως παρέχουν είτε εγγυήσεις ή στόχους επιπέδου υπηρεσιών σχετικά με την υψηλή διαθεσιμότητα αυτών των δεδομένων. Οι πάροχοι υπηρεσιών επιτυγχάνουν τα παραπάνω με την κράτηση πολλαπλών αντιγράφων των δεδομένων. Όταν ο πελάτης του cloud έχει την απαίτηση να διαγραφούν τα δεδομένα, ο βασισμένος στο νέφος χώρος αποθήκευσης ίσως είναι ακατάλληλος για αυτά τα δεδομένα καθ’ όλη την διάρκεια της ζωής τους.

Αναλόγως με τον τύπο των δεδομένων που φιλοξενούνται στο νέφος, οι πελάτες μπορεί να απαιτήσουν τη διαγραφή των δεδομένων σύμφωνα με τα πρότυπα του συγκεκριμένου τομέα. Εκτός από την περίπτωση όπου η αρχιτεκτονική του cloud περιορίζει τα μέσα στα οποία οι πληροφορίες μπορούν να αποθηκευτούν και όπου ο ιδιοκτήτης των δεδομένων έχει τη δυνατότητα να εξουσιοδοτήσει τη χρήση μέσων τεχνικών εξυγίανσης, οι πελάτες μπορεί να χρειαστεί να αποκλείσουν τα δεδομένα τους από το να μεταβιβαστούν στο cloud.

[13] Hypervisor επίπεδο: το επίπεδο του λογισμικού όπου εμπεριέχεται ένας επόπτης των virtual machines και είναι υπεύθυνος για την κατανομή των πόρων, και εξασφαλίζει την εκτέλεση πολλαπλών λειτουργικών συστημάτων.

2.2.4 **Ηλεκτρονικές Έρευνες και Παρακολούθηση της Προστασίας**

Η εφαρμογή προστατευτικής παρακολούθησης στο cloud παρουσιάζει προκλήσεις τόσο στους καταναλωτές όσο και στους παρόχους, δεδομένης της ανομοιογενής τοποθεσίας των φυσικών δεδομένων και του υψηλού αριθμού εμπλεκόμενων παρόχων. Ενώ οι βασικές τεχνολογίες του νέφους έχουν σχεδιαστεί να τοποθετούν μία παράμετρο ασφαλείας μεταξύ των συστημάτων υπηρεσιών cloud και των χρηστών, οι αδυναμίες σε αυτό το επίπεδο ασφαλείας δεν είναι δυνατόν να αποκλεισθούν εντελώς. Πάντα υπάρχει ο φόβος των εσωτερικών απειλών και επιθέσεων στο νέφος, κάτι που απαιτεί εμπεριστατωμένη γνώση στις ηλεκτρονικές έρευνες και στην παρακολούθηση της προστασίας.
Η αποτελεσματική παρακολούθηση της προστασίας των πληροφοριακών στοιχείων στο νέφος, ενδέχεται να απαιτεί συνένωση τόσο των εργαλείων παρακολούθησης που χρησιμοποιούνται από τους παρόχους cloud, όσο και των εργαλείων που χρησιμοποιούνται από τους ίδιους τους χρήστες. Η ανίχνευση των ενεργειών σε υπεύθυνους χρήστες και διαχειριστές στο νέφος ίσως προϋποθέτει μία ολοκληρωμένη ή ομοσπονδιακή (αμοιβαίας εμπιστοσύνης) διαχείριση ταυτότητας και σχετικό σύστημα καταγραφής, το οποίο επιτρέπει αναμφίβολη ταυτοποίηση όλων των μη εξουσιοδοτημένων ατόμων με πρόσβαση στους πόρους του νέφους.

Η διαχείριση την ταυτότητας και την πρόσβασης μίας επιχείρησης στο νέφος ίσως απαιτεί ενσωμάτωση με κάποιο προ-υπάρχων σύστημα διαχείρισης ταυτότητας. Μία λύση είναι η ενοποίηση του συστήματος διαχείρισης ταυτότητας του cloud χρήστη με το σύστημα διαχείρισης πρόσβασης.

Η παρακολούθηση προστασίας του νέφους, σε ορισμένες περιπτώσεις, θα βασίζεται στην ικανότητα του πελάτη να ανιχνεύει ενέργειες από όλους τις εξουσιοδοτημένες ταυτότητες τόσο στο cloud περιβάλλον όσο και στο πληροφοριακό περιβάλλον του πελάτη. Κάτι τέτοιο συνήθως απαιτεί μία προσέγγιση ενοποιημένης διαχείρισης ταυτότητας, που περιλαμβάνει και τους χρήστες αλλά και τον πάροχο υπηρεσιών νέφους.

Η τεχνολογία που υποστηρίζει την ενοποιημένη διαχείριση ταυτότητας προς το παρόν βρίσκεται σε πολύ πρώιμα στάδια, με πολλούς ανταγωνιστές να δίνουν μάχη για την κυριαρχία σε ένα πεδίο πολυάριθμων ιδιοκτησιακών τεχνολογιών διαχείρισης ταυτότητας.

Ασφαλώς και η πρόσβαση στις ακριβείς πληροφορίες είναι ζωτικής σημασίας όσον αφορά την έρευνα των περιστατικών. Η απόκτηση της πρόσβασης σε δεδομένα που βρίσκονται σε συστήματα καταγραφής προστατευτικής παρακολούθησης και η απόκτηση της δυνατότητας να διεξαχθούν δικαστικοί έλεγχοι σε υπολογιστές και άλλες υποδομές μέσα σε ένα περιβάλλον cloud μπορεί να αποδειχθούν δύσκολη υπόθεση για τους πελάτες του νέφους που διεξάγουν μία έρευνα. Ως εκ τούτου, οι πελάτες θα πρέπει να ξεκαθαρίσουν το συγκεκριμένο θέμα στις συμβατικές τους συμφωνίες με τον πάροχο, και να κατανοήσουν τον τρόπο με τον οποίο ο πάροχος εφαρμόζει την προστατευτική παρακολούθηση μέσα στο cloud περιβάλλον τους. Οι πελάτες που θέτουν συγκεκριμένες ρήτρες σχετικές με τις έρευνες στα συμβόλαιά τους, θα πρέπει να εξετάσουν πώς η δική τους ομάδα ερευνών θα συνεργάζεται με την αντίστοιχη ομάδα ερευνών της επιχείρησης – παρόχου του περιβάλλοντος του νέφους. Αυτό είναι μεγάλης σημασίας, ειδικά όταν μιλάμε για έρευνες που λαμβάνουν χώρο σε πολλαπλά ενοικιαζόμενα συστήματα και οι πάροχοι έχουν χρέος να προστατεύσουν τα δεδομένα των άλλων πελατών. Σε γενικές γραμμές, η συλλογή ψηφιακών αποδείξεων στο νέφος θα έπρεπε να ήταν στην δικαιοδοσία του παρόχου, και να παραδίδεται ως μέρος της αλυσίδας της επιτήρησης των στοιχείων στον πελάτη για την δική τους διαδικασία έρευνας. Σε περίπτωση που οι πελάτες αιτήσουν πιο άμεση πρόσβαση σε συγκεκριμένες συσκευές δεδομένων, οι

οποίες ανήκουν σε κάποια υποδομή την οποία την μοιράζονται πελάτες, τότε ο πάροχος έχει την επιλογή να αλλάξει την αρχιτεκτονική της υπηρεσίας του συγκεκριμένου πελάτη, κάτι που μπορεί να αυξήσει σημαντικά το κόστος του πελάτη, και ως επακόλουθο να επηρεάσει τα αρχικά οικονομικά επιχειρήματα με τα οποία επέλεξαν τις υπηρεσίες νέφους.

2.2.5 **Διασφάλιση Ασφαλείας - Εκτίμηση της Ασφαλείας Τρίτου Παρόχου**

Μία από τις πιο σημαντικές προκλήσεις ενός πελάτη του cloud προπαντός είναι διασφάλιση των ελέγχων ασφαλείας που διεξάγουν οι πάροχοι νέφους. Η συγκεκριμένη πρόκληση οξύνεται από το γεγονός ότι την συγκεκριμένη χρονική στιγμή δεν υπάρχει ένα κοινό πρότυπο ασφάλειας της νεφοϋπολογιστικής στον συγκεκριμένο κλάδο με το οποίο ο πελάτης μπορεί να αξιολογήσει τους παρόχους τους. Κατά κύριο λόγο οι πελάτες ανησυχούν για θέματα όπως ο καθορισμός των απαιτήσεων ασφαλείας, ο διαγνωστικός έλεγχος των παρόχων υπηρεσιών cloud και η διαχείριση των κινδύνων των προμηθευτών νέφους.

- Καθορισμός των απαιτήσεων ασφαλείας: Οι απαιτήσεις ασφάλειας των δεδομένων των πελατών προέρχονται από την πολιτική της ίδιας της επιχείρησης, από νομικές και κανονιστικές υποχρεώσεις και μπορεί να εκτελεστούν μέσω άλλων συμβολαίων ή SLA[14] που η επιχείρηση έχει με τους πελάτες της.
- Διαγνωστικός Έλεγχος των Παρόχων Υπηρεσιών Cloud: Οι υποψήφιοι πελάτες του νέφους θα πρέπει να πραγματοποιούν κατάλληλους διαγνωστικούς ελέγχους για τους παρόχους πριν προβούν στην σύναψη συμβατικών σχέσεων. Η επισταμένη έρευνα παρέχει αμερόληπτη και πολύτιμη αντίληψη για τις παρελθούσες επιδόσεις της επιχείρησης - παρόχου, όπως για την οικονομική της κατάσταση, νομικές ενέργειες που πιθανόν να έχουν γίνει από ή ενάντια της επιχείρησης καθώς και την εμπορική της φήμη. Πιστοποιήσεις όπως το ISO27001 παρέχει στους πελάτες κάποια διαβεβαίωση ότι ο πάροχος cloud έχει λάβει κάποια μέτρα για τη διαχείριση των κινδύνων της ασφάλειας πληροφοριών.
- Διαχείριση κινδύνων των προμηθευτών νέφους: Η ανάθεση των καίριων σημασίας υπηρεσιών σε εξωτερικούς εργάτες μπορεί να ωθήσει τις επιχειρήσεις – πελάτες στην αναζήτηση μιας καινούριας και πιο ώριμης αντιμετώπισης της διαχείρισης των κινδύνων και της υπευθυνότητας. Ενώ η έννοια της νεφοϋπολογιστικής ταυτίζεται με την ανάθεση υπηρεσιών σε τρίτους, ο κίνδυνος παραμένει για τον πελάτη και συνεπώς είναι στο συμφέρον του πελάτη να διαβεβαιώσει ότι οι κίνδυνοι δέχονται την κατάλληλη διαχείριση ανάλογα με το προφίλ τους. Η αποτελεσματική διαχείριση κινδύνου επίσης προϋποθέτει ωριμότητα τόσο στις διαδικασίες διαχείρισης σχέσεων των προμηθευτών, όσο και στις διαδικασίες της επιχειρησιακής ασφάλειας.

[14] Service Level Agreement (SLA) – Σύμβαση Παροχής Υπηρεσιών: Γίνεται ανάμεσα σε έναν πάροχο υπηρεσιών και σε έναν πελάτη, ορίζοντας τις αμοιβαίες προσδοκίες μεταξύ τους. (Anon., 2016)

2.3 **ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΗ ΝΕΦΟΫΠΟΛΟΓΙΣΤΙΚΗ**

Τα θέματα ασφαλείας στη νεφοϋπολογιστική μπορούν να χωριστούν σε τρεις ευρύτερες κατηγορίες, στις παραδοσιακές ανησυχίες ασφαλείας, στα θέματα διαθεσιμότητας και στα θέματα σχετικά με τους εξωτερικούς συνεργάτες. Θα αναφερθούμε στις τρεις παραπάνω κατηγορίες, αλλά επίσης θα επισημάνουμε και κάποιες περαιτέρω αδυναμίες στο cloud computing.

2.3.1 **Παραδοσιακές Ανησυχίες Ασφαλείας**

Αυτού του είδους τα ζητήματα περιλαμβάνουν πληροφοριακές και δικτυακές παραβιάσεις ή επιθέσεις, οι οποίες γίνονται πιθανές ή τουλάχιστον ευκολότερες όταν συζητάμε για μεταφορά και αποθήκευση δεδομένων στο νέφος. Οι πάροχοι cloud αντιδρούν σε αυτές τις προκλήσεις ισχυριζόμενοι ότι τα μέτρα ασφαλείας τους και οι διαδικασίες τους είναι πιο ώριμες σε σχέση με άλλες μικρότερες επιχειρήσεις. Ένα άλλο επιχείρημα από το Jericho Forum (Don't Cloud Vision) εξηγεί: «Θα ήταν ευκολότερος ο αποκλεισμός πληροφοριών εάν διοικείται από κάποιον εξωτερικό συνεργάτη και όχι εσωτερικώς στην εταιρεία, σε περίπτωση που οι επιχειρήσεις ανησυχούν για εσωτερικές απειλές… Επιπροσθέτως, μπορεί να είναι ευκολότερη η εφαρμογή της ασφάλειας μέσω συμβολαίων με παρόχους online υπηρεσιών από ότι μέσω εσωτερικών ελέγχων.»

Οι ανησυχίες σε αυτήν την κατηγορία περιλαμβάνουν τα εξής:

- Επιθέσεις στο Virtual Machine επίπεδο: Οι ενδεχόμενες αδυναμίες στον υπερόπτη (hypervisor) ή στην VM τεχνολογία που χρησιμοποιείται από τους cloud προμηθευτές είναι ένα πιθανό πρόβλημα στις πολλαπλής ενοικίασης αρχιτεκτονικές. Αδυναμίες έχουν εμφανιστεί στα εξής λογισμικά εικονικοποίησης: VMWare (Security Tracker: VMWare Shared Folder Bug), Xen (Xen Vulnerability), Microsoft Virtual PC και Virtual Server (Microsoft Security Bulletin MS07-049). Προμηθευτές όπως η Third Brigade μετριάζει ενδεχόμενες αδυναμίες στο VM επίπεδο μέσω της παρακολούθησης και των firewalls.
- Αδυναμίες των παρόχων υπηρεσιών cloud: Αυτές οι αδυναμίες μπορεί να είναι είτε στο επίπεδο πλατφόρμας, λόγου χάριν μία παρεμβολή στην SQL ή αδυναμία στο cross-site scripting [15] . Για παράδειγμα, έχουν εντοπιστεί αδυναμίες σε κάποια πρόσφατα Google Docs (Microsoft Security Bulletin MS07-049). Η IBM έχει επανατοποθετήσει το Rational AppScan, το οποίο σαρώνει ψάχνοντας για αδυναμίες σε διαδικτυακές υπηρεσίες σαν υπηρεσία ασφάλειας cloud (IBM Blue Cloud Initiative).
- Phishing – Ηλεκτρονικό Ψάρεμα: Οι phishers και άλλοι που ασκούν τεχνικές κοινωνικής μηχανικής έχουν καινούριου είδους μέσο επιθέσεων (Salesforce.Com – προειδοποιεί τους πελάτες).
- Εκτεταμένη επιφάνεια δικτυακών επιθέσεων: Ο χρήστης του νέφους πρέπει να προστατεύει την υποδομή που χρησιμοποιεί για να συνδεθεί και να αλληλεπιδράσει με το cloud, μία εργασία που είναι αρκετά δύσκολη καθώς το νέφος βρίσκεται σε πολλές περιπτώσεις έξω από το firewall.
- Έλεγχος ταυτότητας και εξουσιοδότηση: Το πλαίσιο ελέγχου ταυτότητας και εξουσιοδότησης της επιχείρησης δεν επεκτείνεται στο cloud. Άρα πώς μία επιχείρηση

[15] Cross-Site Scripting ή XSS: είναι η εκμετάλλευση διαφόρων ευπαθειών υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή JavaScript σε κάποιον ιστοχώρο.

συγχωνεύει στο ήδη υπάρχων πλαίσιο τους πόρους του cloud; Πώς μία επιχείρηση συγχωνεύει τα δεδομένα ασφαλείας του νέφους (εάν υπάρχουν) με τα δικά της κριτήρια και πολιτικές;

- Εγκληματολογία στο cloud: Το έργο CLOIDIFIN (Stephen Biggs, 2009) ανασκοπεί τη δυσκολία των εγκληματολογικών ερευνών στο νέφος: «Οι παραδοσιακές ψηφιακές εγκληματολογικές μεθοδολογίες επιτρέπουν στους ερευνητές να εκμεταλλευτούν τον εξοπλισμό και να διεξάγουν λεπτομερής ανάλυση στα μέσα και στα δεδομένα που ανέκτησαν. Συνεπώς, η πιθανότητα της αφαίρεσης, αντικατάστασης, διαγραφής ή καταστροφής δεδομένων από το δράστη, σε αυτήν την περίπτωση βρίσκεται σε χαμηλά επίπεδα. Πλησιέστερα συνδεδεμένο σε ένα νεφοϋπολογιστικό περιβάλλον, θα μπορούσαμε να πούμε ότι είναι επιχειρήσεις που κατέχουν και διαχειρίζονται την δική τους υποδομή με πολλαπλούς servers, αν και μία τέτοια επιχείρηση θα ήταν σε μία πολύ μικρότερη συγκριτική κλίμακα. Παρ' όλα αυτά, το μέγεθος του νέφους και ο ρυθμός με τον οποίο αντικαθίστανται τα δεδομένα προκαλεί ανησυχία.»

2.3.2 **Διαθεσιμότητα**

Αυτές οι ανησυχίες επικεντρώνονται στη διαθεσιμότητα κρίσιμων εφαρμογών και δεδομένων. Κάποια από τα πολυσυζητημένα παραδείγματα λειτουργικής διακοπής cloud είναι το μονοήμερο κλείσιμο του Gmail στα μέσα Οκτωβρίου του 2008 (Extended Gmail Outage), οι διακοπή λειτουργίας για περισσότερο από επτά ώρες του Amazon S3 στις 20 Ιουλίου 2008 (Amazon S3 Availability Event, 2008) και η δεκαοκτάωρη αναστολή λειτουργίας του FlexiScale στις 31 Οκτωβρίου 2008 (FlexiScale Outage). Η διατήρηση του χρόνου ομαλής λειτουργίας, η αποτροπή επιθέσεων «άρνησης παροχής υπηρεσιών – denial of service (DoS)» (ειδικότερα στην αστοχία ενός και μόνον σημείου) και η εξασφάλιση της ανθεκτικότητας υπολογιστικής ακεραιότητας (π.χ. ο πάροχος νέφους τρέχει μία εφαρμογή πιστά και δίνει έγκυρα αποτελέσματα) είναι κάποια από τα μείζον θέματα σε αυτή την κατηγορία απειλών.

2.3.3 **Έλεγχος Δεδομένων από Εξωτερικούς Συνεργάτες**

Οι νομικές επιπτώσεις των δεδομένων και των εφαρμογών που κρατούνται από κάποιον εξωτερικό συνεργάτη είναι πολύπλοκες και δυσνόητες. Επίσης όταν κάποιος εξωτερικός συνεργάτης είναι υπεύθυνος για τα δεδομένα, υπάρχει και μία πιθανή έλλειψη ελέγχου και διαφάνειας. Μέρος της φήμης της νεφοϋπολογιστικής είναι ότι το νέφος είναι ανεξάρτητο από τις εφαρμογές, αλλά στην πραγματικότητα, η κανονιστική συμμόρφωση απαιτεί διαφάνεια μέσα στο νέφος. Ποικίλα ζητήματα δεδομένων και ασφάλειας παρακινούν μερικές εταιρείες να αναπτύξουν clouds για αποφυγή αυτών των θεμάτων και ακόμη να διατηρήσουν κάποια από τα πλεονεκτήματα του cloud computing. Όμως οφείλουμε να ερευνήσουμε καταλλήλως τις παρακάτω ανησυχίες.

Διαγνωστικός Έλεγχος: Σε περίπτωση κλήτευσης ή κάποιας άλλης δικαστικής αγωγής, μπορεί ο χρήστης του νέφους να υποχρεώσει τον πάροχο να ανταποκριθεί στο απαιτούμενο χρονικό διάστημα; Μία σχετική ερώτηση είναι η αποδειξιμότητα διαγραφής και η αντιστοίχησή της με την πολιτική διατήρηση της επιχείρησης: Πώς μπορεί ο χρήστης να είναι σίγουρος ότι η διαγραφή των δεδομένων έγινε από τον πάροχο cloud;

Δυνατότητα Ελέγχου: Μία επιπλέον αρνητική συνέπεια της έλλειψης χειρισμού στο νέφος είναι η δυσκολία στον έλεγχο. Υπάρχει επαρκής διαφάνεια στις λειτουργίες του παρόχου νέφους για ελεγκτικούς σκοπούς; Προς το παρόν, η διαφάνεια επιτυγχάνεται μέσω της τεκμηρίωσης και από μη αυτοματοποιημένους ελέγχους. Η εκτέλεση ενός οικουμενικού εσωτερικού ελέγχου σε ένα καθολικό και δυναμικό υπολογιστικό περιβάλλον πολλαπλής

ενοικίασης, είναι μία μεγάλη πρόκληση, καθώς ορισμένοι κανονισμοί απαιτούν τα δεδομένα και οι λειτουργίες να παραμένουν σε συγκεκριμένες γεωγραφικές τοποθεσίες.

Συμβατικές Υποχρεώσεις: Ένα πρόβλημα που παρουσιάζεται με την χρήση υποδομής μίας άλλης επιχείρησης, πέρα από την αβέβαιη ευθυγράμμιση των συμφερόντων, είναι η ύπαρξη αιφνίδιων νομικών επιπτώσεων. Για παράδειγμα, ένα απόσπασμα από τους όρους χρήσης του Amazon είναι ως εξής: «Μη διεκδίκηση» κατά τη διάρκεια και μετά τη λήξη της συμφωνίας, εν σχέση με οποιαδήποτε υπηρεσία επιλέξετε να χρησιμοποιήσετε. Δε θα δηλώσετε, ούτε θα εξουσιοδοτήσετε, βοηθήσετε ή ενθαρρύνετε οποιοδήποτε τρίτο μέλος να διεκδικήσει, εναντίον εμάς ή εναντίον οποιουδήποτε πελάτη μας, τελικού χρήστη, προμηθευτή, συνεταίρου (συμπεριλαμβανομένων των εξωτερικών πωλητών σε ιστότοπους που είναι διαχειριζόμενοι από εμάς ή εκ μέρους μας), δικαιούχου ή υπο-δικαιούχου, οποιαδήποτε προσβολή διπλώματος ευρεσιτεχνίας ή κάποιον άλλον ισχυρισμό παραβίασης πνευματικής ιδιοκτησίας σε σχέση με τέτοιες Υπηρεσίες.» Διαβάζοντας τα παραπάνω, μπορούμε να συμπεράνουμε ότι μετά από τη χρήση της υπηρεσίας E2C, δεν υπάρχει δυνατότητα υποβολής ισχυρισμού παραβάσεων εναντίον του Amazon. Δεν είναι ξεκάθαρο εάν ο όρος χρήσης που αφορά την μη διεκδίκηση θα γίνει δεκτός από τα δικαστήρια, αλλά η κάθε αβεβαιότητα θεωρείται κακή για την επιχείρηση.

Κατασκοπία παρόχου νέφους: Είναι απαραίτητο να αναφέρουμε τον φόβο κλοπής ιδιοκτησιακών πληροφοριών της επιχείρησης από τον πάροχο νέφους.

Μεταβατική των συμβολαίων: Μία άλλη πιθανή ανησυχία είναι ότι οι συμβασιούχοι πάροχοι νέφους, μπορεί να χρησιμοποιούν «υπεργολάβους». Ο χρήστης είτε δεν έχει τον έλεγχο ή έχει ελάχιστο έλεγχο πάνω στον «υπεργολάβο». Ωστόσο ο υπεργολάβος είναι σημαντικό να είναι αξιόπιστος. Για παράδειγμα, η online υπηρεσία αποθήκευσης Linkup χρησιμοποιεί την online επιχείρηση αποθήκευσης Nirvanix για τις cloud υπηρεσίες. (Brodkin, 2008) Ένα άλλο παράδειγμα είναι η Carbonite, η οποία χρησιμοποιεί τους δικούς της προμηθευτές hardware για τον ελαττωματικό εξοπλισμό που προκαλεί απώλεια δεδομένων πελατών. (Mearian, 2009)

2.4 **ΑΝΑΔΥΟΜΕΝΕΣ ΑΠΕΙΛΕΣ ΣΤΗΝ ΝΕΦΟΫΠΟΛΟΓΙΣΤΙΚΗ**

Εδώ θα συζητήσουμε κάποιες επιπρόσθετες απειλές ασφαλείας που σχετίζονται με το cloud computing και εντοπίζονται και ερευνώνται ακαδημαϊκά, από οργανισμούς ασφαλείας και από τους παρόχους cloud αλλά και τους χρήστες.

Επιθέσεις πλαγίου μονοπατιού (side channel attacks): Μία διαφαινόμενη ανησυχία για τα μοντέλα υπηρεσιών που χρησιμοποιούν πλατφόρμα εικονικοποίησης είναι ο κίνδυνος των επιθέσεων πλαγίου μονοπατιού, που προκαλούν διαρροή δεδομένων σε αλληλοσυνδεόμενες περιπτώσεις virtual machine. Αυτός ο κίνδυνος είναι εξελίξιμος, αν και την συγκεκριμένη στιγμή θεωρείται ότι βρίσκεται στα αρχικά του στάδια, καθώς οι virtual machine τεχνολογίες τώρα ωριμάζουν. Εν τούτοις, είναι πιθανόν εισβολείς οι οποίοι αποτυγχάνουν να εκθέσουν σε κίνδυνο τελικά σημεία ή να διεισδύσουν στην υποδομή του νέφους έξω από την περίμετρο του cloud, να εξετάσουν τη χρήση αυτής της τεχνικής, δηλαδή να δράσουν ως ανέντιμος πελάτης μέσα σε μία κοινή υποδομή νέφους και να έχουν πρόσβαση στα δεδομένα άλλων πελατών.

Άρνηση παροχής υπηρεσιών (denial of service – DoS): Η διαθεσιμότητα είναι μία από τις πρωταρχικές ανησυχίες που έχουν οι πελάτες του νέφους και το ίδιο αντιστοιχεί για τους

παρόχους νέφους, οι οποίοι πρέπει να σχεδιάσουν λύσεις για τη μείωση της συγκεκριμένης απειλής. Παραδοσιακά, η άρνηση παροχής υπηρεσιών έχει συνδεθεί με τις διανεμημένες επιθέσεις στο network επίπεδο προκαλώντας υπερφόρτωση της υποδομής με υπερβολική κίνηση με σκοπό να επιτύχει την αποτυχία κρίσιμων στοιχείων ή την κατανάλωση όλων των διαθέσιμων hardware πόρων. Μέσα στις υποδομές πολλαπλής ενοικίασης του νέφους, υπάρχουν συγκεκριμένες απειλές που σχετίζονται με την άρνηση παροχής υπηρεσιών. Μία από αυτές είναι η κατανάλωση κοινών πόρων. Πιο συγκεκριμένα, αναφερόμαστε σε επιθέσεις που στερούν από τους υπόλοιπους πελάτες τους πόρους του συστήματος όπως χρόνο εκτέλεσης νήματος[16], μνήμη, χώρο αποθήκευσης και διεπαφή δικτύου. Επίσης υπάρχει η πιθανότητα επιθέσεων εκμετάλλευσης του hypervisor και της Virtual Machine. Σε αυτή την περίπτωση έχουμε επιθέσεις εκμετάλλευσης αδυναμιών στον θεμελιώδη hypervisor και έτσι το λειτουργικό σύστημα που συγκροτεί μία περίπτωση Virtual Machine θα επιτρέψει στους εισβολείς να προκαλέσουν στοχευμένες διακοπές λειτουργίας ή αστάθεια. Οι επιθέσεις που χρησιμοποιούν τέτοιες μεθόδους είναι σχεδιασμένες να παρακάμπτουν την παραδοσιακά καλά σχεδιασμένη αρχιτεκτονική του νέφους, η οποία επικεντρώνεται στην ασφάλεια ενάντια στις επιθέσεις DoS που βασίζονται στο εξωτερικό δίκτυο.

Επιθέσεις κοινωνικών δικτύων: Με την αυξανόμενη δημοτικότητα των επιχειρησιακών και προσωπικών ιστοσελίδων κοινωνικής δικτύωσης, υπάρχει σημαντική αύξηση και στον φόβο για μία πιο προηγμένη επίθεση τύπου κοινωνικής μηχανικής. Τα νεφοϋπολογιστικά συστήματα γίνονται στόχος λόγω του μεγάλου πλήθους πελατών. Οι πολύπλοκες σχέσεις μεταξύ των παρόχων νέφους, πελατών και προμηθευτών σημαίνουν ότι υπάλληλοι αυτών των οργανισμών είναι καταχωρημένοι σε ιστοσελίδες κοινωνικής δικτύωσης και συνδέονται μεταξύ τους. Οι εισβολείς δημιουργούν ταυτότητες για να κερδίσουν την εμπιστοσύνη, και χρησιμοποιούν online πληροφορίες για να καθορίσουν σχέσεις και ρόλους προσωπικού έτσι ώστε να ετοιμάσουν τις επιθέσεις τους. Ένας συνδυασμός τεχνικής επίθεσης και επίθεσης κοινωνικής μηχανικής μπορεί να αναπτυχθεί ενάντια κάποιου στοχευμένου χρήστη, εκμεταλλευόμενοι των γνωριμιών τους και το online κοινωνικό δίκτυο που χρησιμοποιούν.
Επιθέσεις σε κινητές συσκευές: Η χρήση των κινητών συσκευών έχει αυξηθεί και πλέον η συνδεσιμότητα με το νέφος δεν είναι εφικτή μόνο μέσω των φορητών και επιτραπέζιων λογαριασμών. Σήμερα εμφανίζονται επιθέσεις που στοχεύουν τις κινητές συσκευές και βασίζονται σε χαρακτηριστικά που παραδοσιακά σχετίζονται με φορητούς και επιτραπέζιους ηλεκτρονικούς υπολογιστές, συμπεριλαμβανομένων:

- Συσκευές πλούσιες διεπαφές προγραμματισμού εφαρμογών (Application Programming Interface – API)[17] που υποστηρίζουν δικτυακές επικοινωνίες και υπηρεσίες υποστήριξης.
- Συσκευές που βρίσκονται πάντα σε ασύρματη πρόσβαση στο Διαδίκτυο.
- Συσκευές με μεγάλες δυνατότητες αποθήκευσης τοπικών δεδομένων.

Καθώς οι κινητές συσκευές στις μέρες μας διαθέτουν ανάλογα χαρακτηριστικά, διαδικτυακό λογισμικό spyware, ιοί τύποι worm ή ακόμα φυσικής υπόστασης επιθέσεις είναι πιο πιθανόν να συμβούν καθώς θεωρείται ένας λιγότερος ριψοκίνδυνος στόχος από τους εισβολείς που επιθυμούν να παραμείνουν μη ανιχνεύσιμοι. Γενικά αυτό υποστηρίζεται από το γεγονός ότι οι περισσότερες κινητές συσκευές δεν έχουν τις ανάλογες λειτουργίες ασφαλείας

[16] Νήμα εκτέλεσης: Ελαφριά διεργασία. Μικρότερη ακολουθία προγραμματισμένων εντολών που μπορεί να υποστεί διαχείριση ανεξάρτητα από το λειτουργικό σύστημα.
[17] Διεπαφή Προγραμματισμού Εφαρμογών (API): Ονομάζεται η διεπαφή των προγραμματιστικών διαδικασιών που παρέχει ένα λειτουργικό σύστημα, εφαρμογή ή βιβλιοθήκη ώστε να είναι δυνατές οι αιτήσεις από άλλα προγράμματα ή ανταλλαγή δεδομένων.

ενεργοποιημένες, ή ακόμα σε μερικές περιπτώσεις δεν είναι διαθέσιμες. Λόγου χάριν, κάποιο ώριμο antimalware, antivirus ή τεχνολογίες πλήρης κρυπτογράφησης δίσκου δεν είναι διαδεδομένες στα smartphones που κυκλοφορούν σήμερα.

Απειλές δικτυωμένου και οργανωμένου εγκλήματος: Οι πάροχοι νέφους αποθηκεύουν ένα εύρος διαφορετικών τύπων δεδομένων, συμπεριλαμβανομένων των πιστωτικών καρτών και άλλων οικονομικών και προσωπικών δεδομένων. Όλα αυτά τα δεδομένα μπορούν να συγκεντρωθούν από πολλαπλούς πελάτες και συνεπώς να γίνουν μεγάλης σημασίας για τους εγκληματίες. Υπάρχει επίσης ο κίνδυνος ότι οι κάτοχοι προνομιακών πληροφοριών μπορούν να χρησιμοποιηθούν σκόπιμα για απόκτηση πρόσβασης σε δεδομένα πελατών και συστήματα ανίχνευσης, προκειμένου να βοηθηθεί οποιοσδήποτε εξωτερικός επιτιθέμενος που απαιτεί πρόσθετες πληροφορίες για την εκτέλεση σύνθετης επίθεσης μέσω διαδικτύου. Οι πελάτες του νέφους θα πρέπει να διαβεβαιώσουν ότι οι πάροχοι είναι γνώστες της συγκεκριμένης απειλής και ακολουθούν αυστηρές διαδικασίες επικύρωσης ταυτότητας και διαδικασίες ελέγχου ασφαλείας κατά τη διάρκεια της διαδικασίας πρόσληψης προσωπικού.

Φθηνά δεδομένα και ανάλυση δεδομένων: Η διάδοση του cloud computing έχει δημιουργήσει πελώριες συσκευές δεδομένων, οι οποίες μπορούν να αποκομίσουν οικονομικά οφέλη μέσω εφαρμογών όπως για παράδειγμα με τη διαφήμιση. Η Google, λόγου χάρη, επωφελείται την δική της υποδομή νέφους για να συλλέξει και να αναλύσει τα δεδομένα των πελατών της για το δίκτυο διαφήμισής της. Η συλλογή και η ανάλυση των δεδομένων είναι πλέον πολύ φθηνή, ακόμα και για τις εταιρείες που δε διαθέτουν τους πόρους της Google. Η διαθεσιμότητα των δεδομένων και οι φθηνές τεχνικές εξόρυξης δεδομένων έχουν μεγάλο αντίκτυπο στην προστασία των δεδομένων των χρηστών. Οι επιτιθέμενοι έχουν τεράστιες κεντρικές βάσεις δεδομένων διαθέσιμες για ανάλυση καθώς και υπολογιστική ισχύ για την εξόρυξη αυτών των βάσεων δεδομένων. Εξαιτίας των ανησυχιών για την ιδιωτικότητα, οι επιχειρήσεις που χρησιμοποιούν clouds για την συλλογή δεδομένων συναντούν όλο και περισσότερο την απαίτηση ανωνυμοποίησης των δεδομένων τους. Το Electronic Privacy Information Center (EPIC) ζήτησε από την Ομοσπονδιακή Επιτροπή Εμπορίου (US Federal Trade Commission – FTC) να ανασταλθεί η λειτουργία των εφαρμογών της Google (Gmail, Google Docs, Google Desktop, Picasa Web Albums και Google Calendar) μέχρι την ενσωμάτωση κατάλληλης προστασίας προσωπικών δεδομένων. (Digital Trends Staff, 2009) Πλέον η Google και η Yahoo!, λόγω της πίεσης που δέχτηκαν από υπέρμαχους της ιδιωτικότητας, εφαρμόζουν μία πολιτική διατήρησης δεκαοχτώ μηνών για τα δεδομένα αναζήτησής τους. Κατά το πέρας των δεκαοχτώ μηνών τα δεδομένα πρέπει να ανωνυμοποιηθούν, αφαιρώντας κάποια αναγνωριστικά στοιχεία, όπως τις IP διευθύνσεις και τις cookies πληροφορίες. Τα ανωνυμοποιημένα δεδομένα όμως διατηρούνται για την στήριξη των συνεχών δοκιμών των αλγορίθμων τους. Ένας άλλος λόγος για την ανωνυμοποίηση των δεδομένων είναι για την διοχέτευσή τους σε άλλους ενδιαφερόμενους για την υποστήριξη έρευνας (Περιστατικό AOL[18]) ή για την ανάθεση της εξόρυξης

[18] «Περιστατικό της American On Line – AOL»: Το 2006 ήρθε στην δημοσιότητα βάση δεδομένων με 20.000.000 λέξεις – κλειδιά αναζήτησης για παραπάνω από 650.000 χρήστες (περιόδου 3 μηνών), με την αντικατάσταση της ταυτότητας χρήσης τους από αριθμητικό ιδιοχαρακτηριστικό ως το μόνο μέτρο προστασίας της ιδιωτικότητας. Αυτή η ενέργεια είχε ως επακόλουθο τη δημόσια εξακρίβωση ταυτότητας και τοποθεσίας ορισμένων χρηστών. Οι συμβολοσειρές των ερωτημάτων αναζήτησης που υποβάλλονται σε μηχανές αναζήτησης με χρήση ψευδονύμου, κυρίως εάν συνδιαστούν και με άλλα ιδιοχαρακτηριστικά, όπως διευθύνσεις IP και άλλες παραμετροποιήσεις, αυξάνουν τις πιθανότητες ταυτοποίησης. (Ομάδα Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων , 2014)

δεδομένων σε τρίτους (Βραβείο Netflix[19]). Καθώς αυξάνεται η ανάπτυξη εφαρμογών cloud, αναλόγως αυξάνονται και οι απαιτήσεις για πιο εξελιγμένα εργαλεία για την επίτευξη ισχυρής ανωνυμοποίησης.

Οικονομικά αποδοτική προστασία της διαθεσιμότητας: Μία άλλη παράμετρος που οφείλουμε να εξετάσουμε στην περίπτωση ενός αντιπάλου που έχει ως σκοπό το σαμποτάζ των δραστηριοτήτων, είναι η διαθεσιμότητα. Οι συγκεκριμένοι αντίπαλοι αυξάνονται καθώς οι πολιτικές συγκρούσεις μεταφέρονται στο διαδίκτυο, όπως για παράδειγμα οι επιθέσεις στις κυβερνητικές ιστοσελίδες της Λιθουανίας το 2016. Οι ζημιές από αυτού του είδους τις επιθέσεις, δε συνδέονται μόνο με απώλεια παραγωγικότητας αλλά επίσης υποβαθμίζουν την εμπιστοσύνη απέναντι στην υποδομή και καθιστούν την διαδικασία δημιουργίας αντιγράφων ασφαλείας πιο δαπανηρή.

Αυξημένες απαιτήσεις ταυτοποίησης: Η ανάπτυξη του cloud computing μπορεί, καθ’ υπερβο (Ward, 2009)λήν, να επιτρέψει στους πελάτες τη χρήση ελαφρών τερματικών (thin client). Αντί να αγοραστεί μία άδεια χρήσης και να εγκατασταθεί κάποιο software στην πλευρά του πελάτη, οι χρήστες θα επαληθεύουν την ταυτότητά τους για να χρησιμοποιήσουν μία εφαρμογή στο νέφος. Σε αυτό το μοντέλο, υπάρχουν κάποια προτερήματα, όπως η δυσκολότερη software πειρατεία και η διευκόλυνση της κεντρικής παρακολούθησης. Επίσης, είναι πιθανόν να βοηθήσει στην αποτροπή διάδοσης ευαίσθητων δεδομένων ή αναξιόπιστων πελατών. Αυτή η αρχιτεκτονική επιπλέον υποστηρίζει την αυξημένη κινητικότητα των χρηστών, αλλά ταυτόχρονα απαιτεί και πιο ισχυρά πρωτόκολλα επικύρωσης ταυτότητας. Επιπρόσθετα, το κίνημα υπέρ της αύξησης φιλοξενίας των δεδομένων και των εφαρμογών στο νέφος και της μείωσης εξάρτησης από συγκεκριμένες μηχανές χρηστών, είναι πιθανό να αυξήσει την απειλή του phishing και της κλοπής των στοιχείων πρόσβασης.

Συνδυαστική εφαρμογή επαλήθευσης ταυτότητας: Καθώς η υιοθέτηση της νεφοϋπολογιστικής εξαπλώνεται, θα εμφανίζονται όλο και περισσότερες υπηρεσίες συνδυαστικής εφαρμογής δεδομένων. Αυτή η εξέλιξη έχει πιθανές επιπτώσεις στην ασφάλεια τόσο από την πλευρά της διαρροής των δεδομένων όσο και από τον αριθμό των πηγών που ενδέχεται να χρειαστεί να τραβήξει ο χρήστης δεδομένα. Αυτό, με τη σειρά του, θέτει απαιτήσεις για τον τρόπο με τον οποίο επιτρέπεται η πρόσβαση. Ένας κεντρικός μηχανισμός ελέγχου πρόσβασης πιθανόν δεν είναι εφικτή λύση σε τέτοια σενάρια ανάπτυξης. Μπορούμε να πάρουμε ως παράδειγμα το Facebook. Οι χρήστες του Facebook ανεβάζουν ευαίσθητα και μη ευαίσθητα δεδομένα. Αυτά τα δεδομένα χρησιμοποιούνται από το ίδιο το Facebook και παρουσιάζονται σε άλλους χρήστες, αλλά επίσης αξιοποιούνται και από τρίτες εφαρμογές. Καθώς αυτές οι εφαρμογές συνήθως δεν είναι επαληθευμένες από το Facebook, κακόβουλες εφαρμογές που εκτελούνται στο νέφος του Facebook μπορούν δυνητικά να κλέψουν ευαίσθητα δεδομένα, όπως και έγινε τον Μάρτιο του 2009. (Ward, 2009)

[19] «Βραβείο Netflix»: Ανοιχτός διαγωνισμός που διεξήχθει το 2009 για την εύρεση του καλύτερου συνεργατικού φιλτραρίσματος της πρόβλεψης των αξιολογήσεων που γίνονταν από τους χρήστες για της ταινίες.

ΚΕΦΑΛΑΙΟ 3

3.1 **ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΑΣΦΑΛΕΙΑ ΣΤΟ** CLOUD COMPUTING

Το βασικό ζήτημα είναι ότι με την άφιξη της νεφοϋπολογιστικής, ο πάροχος νέφους έχει και αυτός κάποιον έλεγχο των δεδομένων των χρηστών του νέφους. Συνεπώς, κάποιες προτάσεις παρακάτω έχουν γίνει με τέτοιον τρόπο ώστε οι τρέχουσες δυνατότητες του cloud να μην περιορίζονται, περιορίζοντας παράλληλα τον έλεγχο του παρόχου νέφους στα δεδομένα, και επιτρέποντας σε όλους του χρήστες cloud να επωφεληθούν από τη χρήση της υπηρεσίας.
Ασφάλεια επικεντρωμένη στις πληροφορίες: Προκειμένου οι επιχειρήσεις να επεκτείνουν τον έλεγχο των δεδομένων στο cloud, ίσως αξίζει να ακολουθήσουμε μία προσέγγιση εσωτερικής προστασίας δεδομένων. Αυτή η προσέγγιση είναι γνωστή ως ασφάλεια πληροφοριών (information-centric computing). Η συγκεκριμένη τεχνική αυτοπροστασίας απαιτεί την εισαγωγή ευφυίας στα ίδια τα δεδομένα. Τα δεδομένα θα πρέπει να είναι αυτοπεριγραφικά και να αυτοελέγχονται, ανεξάρτητα από το περιβάλλον στο οποίο βρίσκονται. Όταν γίνεται πρόσβαση στα δεδομένα, αυτά λαμβάνουν υπ' όψιν την πολιτική τους και επιχειρούν να αναδημιουργήσουν ένα ασφαλές περιβάλλον το οποίο έχει πιστοποιηθεί ως αξιόπιστο στα πλαίσια του trusted computing[20].

Πιστοποίηση απομακρυσμένου διακομιστή υψηλού βαθμού βεβαιότητας: Επί του παρόντος, η έλλειψη διαφάνειας αποθαρρύνει τις επιχειρήσεις να μεταφέρουν τα δεδομένα τους στο νέφος. Οι κάτοχοι των δεδομένων επιθυμούν να ελέγχουν τον τρόπο με τον οποίο γίνεται ο χειρισμός των δεδομένων τους στο περιβάλλον του cloud, και ειδικότερα να διασφαλίσουν ότι τα δεδομένα τους βρίσκονται σε μικρότερο κίνδυνο κατάχρησης ή διαρροής (σε περίπτωση που γίνει κάτι τέτοιο απαιτείται τουλάχιστον ένα αναλλοίωτο ιστορικό ελέγχου). Προς το παρόν, οι πελάτες αρκούνται με τις διαδικασίες χειροκίνητου ελέγχου, όπως το SAS-70 [21] . Μία πολλά υποσχόμενη προσέγγιση για την αντιμετώπιση αυτού του προβλήματος βασίζεται στο trusted computing. Σε ένα περιβάλλον trusted computing, εγκαθίσταται ένα αξιόπιστο σύστημα παρακολούθησης στον cloud server, το οποίο παρακολουθεί ή ελέγχει τις διεργασίες του ίδιου του cloud server. Αυτό το σύστημα παρακολούθησης έχει τη δυνατότητα να παρέχει απόδειξη συμμόρφωσης στους κανόνες στον κάτοχο των δεδομένων, διασφαλίζοντας με αυτόν τον τρόπο ότι δεν έχουν παραβιαστεί συγκεκριμένες πολιτικές πρόσβασης. Για την διασφάλιση του συστήματος παρακολούθησης, το trusted computing επίσης επιτρέπει την ασφαλή εκκίνηση του συγκεκριμένου συστήματος παρακολούθησης ώστε να τρέχει δίπλα (και με ασφάλεια απομονωμένο) από το λειτουργικό σύστημα και τις εφαρμογές. Το σύστημα παρακολούθησης μπορεί να επιβάλλει πολιτικές ελέγχου πρόσβασης και εκτελεί εργασίες παρακολούθησης και ελέγχου. Για την απόδειξη της συμμόρφωσης υπογράφεται ο κώδικας της παρακολούθησης, καθώς και μία δήλωση συμμόρφωσης που παράγεται από το σύστημα παρακολούθησης. Όταν ο κάτοχος προσττων δεδομένων λαμβάνει αυτή την απόδειξη συμμόρφωσης, μπορεί να επαληθεύσει ότι εκτελείται ο σωστός κώδικας του συστήματος παρακολούθησης και ότι ο server του cloud έχει συμμορφωθεί με τις πολιτικές ελέγχου πρόσβασης.

[20] Trusted Computing: ο υπολογιστής συμπεριφέρεται σταθερά με τους αναμενόμενους τρόπους και αυτές οι συμπεριφορές εκτελούνται από το hardware και το software του υπολογιστή. Η εκτέλεση της συμπεριφοράς αυτής επιτυγχάνεται με την φόρτωση του hardware με ένα μοναδικό κλειδί κρυπτογράφησης μη προσβάσιμο στο υπόλοιπο σύστημα. Η τεχνολογία αυτή αναπτύχθηκε από το Trusted Computing Group (TCG). (Mitchell, 2005)

[21] SAS-70: αναγνωρισμένο πρότυπο ελέγχου και διαδικασιών. Δημιούργημα του American Institute of Certified Public Accountants (AICPA).

Επιχειρηματική ευφυΐα επαυξημένου απορρήτου: Μία διαφορετική προσέγγιση για τη διατήρηση του ελέγχου των δεδομένων είναι απαραίτητη κρυπτογράφηση όλων των δεδομένων στο νέφος. Το πρόβλημα στη συγκεκριμένη προσέγγιση είναι ότι η κρυπτογράφηση περιορίζει τη χρήση των δεδομένων. Συγκεκριμένα, η αναζήτηση και η εύρεση των δεδομένων καθίστανται προβληματικές, εάν όχι αδύνατον. Για παράδειγμα, εάν τα δεδομένα είναι αποθηκευμένα σε μορφή ακρυπτογράφητου κειμένου, μπορεί κάποιος αποτελεσματικά να αναζητήσει ένα έγγραφο με μία λέξη-κλειδί, κάτι που είναι αδύνατο να γίνει με την εφαρμογή προγραμμάτων παραδοσιακής και τυχαίας κρυπτογράφησης. Οι σύγχρονοι κρυπτογραφικοί μηχανισμοί μπορούν να προσφέρουν νέα εργαλεία για την επίλυση αυτών των προβλημάτων. Οι κρυπτογράφοι έχουν εφεύρει ευέλικτα συστήματα κρυπτογράφησης που επιτρέπουν λειτουργίες και υπολογισμούς στο κρυπτογραφημένο κείμενο. Λόγου χάριν, η κρυπτογράφηση με δυνατότητα αναζήτησης (searchable encryption ή αλλιώς predicate encryption) επιτρέπει στον κάτοχο των δεδομένων να υπολογίσει κάποια δυνατότητα από το μυστικό του κλειδί. Αυτή η δυνατότητα κωδικογραφεί ένα ερώτημα αναζήτησης, και το νέφος μπορεί να χρησιμοποιήσει τη δυνατότητα για να κρίνει ποια έγγραφα ταιριάζουν στο ερώτημα αναζήτησης, χωρίς να αποκτά πρόσβαση σε πρόσθετες πληροφορίες. Άλλες αρχικές μορφές κρυπτογράφησης, όπως η ομοιομορφική κρυπτογράφηση και ιδιωτική ανάκτηση πληροφοριών εκτελούν υπολογισμούς σε κρυπτογραφημένα δεδομένα πηγών χωρίς να γίνει αποκρυπτογράφηση. Καθώς αυτές οι κρυπτογραφικές τεχνικές ωριμάζουν, θα δημιουργηθούν νέες δυνατότητες και κατευθύνσεις για την έρευνα και την ανάπτυξη πρωτοκόλλων και αλγορίθμων για την ασφάλεια του cloud.

Ενώ σε πολλές περιπτώσεις χρειαζόμαστε την διεξαγωγή περεταίρω έρευνας για να καταστούν αυτά τα κρυπτογραφικά εργαλεία επαρκώς πρακτικά για το νέφος, αυτήν τη στιγμή παρουσιάζουν την καλύτερη ευκαιρία καθαρής διαφοροποίησης για τη νεφοϋπολογιστική, καθώς αυτοί οι μηχανισμοί μπορούν να επιτρέψουν στους χρήστες να επωφεληθούν από τα δεδομένα κάποιου άλλου με ελεγχόμενο τρόπο. Πιο συγκεκριμένα, ακόμα και τα κρυπτογραφημένα δεδομένα μπορούν να διευκολύνουν την ανίχνευση ανωμαλιών, η οποία είναι πολύτιμη από την πλευρά της επιχειρηματικής ευφυίας. Εκτός από την εξασφάλιση της ιδιωτικότητας, η εφαρμοσμένη κρυπτογραφία προσφέρει επίσης εργαλεία για την αντιμετώπιση άλλων προβλημάτων ασφαλείας που σχετίζονται με τη νεφοϋπολογιστική.

Στον παρακάτω πίνακα συνοψίζουμε μερικά θέματα ασφαλείας σημαντικής σημασίας που συναντούμε στο cloud computing και τους πιθανούς αμυντικούς μηχανισμούς τους.

ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ	ΑΜΥΝΤΙΚΟΙ ΜΗΧΑΝΙΜΟΙ
Πλαστογράφηση ταυτότητας	Έλεγχος ταυτότητας Προστασία μυστικών πληροφοριών Αποφυγή δημοσίευσης μυστικών πληροφοριών
Παραβίαση δεδομένων	Εξουσιοδότηση Κατακερματισμός Κωδικοί αναγνώρισης μηνυμάτων Ψηφιακή υπογραφή Πρωτόκολλα ανθεκτικά στις παραβιάσεις
Αποκήρυξη ταυτότητας	Ψηφιακή υπογραφή Ψηφιακή χρονοσφραγίδα Ιστορικό ελέγχου
Δημοσιοποίηση πληροφοριών	Εξουσιοδότηση Πρωτόκολλα βελτιωμένης προστασίας ιδιωτικότητας Κρυπτογράφηση Προστασία μυστικών πληροφοριών Αποφυγή δημοσίευσης μυστικών πληροφοριών
Άρνηση παροχής υπηρεσιών	Έλεγχος ταυτότητας Εξουσιοδότηση Φιλτράρισμα Περιορισμός αριθμού αιτήσεων (Throttling) Ποιότητα υπηρεσίας (Quality of Service – QoS)
Προβιβασμός δικαιωμάτων	Παραχώρηση λιγότερων δικαιωμάτων

Πίνακας 2: Θέματα ασφαλείας στο cloud computing και οι πιθανοί αμυντικοί μηχανισμοί.

3.2 **ΑΝΑΔΥΟΜΕΝΕΣ ΤΑΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΟ** CLOUD COMPUTING

Τα cloud computing περιβάλλοντα είναι περιβάλλοντα πολλαπλών domain, στα οποία ο κάθε domain μπορεί να χρησιμοποιήσει ξεχωριστή ασφάλεια, ιδιωτικότητα, και απαιτήσεις εμπιστοσύνης και ενδεχομένως να χρησιμοποιούνται διάφοροι μηχανισμοί, διασυνδέσεις και σημασιολογία. Ένας τέτοιου είδους domain θα μπορούσε να φιλοξενεί μεμονωμένες ενεργοποιημένες υπηρεσίες καθώς και άλλα στοιχεία υποδομών και υπηρεσιών. Οι αρχιτεκτονικές που είναι βασισμένες στις υπηρεσίες χρησιμοποιούν σχετική τεχνολογία ώστε να διευκολυνθεί αυτός ο multi-domain σχηματισμός, μέσω της σύνθεσης και της ενορχήστρωσης των υπηρεσιών. Κρίσιμης σημασίας είναι η αξιοποίηση της υπάρχουσας έρευνας σχετικά με την ενσωμάτωση της multi-domain πολιτικής και της σύνθεσης ασφαλών υπηρεσιών, για τη δημιουργία ενός ολοκληρωμένου πλαισίου διαχείρισης πολιτικού χαρακτήρα τα περιβάλλοντα της νεφοϋπολογιστικής (Hassan Takabi, 2010). Στο μέρος που ακολουθεί, προσδιορίζουμε κάποια κρίσιμα ζητήματα ασφαλείας και ιδιωτικότητας στο

cloud computing, τα οποία χρήζουν άμεσης προσοχής για την επίτευξη της καθολικής υιοθέτησης αυτής της τεχνολογίας.

Έλεγχος και διαχείριση ταυτότητας: Με τη χρήση των υπηρεσιών cloud, ο χρήστης μπορεί με ευκολία να έχει πρόσβαση στα προσωπικά του δεδομένα και να τα διαθέσει και σε άλλες διάφορες υπηρεσίες στο Internet. Ένας μηχανισμός διαχείρισης ταυτοτήτων (IDM) μπορεί να βοηθήσει στον έλεγχο της ταυτότητας των χρηστών και των εφαρμογών μέσω διαπιστευτηρίων και χαρακτηριστικών. Ένα σημαντικό ζήτημα σχετικά με αυτόν τον μηχανισμό στο νέφος είναι τα μειονεκτήματα της διαλειτουργικότητας, τα οποία μπορεί να προέρχονται από τη χρήση διαφορετικών διακριτικών ταυτοτήτων και πρωτοκόλλων διαπραγμάτευσης ταυτότητας. Ο υπάρχων έλεγχος ταυτότητας, που βασίζεται στους κωδικούς πρόσβασης, έχει περιορισμούς και παρουσιάζει μεγάλους κινδύνους. Ένα IDM σύστημα θα έπρεπε να είναι ικανό να προστατεύει τις προσωπικές και ευαίσθητες πληροφορίες που αφορούν τους χρήστες και τις διαδικασίες. Ωστόσο, τα πολλαπλής-ενοικίασης cloud περιβάλλοντα μπορούν να επηρεάσουν την ιδιωτικότητα των πληροφοριών ταυτότητας, και εκτός αυτού δεν είναι ακόμα πλήρως κατανοητά σε εμάς. Επιπλέον, το θέμα της πολλαπλής δικαιοδοσίας μπορεί να περιπλέξει ακόμα πιο πολύ τα μέτρα προστασίας που θα πρέπει να ληφθούν (Tracey, 2009). Ενώ οι χρήστες αλληλεπιδρούν με μία front-end υπηρεσία, η συγκεκριμένη υπηρεσία είναι πιθανό να χρειαστεί να διασφαλίσει ότι η ταυτότητα των χρηστών της είναι προστατευμένη από τις άλλες υπηρεσίες με τις οποίες αλληλεπιδρά (Ahn G.-J., 2009). Σε περιβάλλοντα πολλαπλής-ενοικίασης καθίσταται αναγκαίο οι πάροχοι να διαχωρίζουν την ταυτότητα του πελάτη και τις πληροφορίες ελέγχου ταυτότητας. Επίσης τα στοιχεία του ελέγχου ταυτότητας και του IDM θα έπρεπε να ενοποιούνται με ευκολία με άλλα στοιχεία ασφαλείας. Ο σχεδιασμός και η ανάπτυξη ισχυρών πρωτοκόλλων ελέγχου και διαχείρισης ταυτότητας αποτελεί καθοριστικής σημασίας απαίτηση για το cloud computing.

Έλεγχος πρόσβασης: Η ετερογένεια και η ποικιλότητα των υπηρεσιών, καθώς και οι διάφορες απαιτήσεις πρόσβασης του domain στη νεφοϋπολογιστική, απαιτούν λεπτομερείς πολιτικές ελέγχου πρόσβασης. Προπαντός, οι υπηρεσίες ελέγχου πρόσβασης θα πρέπει να είναι αρκετά ευέλικτες ώστε να αποτυπώνουν δυναμικές απαιτήσεις πρόσβασης και να επιβάλλουν την αρχή των μειωμένων προνομίων. Τέτοιες υπηρεσίες ελέγχου πρόσβασης ενδέχεται να χρειαστεί να ενσωματώσουν απαιτήσεις προστασίας της ιδιωτικότητας, οι οποίες εκφράζονται μέσα από πολύπλοκους κανόνες. Είναι πολύ σημαντικό το σύστημα ελέγχου πρόσβασης που χρησιμοποιείται από το νέφος να είναι εύκολα διαχειρίσιμο και η κατανομή των προνομίων να γίνεται αποτελεσματικά. Επίσης είναι απαραίτητο να διασφαλιστεί ότι τα μοντέλα υπηρεσιών νέφους παρέχουν διασυνδέσεις γενικού ελέγχου πρόσβασης για την ορθή διαλειτουργικότητα, η οποία απαιτεί προδιαγραφές ελέγχου πρόσβασης ουδέτερης πολιτικής και ένα πλαίσιο επιβολής που μπορεί να χρησιμοποιηθεί για την αντιμετώπιση ζητημάτων πρόσβασης στους domain (Joshi, 2004). Η αξιοποίηση ενός πλαισίου ευαισθητοποιημένου προς την ιδιωτικότητα για τον έλεγχο της πρόσβασης που υπόκειται εύκολα σε ελέγχους συμμόρφωσης, αποτελεί επομένως κρίσιμη απαίτηση, η οποία χρήζει άμεσης προσοχής.

Διαχείριση εμπιστοσύνης και ολοκλήρωση πολιτικής: Παρόλο που πολλοί πάροχοι υπηρεσιών συνυπάρχουν στο νέφος και συνεργάζονται για να παρέχουν ποικίλες υπηρεσίες, μπορεί να έχουν διαφορετικές προσεγγίσεις στο θέμα της ασφαλείας και διαφορετικούς μηχανισμούς προστασίας της ιδιωτικότητας. Ως εκ τούτου, είναι απαραίτητο να αντιμετωπιστεί η ετερογένεια στις πολιτικές τους. Οι πάροχοι υπηρεσιών cloud είναι πιθανόν να χρειαστούν να συνθέσουν πολλαπλές υπηρεσίες, ώστε να καταστήσουν δυνατές

μεγαλύτερες υπηρεσίες εφαρμογών. Έτσι απαιτούνται μηχανισμοί για να διασφαλιστεί ότι μία τέτοια δυναμική συνεργασία αντιμετωπίζεται με ασφάλεια και ότι η κάθε πιθανή παραβίαση ασφαλείας παρακολουθείται στενά και αποτελεσματικά κατά τη διαδικασία της διαλειτουργικότητας. Η μέχρι τώρα εμπειρία έχει δείξει ότι παρόλο που οι επιμέρους domain πολιτικές είναι επαληθευμένες, παραβιάσεις ασφαλείας μπορεί πολύ εύκολα να προκύψουν κατά την διαδικασία της συγχώνευσης (Zhang, 2011). Επομένως, οι πάροχοι υπηρεσιών θα πρέπει να διαχειρίζονται προσεκτικά τις πολιτικές ελέγχου πρόσβασης έτσι ώστε να διασφαλίζουν ότι η συγχώνευση των πολιτικών δεν οδηγεί σε παραβιάσεις της ασφάλειας. Στη νεφοϋπολογιστική, οι αλληλεπιδράσεις μεταξύ διαφορετικών domain υπηρεσιών, που καθοδηγούνται από τις απαιτήσεις των υπηρεσιών, μπορεί να είναι δυναμικές, εφήμερες και εντατικές. Τοιουτοτρόπως, είναι απαραίτητο να αναπτυχθεί ένα πλαίσιο εμπιστοσύνης που θα επιτρέπει την αποτελεσματική καταγραφή ενός γενικού συνόλου παραμέτρων που απαιτούνται για τη δημιουργία εμπιστοσύνης καθώς και για τη διαχείριση εξελισσόμενων απαιτήσεων εμπιστοσύνης και κοινής χρήσεως/αλληλεπιδράσεων (Dongwan Shin, 2005).

Επιπλέον, τα αναπόσπαστα στοιχεία της πολιτικής του cloud θα πρέπει να είναι σε θέση να αντιμετωπίζουν προκλήσεις όπως η σημασιολογική ετερογένεια, η ασφαλής διαλειτουργικότητα και η διαχείριση της εξέλιξης της πολιτικής. Δεδομένου ότι η συμπεριφορά των καταναλωτών εξελίσσεται ραγδαία, υπάρχει μεγάλη ανάγκη για ένα ολοκληρωμένο, ασφαλές και έμπιστο πλαίσιο διαλειτουργικότητας, το οποίο συμβάλλει στη δημιουργία, στη διαπραγμάτευση και στη διατήρηση της εμπιστοσύνης για την ευέλικτη ενσωμάτωση της υποστηρικτικής πολιτικής. Ο σχεδιασμός αποτελεσματικών πλαισίων διαχείρισης εμπιστοσύνης για ασύρματα και peer-to-peer δίκτυα αποτελεί ένα ευρέως διερευνημένο πρόβλημα. Ωστόσο, υπάρχει επείγουσα ανάγκη για ανάπτυξη αξιόπιστων μοντέλων εμπιστοσύνης στα περιβάλλοντα του cloud computing. Αυτό θα είναι ένα ιδιαιτέρως δύσκολο ζήτημα λόγω των διαφόρων θεμάτων διαλειτουργικότητας και της παγκόσμιας ανάπτυξης των μοντέλων υπηρεσιών.

Ασφαλής διαχείριση υπηρεσιών: Στα cloud computing περιβάλλοντα, οι πάροχοι υπηρεσιών νέφους και οι ολοκληρωμένοι πάροχοι υπηρεσιών συνθέτουν υπηρεσίες για τους πελάτες τους. Ο ολοκληρωμένος πάροχος υπηρεσιών παρέχει μία πλατφόρμα η οποία επιτρέπει σε ανεξάρτητους παρόχους υπηρεσιών να συντονίζουν τις υπηρεσίες τους και να παρέχουν συλλογικά πρόσθετες υπηρεσίες, οι οποίες ικανοποιούν τις απαιτήσεις προστασίας των πελατών. Παρόλο που πολλοί πάροχοι υπηρεσιών νέφους χρησιμοποιούν τη Γλώσσα Περιγραφής Υπηρεσιών Διαδικτύου (Web Services Description Language-WSDL), η παραδοσιακή WSDL δε μπορεί να ανταποκριθεί πλήρως στις απαιτήσεις περιγραφής υπηρεσιών στο cloud computing. Στο νέφος, ζητήματα όπως η ποιότητα των υπηρεσιών, η τιμή και τα SLA είναι κρίσιμης σημασίας στην αναζήτηση και τη σύνθεση των υπηρεσιών. Αυτά τα ζητήματα πρέπει να αντιμετωπιστούν για την περιγραφή των υπηρεσιών και την εισαγωγή των χαρακτηριστικών τους, για την εύρεση των καλύτερων διαλειτουργικών επιλογών τους, για την ομαλή ενσωμάτωσή τους, αποφεύγοντας τις παραβιάσεις των πολιτικών του κατόχου της υπηρεσίας, και για την διασφάλιση ικανοποίησης των SLA (Hassan Takabi, 2010). Κατ’ ουσίαν, ένα αυτόματο και συστηματικό πλαίσιο παροχής και σύνθεσης υπηρεσιών που εξετάζει θέματα ασφαλείας και ιδιωτικότητας, είναι ζωτικής σημασίας και χρήζει επείγουσας προσοχής.

Ιδιωτικότητα και προστασία δεδομένων: Η ιδιωτικότητα αποτελεί ένα βασικό ζήτημα σε πολλές προκλήσεις που παρουσιάζονται στη νεφοϋπολογιστική, όπως η ανάγκη προστασίας των πληροφοριών ταυτότητας, τις συνιστώσες της πολιτικής κατά τη διαδικασία την ενσωμάτωσης και τα ιστορικά συναλλαγών. Πολλές επιχειρήσεις δε συμφωνούν με την

αποθήκευση των δεδομένων τους και των υπηρεσιών σε συστήματα που διαμένουν εκτός των εσωτερικών εγκαταστάσεων των κέντρων δεδομένων (Yanpei Chen, 2010). Με την μετακόμιση φόρτου εργασίας σε μία κοινή υποδομή, οι προσωπικές πληροφορίες των πελατών αντιμετωπίζουν αυξημένο κίνδυνο πιθανής μη εξουσιοδοτημένης πρόσβασης και έκθεσης. Οι πάροχοι υπηρεσιών νέφους πρέπει να διαβεβαιώνουν τους πελάτες τους και να τους παρέχουν μεγάλου βαθμού διαφάνεια στις λειτουργίες τους και στη διασφάλιση της ιδιωτικότητας. Οι μηχανισμοί προστασίας της ιδιωτικότητας πρέπει να είναι μέρος όλων των λύσεων που αφορούν την ασφάλεια του νέφους. Σε ένα συναφές πρόβλημα, είναι σημαντικής σημασίας να γνωρίζουμε ποιος δημιούργησε ένα κομμάτι δεδομένων, ποιος το τροποποίησε, πώς και ούτω καθεξής. Οι πληροφορίες προέλευσης θα μπορούσαν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως ο εντοπισμός και ο έλεγχος πρόσβασης βάσει ιστορικού. Η εξισορρόπηση μεταξύ της προέλευσης και της ιδιωτικότητας των δεδομένων αποτελεί σημαντική πρόκληση στο cloud, όπου δεν υπάρχουν φυσικές παράμετροι. Αυτή είναι επίσης μία κρίσιμη ερευνητική πρόκληση.

Οργανωτική διαχείριση ασφαλείας: Τα υπάρχοντα μοντέλα διαχείρισης της ασφάλειας και κύκλου ζωής ασφάλειας πληροφοριών αλλάζουν ριζικά όταν οι επιχειρήσεις αρχίζουν να χρησιμοποιούν το cloud computing. Συγκεκριμένα, οι κοινές προτεραιότητες μπορούν να αποτελέσουν σημαντικό ζήτημα εάν δεν αντιμετωπιστεί σωστά. Παρά τα πιθανά οφέλη της χρήσης του cloud, υπάρχει και το πρόβλημα συντονισμού μεταξύ των διαφορετικών ομάδων ενδιαφερόντων εντός των πελατειακών οργανισμών. Η εξάρτηση από εξωτερικές οντότητες μπορεί επίσης να εγείρει φόβους για την έγκαιρη απόκριση σε συμβάντα ασφαλείας και για την εφαρμογή πλάνων συστηματικής επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών. Επίσης, στα ζητήματα κινδύνου και κόστους-οφέλους θα πρέπει να εμπλακούν και εξωτερικοί φορείς. Συνεπώς, οι πελάτες οφείλουν να εξετάσουν τους νεοεμφανιζόμενους κινδύνους που εισάγονται από ένα περιβάλλον χωρίς παραμέτρους, όπως η διαρροή δεδομένων σε ένα πολλαπλής ενοικίασης περιβάλλον και θέματα όπως η οικονομική αστάθεια του παρόχου και οι τοπικές καταστροφές. Ομοίως, η πιθανότητα εσωτερικής απειλής επεκτείνεται σημαντικά όταν τα δεδομένα και η διεργασίες ανατίθενται σε τρίτους. Μέσα σε ένα περιβάλλον πολλαπλής ενοικίασης, ένας ενοικιαστής μπορεί να είναι στόχος επίθεσης, κάτι που επηρεάζει σε μεγάλο βαθμό και τον άλλον ενοικιαστή. Τα υπάρχοντα μοντέλα κύκλου-ζωής, οι διαδικασίες ανάλυσης και διαχείρισης κινδύνου, οι δοκιμές διείσδυσης και ο έλεγχος ποιότητας της υπηρεσίας πρέπει να επανεξετασθούν για την διασφάλιση των πιθανών πλεονεκτημάτων του νέφους (Hassan Takabi, 2010).

Ο τομέας της ασφάλειας των πληροφοριών έχει αντιμετωπίσει αρκετές δυσκολίες στη θέσπιση καταλλήλων παραμέτρων ασφαλείας για συνεχείς και ρεαλιστικές μετρήσεις που βοηθούν στην αξιολόγηση του κινδύνου. Κρίνεται απαραίτητο να επανεξετάσουμε τις βέλτιστες πρακτικές και να αναπτύξουμε πρότυπα για την εξασφάλιση της ανάπτυξης και της υιοθέτησης ασφαλών clouds. Αυτά τα ζητήματα προϋποθέτουν έναν άρτια δομημένο κλάδο ασφάλισης στον κυβερνοχώρο, αλλά η παγκόσμια φύση της νεφοϋπολογιστικής καθιστά αυτήν την προϋπόθεση εξαιρετικά πολύπλοκη. Παράλληλα με τις προαναφερθείσες τάσεις στο cloud computing, οι τάσεις στον τομέα της γενικής πληροφορικής θα οδηγήσουν επίσης την αλλαγή στις υπηρεσίες του cloud computing και θα προσεγγίσουν μελλοντικές υπηρεσίες, αρχιτεκτονικές και καινοτομίες (Center for the Protection of National Infrastructure, CPNI, 2010). Κάποιες από αυτές τις τάσεις είναι οι εξής:

Αύξηση χρήσεις των κινητών συσκευών: Οι πωλήσεις των φορητών υπολογιστών έχουν ξεπεράσει αυτές των επιτραπέζιων τα τελευταία χρόνια και αυτή η τάση θα συνεχίσει καθώς ένα αυξανόμενο φάσμα κινητών συσκευών, όπως τα notebooks, τα PDAs και τα κινητά

τηλέφωνα ενσωματώνουν στο λογισμικό τους πολλές από τις λειτουργίες που μέχρι μόνο πριν δέκα χρόνια βρίσκαμε αποκλειστικά σε επιτραπέζιους ηλεκτρονικούς υπολογιστές, συμπεριλαμβανομένου της σύνδεσης στο διαδίκτυο και προστατευμένης λειτουργικότητας εφαρμογής.

Βελτιώσεις δυνατοτήτων hardware: Οι αναπόφευκτες βελτιώσεις στην ταχύτητα του επεξεργαστή και οι αυξημένες δυνατότητες της μνήμης κατά μήκος των υποδομών της πληροφορικής που θα συναντήσουμε τα επόμενα χρόνια θα σημάνουν τη δυνατότητα υποστήριξης πιο περίπλοκων περιβαλλόντων με βελτιωμένες δυνατότητες απόδοσης στον χώρο του cloud.

Αντιμετώπιση της πολυπλοκότητας: Παρά τις προσπάθειες πολλών προμηθευτών τεχνολογίας, αυτή η πρόκληση της πολυπλοκότητας δεν έχει επιλυθεί ακόμα. Οι πληροφοριακές αρχιτεκτονικές συνεχίζουν να είναι πολύ δύσκολα εφαρμόσιμες, υποχρησιμοποιούμενες και πολύ ακριβές στην λειτουργία τους. Το τεράστιο μέγεθος του cloud computing ενισχύει την ανάγκη για συστήματα αυτό-παρακολούθησης, αυτό-θεραπείας και αυτόματης διαμόρφωσης, που περιλαμβάνουν ετερογενή συστήματα αποθήκευσης, servers, εφαρμογές, δίκτυα και άλλα στοιχεία του συστήματος.

Ασφάλεια και νομοθεσία: Όταν οι μεγαλύτερες επιχειρήσεις εξετάζουν το ενδεχόμενο χρήσης του νεφοϋπολογιστικού μοντέλου, οι πωλητές και οι προμηθευτές ανταποκρίνονται αλλά με βάσει τους όρους που θέτουν οι εν δυνάμει πελάτες τους. Καθώς υπάρχουν ακόμα πολλά προβλήματα που αφορούν την ιδιωτικότητα των δεδομένων και τη μεταφορά τους διασυνοριακά, οι πάροχοι υπηρεσιών cloud οφείλουν να συνεχίσουν να επενδύουν χρόνο και προσπάθεια προκειμένου να τηρούν τις απαραίτητες νομοθεσίες που απαιτούνται για να λειτουργούν σε ορισμένες από τις περιοχές επαγγελματικής δραστηριότητας των μεγάλων πελατών τους. (Sen, 2013)

ΚΕΦΑΛΑΙΟ 4

4.1 **ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ**

4.1.1 **Στόχοι Έρευνας**

Σκοπός της παρούσας έρευνας είναι να μελετηθεί η χρήση της νεφοϋπολογιστικής στις σύγχρονες επιχειρήσεις. Η έρευνα αφορά ελληνικές επιχειρήσεις στην ευρύτερη περιοχή της Πάτρας και της Αθήνας. Επιπροσθέτως, διερευνάται η άποψη αυτών των επιχειρήσεων πάνω στη χρήση και την ασφάλεια των υπηρεσιών νέφους που έχουν επιλέξει.

4.1.2 **Δείγμα και Υλικό Έρευνας**

Το δείγμα της έρευνας αφορά επιχειρήσεις που βρίσκονται στην πόλη της Αθήνας και της Πάτρας. Επιλέξαμε επιχειρήσεις από διάφορους κλάδους, όπως πληροφορική, ταξίδια και τουρισμός, συμβατικός ηλεκτρισμός, παροχή οικονομικών υπηρεσιών, μηχανήματα βιομηχανικού εξοπλισμού, τρόφιμα, τεχνολογία, είδη προσωπικής φροντίδας, κινητή τηλεφωνία, προσωπικά και οικιακά αγαθά κ.α.

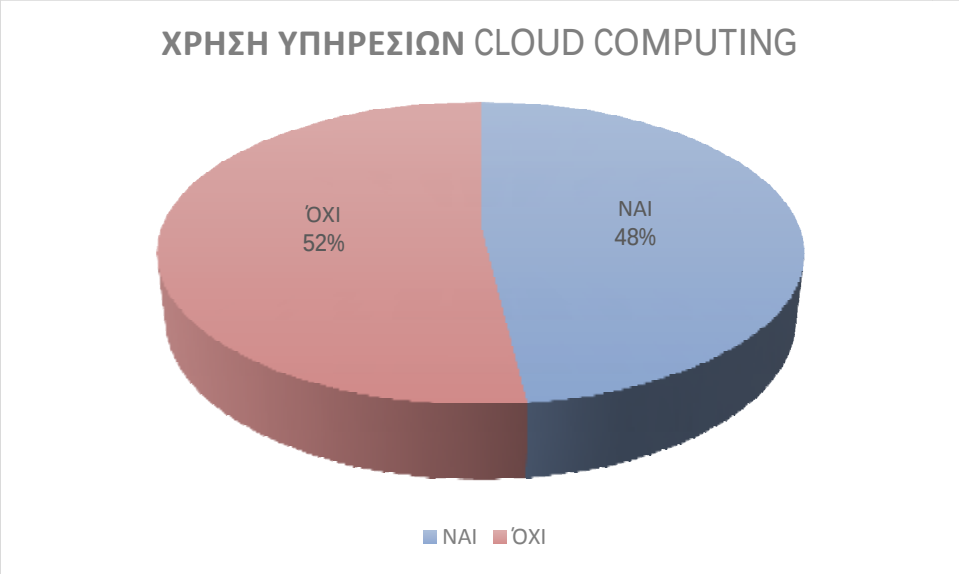
Ως ερευνητικό εργαλείο για την διεξαγωγή της έρευνάς μας επιλέξαμε τη μέθοδο του ερωτηματολογίου. Το ερωτηματολόγιο είναι ένα έντυπο, στην δική μας περίπτωση σε ηλεκτρονική μορφή, το οποίο περιλαμβάνει μία σειρά δομημένων ερωτήσεων και ο κάθε ερωτώμενος απαντά στο ίδιο σύνολο ερωτήσεων, με προκαθορισμένη σειρά. Η επιλογή του ερωτηματολογίου έγινε καθώς είναι ένας οικονομικός τρόπος διεξαγωγής έρευνας και υπάρχει η δυνατότητα αποστολής σε μεγάλο αριθμό ατόμων. Επίσης η χρήση και η δημιουργία του είναι εξαιρετικά εύκολη. Το γεγονός ότι υπάρχει έλλειψη άμεσης επικοινωνίας βοηθά τον ερωτώμενο να εκφραστεί με απόλυτη ελευθερία, χωρίς να έχει τη δυνατότητα ο ερευνητής να επηρεάσει τις απαντήσεις. Τέλος, η διαδικασία δεν είναι καθόλου χρονοβόρα. (Λαγουμντζής, et al., 2015).

Οι ερωτήσεις που επιλέχθηκαν για την δημιουργία αυτού του ερωτηματολογίου καλύπτουν το εύρος της παραπάνω θεωρίας για την χρήση του cloud computing και την ασφάλεια των υπηρεσιών νέφους. Το ερωτηματολόγιο, έχει έκταση δύο σελίδων και αποτελείται από 9 ερωτήσεις κλειστού τύπου, οι οποίες αποτελούν ερωτήματα που χαρακτηρίζονται από ομοιογένεια, σαφήνεια και ακρίβεια ώστε να διευκολύνεται η συμπλήρωση τους από το δείγμα και με αυτό τον τρόπο να εξασφαλιστεί η αξιοπιστία και η εγκυρότητα των στοιχείων. Οι ερωτήσεις του ερωτηματολογίου είναι κλειστού τύπου και αποτελούνται τόσο από πολλαπλής επιλογής όσο και από ερωτήσεις βασιζόμενες στις κλίμακες ιεράρχησης Likert από το 1 έως το 5, όπου το 1 σημαίνει καθόλου ή πολύ κακή και το 5 σημαίνει πάρα πολύ ή άριστη. Στο τέλος της εργασίας, παρατίθεται το ερωτηματολόγιο που χρησιμοποιήθηκε κατά την διενέργεια της έρευνας.

Για την δημιουργία του ερωτηματολογίου μας χρησιμοποιήσαμε την υπηρεσίες της Google «Google Forms», η οποία είναι μέλος των εφαρμογών της «Google Drive». Μετά την ολοκλήρωση της δημιουργίας του, αποστείλαμε το ερωτηματολόγιο σε πάνω από 110 επιχειρήσεις και λάβαμε απάντηση από τις 79, μέσα σε διάστημα δύο μηνών περίπου. Έπειτα, αφού συλλέξαμε όλα τα δεδομένα, τα εισαγάγαμε στο λογισμικό υπολογιστικού φύλλου Microsoft Excel, για τη δημιουργία των διαγραμμάτων που θα αναλύσουμε παρακάτω.

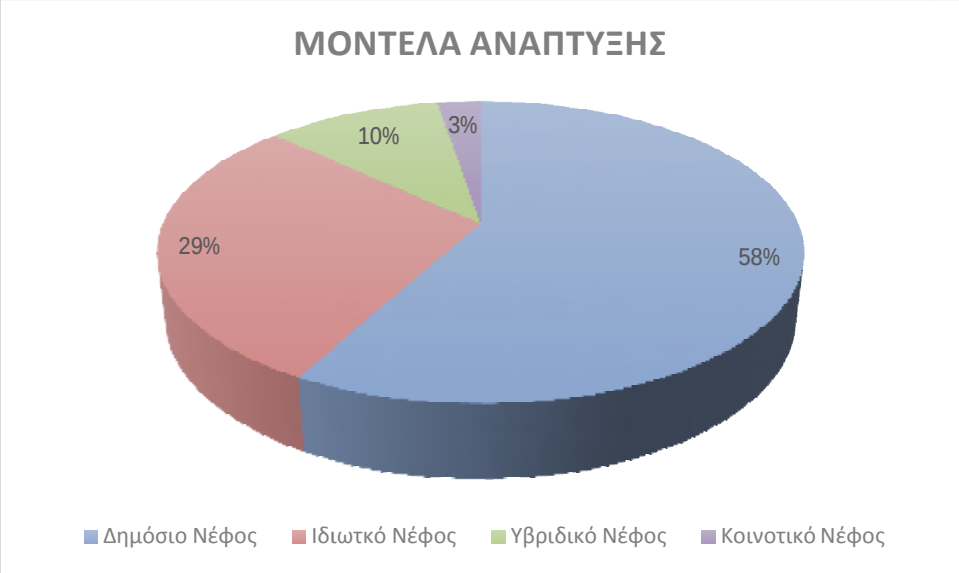
4.2 **ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ**

Το κεφάλαιο αυτό παρουσιάζει την έρευνα που διεξήχθη στο δείγμα των 79 επιχειρήσεων. Γίνεται ανάλυση των στοιχείων που συγκεντρώθηκαν και τα αποτελέσματα παρουσιάζονται σε διαγράμματα.



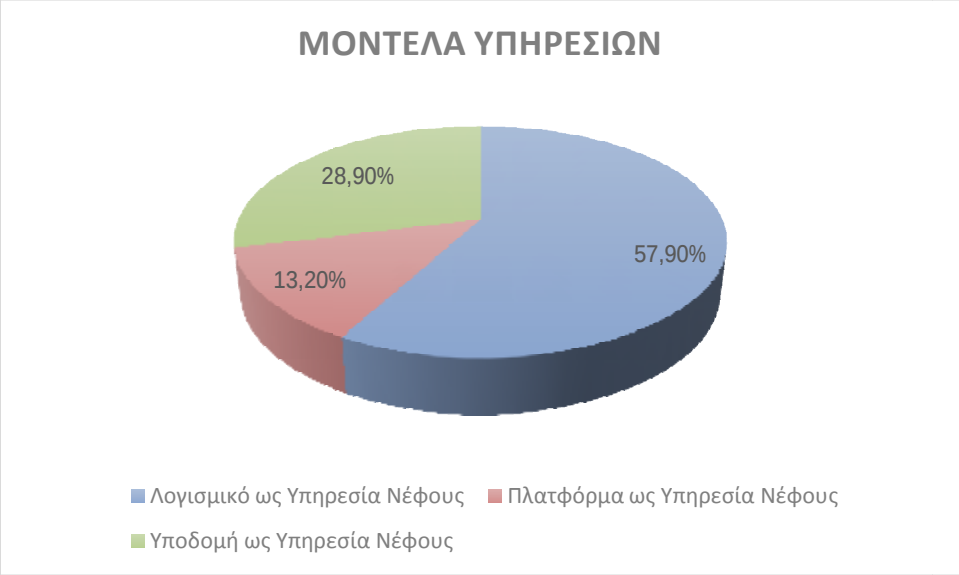
Γράφημα 1: Απαντήσεις στην ερώτηση σχετικά με την χρήση υπηρεσιών cloud computing

Στην ερώτηση «Χρησιμοποιείται υπηρεσίες Cloud Computing;» 38 επιχειρήσεις, δηλαδή το 48%, απάντησε θετικά, ενώ οι υπόλοιπες 41 επιχειρήσεις απάντησαν αρνητικά, ποσοστό που ανέρχεται στο 52%. Οι ερωτηθέντες που απάντησαν όχι αποκλείστηκαν από τις επόμενες ερωτήσεις και συνεπώς πλέον το δείγμα μας διαμορφώνεται στις υπόλοιπες 38 επιχειρήσεις.



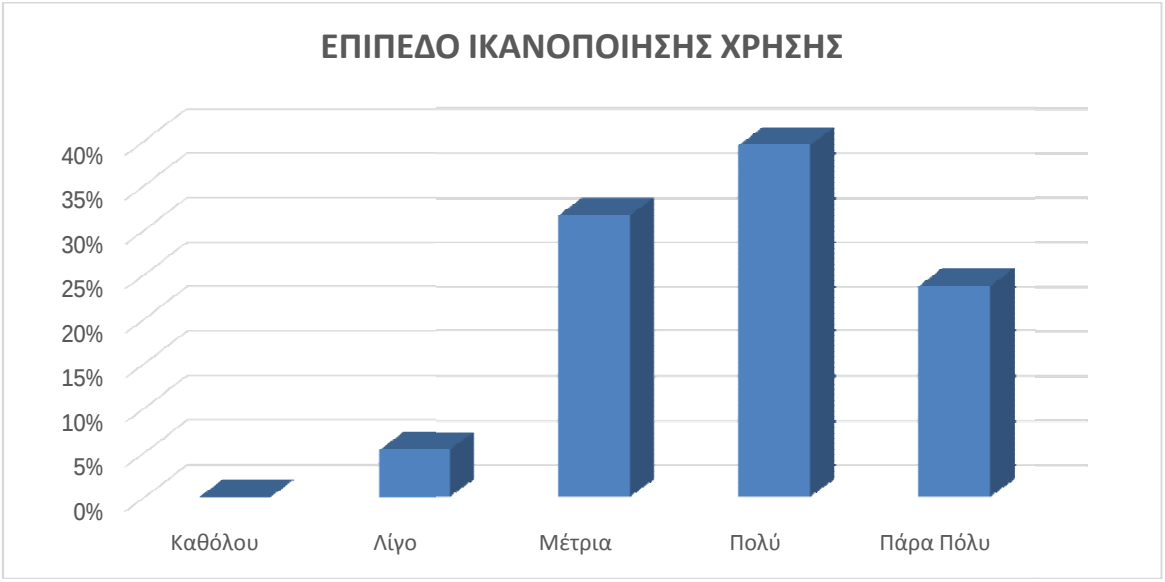
Γράφημα 2: Απαντήσεις σχετικά με τα μοντέλα ανάπτυξης

Στην ερώτηση «Ποιο μοντέλο ανάπτυξης χρησιμοποιείτε;» οι 22 επιχειρήσεις, ποσοστό 58%, απάντησαν πως χρησιμοποιούν το δημόσιο νέφος. Έπειτα, ακολουθεί το ιδιωτικό νέφος με ποσοστό 29%, δηλαδή 11 επιχειρήσεις. Τελευταία έρχονται το υβριδικό και το κοινοτικό νέφος με 10,5% (4 επιχειρήσεις) και 2,6% (1 επιχείρηση) αντίστοιχα.



Γράφημα 3: Απαντήσεις σχετικά με τα μοντέλα υπηρεσιών

Στην ερώτηση «Ποιο μοντέλο υπηρεσιών χρησιμοποιείτε;» η πλειοψηφία των επιχειρήσεων, δηλαδή 22 επιχειρήσεις, απάντησε ότι χρησιμοποιεί το λογισμικό ως υπηρεσία νέφους, με ποσοστό 57,9%. Στη συνέχεια, 11 επιχειρήσεις επέλεξαν την υποδομή ως υπηρεσία νέφους, με ποσοστό 28,9%. Ενώ μόνο 5 επιχειρήσεις, δηλαδή το 13,2%, επέλεξαν την υποδομή ως υπηρεσία νέφους.

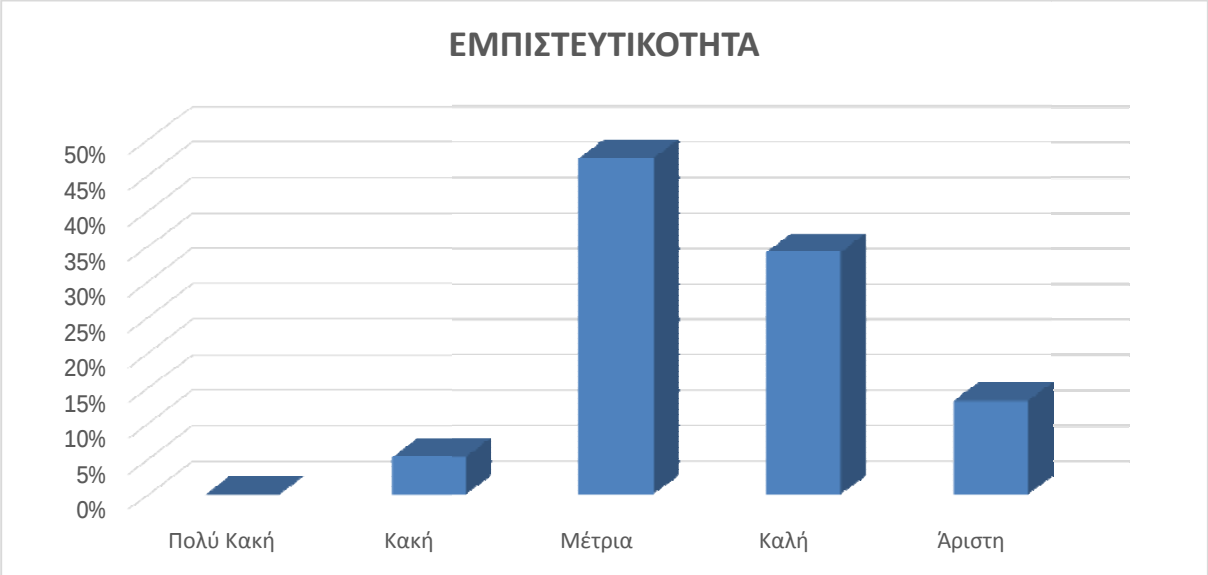


Γράφημα 4: Απαντήσεις σχετικά με το επίπεδο ικανοποίησης των χρηστών

Στην ερώτηση «Πόσο ικανοποιημένοι είστε από τη χρήση υπηρεσιών cloud;» οι 15 επιχειρήσεις απάντησαν πως είναι πολύ ικανοποιημένες, με ποσοστό 39,5%. Αμέσως μετά ακολουθεί η απάντηση «Μέτρια» με ποσοστό 31,6%, δηλαδή 12 επιχειρήσεις. 9 επιχειρήσεις απάντησαν πώς είναι πάρα πολύ ικανοποιημένες, με ποσοστό 23,7%, ενώ μόνο 2 επιχειρήσεις, ποσοστό 5,3%, απάντησαν πως είναι λίγο ικανοποιημένες από τη χρήση των υπηρεσιών cloud.

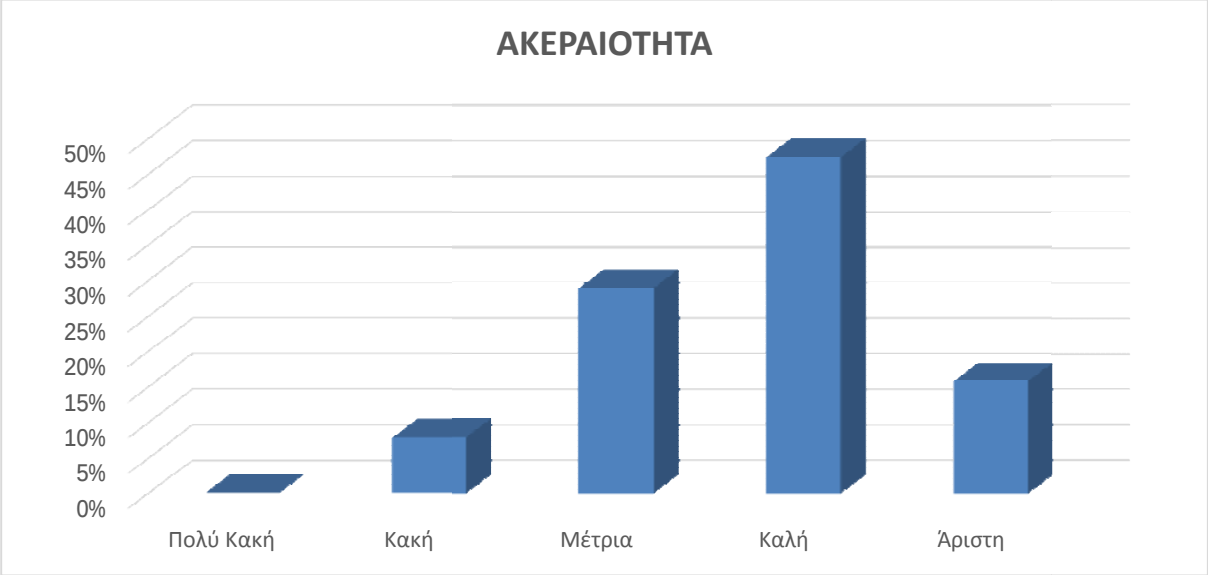
Γράφημα 5: Απαντήσεις σχετικά με το επίπεδο ασφαλείας που αισθάνονται οι χρήστες

Στην ερώτηση «Αισθάνεστε ασφάλεια κατά τη χρήση του Cloud Computing;» οι 21 επιχειρήσεις απάντησαν πως νιώθουν πολύ ασφαλείς κατά τη χρήση της νεφοϋπολογιστικής, ποσοστό που ανέρχεται στο 55,3%. Έπειτα, ακολουθεί η απάντηση «Μέτρια» με ποσοστό 26,3%, δηλαδή 10 επιχειρήσεις. Από 3 επιχειρήσεις επέλεξαν τις απαντήσεις «Λίγο», με ποσοστό 7,9% και «Πάρα Πολύ», ποσοστό επίσης 7,9%. Τέλος, μόνο 1 επιχείρηση, ποσοστό 2,6%, απάντησε πως δεν νιώθει καθόλου ασφάλεια κατά τη χρήση του cloud.



Γράφημα 6: Απαντήσεις σχετικά με το επίπεδο εμπιστευτικότητας των υπηρεσιών Cloud

Στην ερώτηση «Πώς θα βαθμολογούσατε την εμπιστευτικότητα στις υπηρεσίες Cloud;» οι περισσότερες επιχειρήσεις, συγκεκριμένα οι 18 με ποσοστό 47,4% απάντησαν «Μέτρια». Στη συνέχεια, 13 επιχειρήσεις, με ποσοστό 34,2% βαθμολόγησαν την εμπιστευτικότητα που τους παρέχει η υπηρεσία Cloud που χρησιμοποιούν, ως «Καλή». Τέλος, 5 επιχειρήσεις, με ποσοστό 13,2%, βαθμολόγησαν την εμπιστευτικότητα ως «Άριστη» και μόνο 2, με ποσοστό 5,3%, την βαθμολόγησαν ως «Κακή».

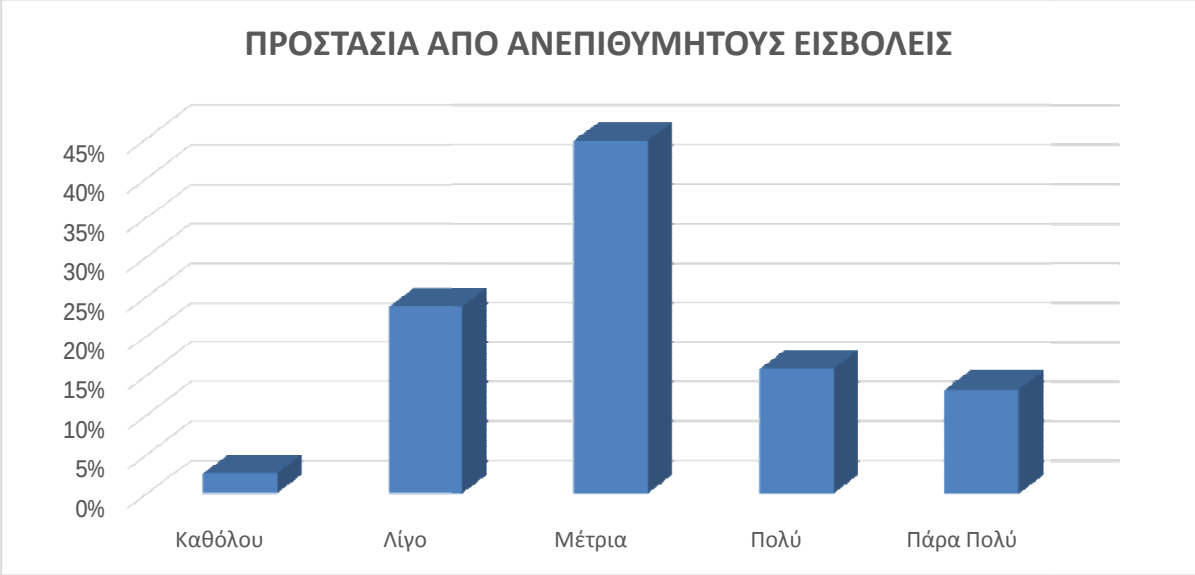


Γράφημα 7: Απαντήσεις σχετικά με την ακεραιότητα των υπηρεσιών Cloud

Στην ερώτηση «Πώς θα βαθμολογούσατε την ακεραιότητα στις υπηρεσίες Cloud;» η πλειοψηφία, δηλαδή 18 επιχειρήσεις με ποσοστό 47,4%, απάντησε «Καλή». Έπειτα, 11 επιχειρήσεις, με ποσοστό 28,9%, απάντησαν «Μέτρια». Τέλος, 6 επιχειρήσεις, με ποσοστό 15,8% χαρακτήρισαν την ακεραιότητα «Άριστη» και 3 επιχειρήσεις, με ποσοστό 7,9% την χαρακτήρισαν «Κακή».

Γράφημα 8: Απαντήσεις σχετικά με την διαθεσιμότητα των υπηρεσιών Cloud

Στην ερώτηση «Πώς θα βαθμολογούσατε την διαθεσιμότητα στις υπηρεσίες Cloud;» οι μισές(19) επιχειρήσεις, με ποσοστό 50%, επέλεξαν την απάντηση «Άριστη». Η αμέσως επόμενη επικρατέστερη απάντηση είναι η επιλογή «Καλή», η οποία επιλέχθηκε από 14 επιχειρήσεις, με ποσοστό 36,8%. Έπειτα ακολουθεί η απάντηση «Μέτρια», που επιλέχθηκε από 4 επιχειρήσεις, με ποσοστό 10,5% και τέλος η επιλογή «Κακή» που μόνο μία επιχείρηση την επέλεξε, με ποσοστό 2,6%.



Γράφημα 9: Απαντήσεις σχετικά με την προστασία των υπηρεσιών Cloud από τους ανεπιθύμητους εισβολείς

Στην τελική ερώτηση «Είναι επαρκής η προστασία από ανεπιθύμητους εισβολείς;» οι 17 επιχειρήσεις επέλεξαν την απάντηση «Μέτρια», ποσοστό που ανέρχεται στο 44,7%. Στη συνέχεια, 9 επιχειρήσεις απάντησαν «Λίγο», με ποσοστό 23,7%. Οι 6 επιχειρήσεις, με ποσοστό 15,8%, επέλεξαν την απάντηση «Πολύ», ενώ 5 επιχειρήσεις, με ποσοστό 13,2%, επέλεξαν την απάντηση «Πάρα Πολύ». Τέλος, μόνο 1 επιχείρηση επέλεξε την απάντηση «Καθόλου», με το μικρό ποσοστό 2,6%.

4.3 **ΑΝΑΛΥΣΗ ΕΥΡΥΜΑΤΩΝ**

Παρά την εξέλιξη που έχει γνωρίσει ο κλάδος του cloud computing στον επιχειρησιακό τομέα, παρατηρούμε ότι με βάση το δείγμα που επιλέγει, το ποσοστό των επιχειρήσεων που χρησιμοποιεί τις υπηρεσίες cloud είναι σχετικά υψηλός.

Όσον αφορά τα μοντέλα ανάπτυξης που χρησιμοποιούν οι ερωτηθέντες, παρατηρείται ότι το δημόσιο νέφος χρησιμοποιείται από περισσότερες από τις μισές επιχειρήσεις. Όπως αναλύθηκε και σε προηγούμενο κεφάλαιο, το δημόσιο νέφος, αποτελεί μια σχετικά οικονομική λύση, η οποία καλύπτει μεν τις ανάγκες των επιχειρήσεων για αποθήκευση, διαχείριση και επεξεργασία δεδομένων, παρόλα αυτά, αποτελεί και το πιο αδύναμο μοντέλο ανάπτυξης.

Οι απαντήσεις σχετικά με το επίπεδο ικανοποίησης από την χρήση των υπηρεσιών cloud, παρουσιάζουν μια γενική ικανοποίηση των ερωτηθέντων, καθώς στην πλειοψηφία τους έδωσαν θετική απάντηση. Το ίδιο επίσης παρατηρείται και στις απαντήσεις σχετικά με την γνώμη των ερωτηθέντων σχετικά με το επίπεδο ασφαλείας των υπηρεσιών cloud. Η πλειοψηφία των ερωτηθέντων απάντησε ότι είναι αρκετά ικανοποιημένοι. Αυτό θα μπορούσε να ερμηνευτεί ποικιλοτρόπως καθώς, αναλογιζόμενοι ότι η πλειοψηφία των ερωτηθέντων χρησιμοποιεί το δημόσιο και κατά συνέπεια πιο ευάλωτο νέφος, προκύπτει το συμπέρασμα ότι είτε δεν είναι πλήρως ενήμεροι σχετικά με τις ιδιότητες ασφαλείας του δημόσιου νέφους, είτε ότι δεν γνωρίζουν σχετικά με τις απειλές στις οποίες τα δεδομένα τους είναι ευάλωτα.

Σχετικά με την εμπιστευτικότητα στις υπηρεσίες cloud, στην πλειοψηφία τους, οι ερωτηθέντες δήλωσαν θετικές απαντήσεις, βαθμολογώντας την εμπιστευτικότητα από μέτρια έως καλή. Όμοια αποτελέσματα προέκυψαν και από τις απαντήσεις σχετικά με την ακεραιότητα των υπηρεσιών cloud, καθώς η πλειοψηφία των ερωτηθέντων την βαθμολόγησαν καλή έως μέτρια. Μόνο στην ερώτηση σχετικά με την διαθεσιμότητα των υπηρεσιών αυτών, οι ερωτηθέντες την χαρακτήρισαν ως επί το πλείστο από άριστη έως καλή.

Στην τελευταία ερώτηση σχετικά με το αν παρέχεται επαρκής προστασία από ανεπιθύμητους εισβολείς, η πλειοψηφία των ερωτηθέντων την χαρακτήρισαν ως μέτρια και λίγο. Εδώ παρατηρείται μια γενική επίγνωση των απειλών που υφίστανται οι χρήστες του cloud από τους ανεπιθύμητους εισβολείς, η οποία όμως έρχεται σε αντίκρουση με τις απαντήσεις τους στην ερώτηση σχετικά με το επίπεδο της ασφάλειας που παρέχεται. Από την μια πλευρά δηλώνουν ικανοποιημένοι από την παρεχόμενη ασφάλεια κατά την χρήση ενώ από την άλλη, δηλώνουν πως η παρεχόμενη προστασία δεν επιφέρει ικανοποίηση.

ΚΕΦΑΛΑΙΟ 5

5.1 **ΣΥΖΗΤΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ**

Το cloud computing είναι ίσως η πιο ενδιαφέρουσα τεχνολογία για τις επιχειρήσεις, και για αυτόν τον λόγο οι επιχειρήσεις ανησυχούν για το επίπεδο ασφαλείας που προσφέρεται στη νεφοϋπολογιστική. Στο μέρος της βιβλιογραφικής επισκόπησης καλύψαμε τις απειλές που συναντάμε σήμερα στη χρήση του cloud computing, καθώς και τις προτάσεις που έχουν γίνει για την αντιμετώπιση αυτών των απειλών. Επίσης, μέσω της έρευνάς μας μπορέσαμε να βγάλουμε κάποια συμπεράσματα για το πώς εκλαμβάνουν οι ελληνικές επιχειρήσεις αυτές τις απειλές.

Με δεδομένα τα αποτελέσματα της έρευνάς μας, όπως παρουσιάστηκαν στο προηγούμενο κεφάλαιο, κρίνεται απαραίτητο πρώτα από όλα να αναφέρουμε, ότι παρόλη τη ραγδαία και καθημερινή εξέλιξη της τεχνολογίας, πολλές επιχειρήσεις δεν έχουν εισάγει τη χρήση της νεφοϋπολογιστικής. Ο φόβος των απειλών, η έλλειψη τεχνολογικής κατάρτισης και το κόστος της συγκεκριμένης τεχνολογίας έχουν καθυστερήσει την εισαγωγή της συγκεκριμένης τεχνολογίας στο καθημερινό εργασιακό περιβάλλον.

Όσον αφορά τα μοντέλα ανάπτυξης του νέφους παρατηρούμε μία σαφή προτίμηση στο δημόσιο νέφος. Το συγκεκριμένο μοντέλο ανάπτυξης είναι το πιο φθηνό, καθώς αποφεύγεται η δημιουργία μίας καινούριας βάσης δεδομένων από τις ίδιες τις επιχειρήσεις, και απλά γίνεται ενοικίαση κάποιας ήδη υπάρχουσας βάσης. Οι επιχειρήσεις έχουν το πλεονέκτημα να πληρώνουν για όσο χώρο χρειάζονται και την ώρα που τον χρειάζονται. Γενικά, είναι πολύ δύσκολο μία μέση επιχείρηση να δημιουργήσει μία βάση δεδομένων τόσο ασφαλή και επαρκής όσο είναι αυτές οι βάσεις που προσφέρουν επιχειρήσεις σαν την Google και την Amazon, τις πιο διάσημες εταιρείες παροχής δημόσιου νέφους.

Το πιο διαδεδομένο μοντέλο υπηρεσιών είναι το λογισμικό ως υπηρεσία νέφους. Το συγκεκριμένο μοντέλο αναμένεται να παραμείνει το πιο δημοφιλές και τα επόμενα χρόνια καθώς η μόνη υποδομή που χρειάζεται για την υιοθέτησή του είναι ευρυζωνική σύνδεση στο διαδίκτυο. Το κόστος είναι μικρό αφού οι επιχειρήσεις αντί να πληρώσουν για άδεια χρήσης πληρώνουν συνδρομή.

Βλέπουμε ότι οι περισσότερες επιχειρήσεις που ενσωμάτωσαν την νεφοϋπολογιστική στην καθημερινότητά τους είναι πολύ ικανοποιημένες από τη χρήση της και νιώθουν αρκετά ασφαλείς. Η χρήση του νέφους διευκολύνει κατά πολύ την διαχείριση των πληροφοριών και παρατηρούμε ότι υπάρχουν πολλές θετικές απόψεις για την ακεραιότητα και τη διαθεσιμότητά του. Ειδικά η διαθεσιμότητα στο νέφος βαθμολογήθηκε με άριστα από την συντριπτική πλειοψηφία, αποτέλεσμα αναμενόμενο καθώς η άμεση προσβασιμότητα είναι ένα από τα μεγαλύτερα πλεονεκτήματα, εάν όχι το μεγαλύτερο, της συγκεκριμένης τεχνολογίας. Όμως, κρίνεται απαραίτητο να τονίσουμε ότι οι περισσότερες επιχειρήσεις εξέφρασαν μία ανησυχία ως προς την εμπιστευτικότητα, βαθμολογώντας την ως μέτρια. Η πολυ-ενοικιαστική φύση του νέφους είναι λογικό να προκαλεί ανασφάλεια στου χρήστες, καθώς ο αυξημένος αριθμός συνεργατών, συσκευών και εφαρμογών που εμπλέκονται, οδηγούν σε έναν μεγαλύτερο αριθμό σημείων πρόσβασης, κάτι που κάνει το νέφος πιο ευάλωτο. Ως μέτρια βαθμολόγησαν και την προστασία από τους ανεπιθύμητους εισβολείς. Ένας από τους μεγαλύτερους φόβους των χρηστών του νέφους είναι οι επιθέσεις από

εισβολείς. Ενώ οι πάροχοι νέφους λαμβάνουν τα απαραίτητα μέτρα για την αντιμετώπιση αυτών των επιθέσεων, πολλές φορές οι εισβολείς καταφέρνουν τον σκοπό τους. Συνεπώς, κρίνεται επιτακτική η ανάγκη να επενδυθεί χρόνος και χρήμα στην περεταίρω ανάπτυξη της ασφάλειας, ώστε ο χρήστης να νιώθει περισσότερη ασφάλεια χρησιμοποιώντας τις υπηρεσίες νέφους.

Η νεφοϋπολογιστική είναι σαφώς ένας από τους πιο δελεαστικούς τομείς στην τεχνολογία την τρέχουσα εποχή και αυτό οφείλεται εν μέρει στην αποδοτικότητα του κόστους και στην ευελιξία της. Ωστόσο, παρά την αύξηση στην δραστηριότητα και το ενδιαφέρον, υπάρχουν σημαντικές ανησυχίες που παρεμποδίζουν την ταχύτητα εξάπλωσης και τελικά ίσως θέσουν σε κίνδυνο τη δυνατότητα του cloud computing να γίνει το επικρατέστερο μοντέλο της πληροφορικής. Παρά τα αδιαμφησβήτητα επιχειρήματα και τεχνικά πλεονεκτήματα του cloud computing, πολλοί εν δυνάμει χρήστες cloud δεν τολμούν να την υιοθέτησή του, και όσες το χρησιμοποιούν είναι στην πλειοψηφία επιχειρήσεις μεγάλου μεγέθους, οι οποίες ως επί το πλείστον τοποθετούν μόνο τα λιγότερο ευαίσθητα δεδομένα τους στο cloud. Η μείωση του κόστους αποθήκευσης και επεξεργασίας δεδομένων αποτελεί υποχρεωτική απαίτηση οποιασδήποτε εταιρείας, ενώ η ανάλυση δεδομένων και πληροφοριών είναι πάντα από τα πιο σημαντικά καθήκοντα σε όλες τις λήψεις αποφάσεων. Συνεπώς, είναι δύσκολο για τις επιχειρήσεις να μεταφέρουν τα δεδομένα τους και τις πληροφορίες τους στο νέφος έως ότου δημιουργηθεί εμπιστοσύνη ανάμεσα στους παρόχους υπηρεσιών νέφους και τους καταναλωτές. Ουσιαστικά, οι δυνατότητες του νέφους ακόμα δεν έχουν αξιοποιηθεί στο έπακρον.

Όταν αναφερόμαστε σε λύσεις για το πρόβλημα της υιοθεσίας της νεφοϋπολογιστικής από τις επιχειρήσεις, είναι σημαντικό να συνειδητοποιήσουμε ότι η πλειοψηφία των θεμάτων στην ουσία είναι παλιά προβλήματα σε ένα νέο περιβάλλον και ίσως πιο έντονα. (Chow , et al., 2009) Όμως, γίνονται σημαντικές προσπάθειες έρευνας πάνω σε τρόπους αποφυγής των προβλημάτων αυτών, καθώς στις περισσότερες περιπτώσεις η βάση για την εύρεση λύσεων υπάρχει ήδη. Για την βελτιστοποίηση της τεχνολογίας, και κατά συνέπεια για την υγιή ανάπτυξη της παγκόσμιας οικονομίας , κρίνεται απαραίτητη η εξομάλυνση των θεμάτων που προκαλούν αυτή την αίσθηση ανασφάλειας στους καταναλωτές.

Το cloud computing χρειάζεται παγκοσμίως τυποποιημένες μεθοδολογίες και τεχνικές λύσεις, για την σωστή αξιολόγηση κινδύνου και θέσπιση επαρκών επιπέδων προστασίας. Κοιτάζοντας από την οπτική γωνία των παρόχων, η ιδιωτικότητα είναι ένας από τους τομείς που θα πρέπει άμεσα να βελτιστοποιήσουν. Για παράδειγμα, η ενσωμάτωση διαλειτουργικών στοιχείων απορρήτου διασφαλίζει την τήρηση αρχών, όπως η ελαχιστοποίηση των δεδομένων σε περιβάλλοντα με σύνθετη αρχιτεκτονική. Τα πρότυπα προστασίας της ιδιωτικότητας θα διαδραματίσουν πολύ σημαντικό ρόλο στην προώθηση της υιοθέτησης των υπηρεσιών του νέφους, προβάλλοντας στοιχεία κοινωνικής ευθύνης και αντιμετωπίζοντας τα φλέγοντα ζητήματα της ιδιωτικότητας.

Ένας άλλος παράγοντας που αναφέραμε ότι συμβάλλει σε αυτό το κλίμα φόβου ως προς αυτήν την τεχνολογία, είναι η ηλεκτρονική εγκληματικότητα, όπως απάτη ή η κακόβουλη παραβίαση των δεδομένων. Οι πάροχοι υπηρεσιών νέφους, έρχονται αντιμέτωποι με πολλαπλές, και πολλές φορές αντίθετες, νομοθεσίες που αφορούν την διαχείριση και αποθήκευση των δεδομένων. Η καλύτερη κατανόηση των ζητημάτων δικαιοδοσίας κρίνεται απαραίτητη, και μπορεί να επιτευχθεί μέσα από την διεξαγωγή εκπαίδευσης και διαλόγου.
Έχοντας υπόψιν όλα τα παραπάνω, δεν πρέπει να αμελούμε το γεγονός ότι στην ουσία, εάν μία επιχείρηση δεν ρισκάρει τίποτα δεν αλλάζει, άρα δεν υπάρχει πρόοδος. Συνεπώς, το

κόστος του ρίσκου πρέπει πάντα να αντισταθμίζεται με τα επικείμενα κέρδη. Στην περίπτωση του cloud computing, το μεγαλύτερο κέρδος που προσφέρεται είναι η καλύτερη λειτουργική αποτελεσματικότητα , η οποία συνεπάγεται χαμηλότερο λειτουργικό κόστος. Επίσης, βελτιώνει την προσαρμοστική ευελιξία της ίδιας της επιχείρησης, αναγκαία για την αντιμετώπιση των αναπόφευκτων αλλαγών της αγοράς.

Άλλωστε, το ρίσκο μειώνεται δραματικά με τον σωστό προγραμματισμό. Καταρχάς, κρίνεται απαραίτητη η διάθεση χρόνου για αναγνώριση των ζητημάτων και έπειτα η αξιολόγηση για το πώς –και αν- η νεφοϋπολογιστική είναι ικανή να λύσει και σε τι βαθμό τα ζητήματα αυτά, με όσο το δυνατόν μικρότερο ρίσκο και κόστος. Όπως προαναφέραμε, η ασφάλεια, για παράδειγμα, είναι πάντα ένας μεγάλος κίνδυνος, αλλά με τις σωστές προσεγγίσεις και τεχνολογίες, το σύστημα που βασίζεται στο νέφος, έχει την δυνατότητα στην πραγματικότητα να είναι πολύ πιο ασφαλές από τα «κλασικά» συστήματα τα οποία βρίσκονται στις εγκαταστάσεις της επιχείρησης. (Linthicum, 2018)

Δυστυχώς, όμως, βλέπουμε ότι πολλές εγχώριες επιχειρήσεις επιλέγουν να μην υιοθετήσουν την τεχνολογία του cloud computing, επηρεασμένες από τον φόβο τους για τα ρίσκα που παρουσιάζονται, χωρίς να θέτουν υπό ενδελεχή έλεγχο το γεγονός ότι το κέρδος ξεπερνά κατά πολύ τα μειονεκτήματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ahn G.-J., K. M. S. M., 2009. *Privacy-Enhanced User-Centric Identity Management.* Dresden, Germany, IEEE.

Allen, A., 1999. *Coercing Privacy.* s.l.:William & Mary Law Review.

Angeles, S., 2013. *Business News Daily.* [Ηλεκτρονικό] Available at: https://www.businessnewsdaily.com/5215-dangers-cloud-computing.html

Anon., 2003. *AMD.* [Ηλεκτρονικό] Available at: http://www.amd.com/usen/Corporate/VirtualPressRoom/0,,51_104_543_10218~74465,00.html

Anon., 2016. *InternetDict.com.* [Ηλεκτρονικό] Available at: http://www.internetdict.com/el/answers/what-is-sla.html

Anon., n.d. *CITED.gr I.T and Education Services.* [Ηλεκτρονικό] Available at: https://cited.gr/infrastructure-as-a-service-iaas/

Anon., n.d. *Guru99.* [Ηλεκτρονικό] Available at: https://www.guru99.com/cloud-computing-for-beginners.html

Anon., n.d. *Official Site | Norton™ - Antivirus & Cybersecurity Software.* [Ηλεκτρονικό] Available at: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Avatier, 2018. *Avatier.* [Ηλεκτρονικό] Available at: https://www.avatier.com/blog/7-fatal-cloud-computing-security-mistakes-bankers-need-to-know-about/

Badger, L., Grance, T., Patt-Corner, R. & Voas, J., 2011. *Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce.,* s.l.: s.n.

Behl, A., 2011. Emerging Security Challenges in Cloud Computing: An Insight to Cloud Security Challenges and their mitigations. Στο: *Proceedings of the World Congress on Information and Communication Technologies (WITC '11).* s.l.:s.n., pp. 217-222.

Bowers, K., Juels, A. & Oprea, A., 2009. Proofs of retrievability: theory and implementation. Στο: *Proceddings of the ACM Workshop on Cloud Computing Security (CCSW'09).* s.l.:s.n., pp. 43-53.

Brodkin, J., 2008. *Loss of customer data spurs closure of 'The Linkup'.* [Ηλεκτρονικό] Available at: https://www.computerworld.com.au/article/256610/loss_customer_data_spurs_closure_linkup_/

Catteddu, D., 2010. Cloud Computing: benefits, risks and recommendations for information security. Στο: *Web Application Security.* Berlin, Heidelberg: Springer, pp. 17-17).

Center for the Protection of National Infrastructure, CPNI, 2010. *INFORMATION SECURITY BRIEFING 01/2010 ON CLOUD COMPUTING,* s.l.: s.n.

CERT, 2011. *2011 CyberSecurity Watch Survey.* [Ηλεκτρονικό] Available at: https://resources.sei.cmu.edu/asset_files/Presentation/2011_017_001_54029.pdf [Πρόσβαση 10 03 2018].

Chen, D. & Zhao, H., 2012. Data Security and Privacy Protection issues in Cloud Computing. Στο: *Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE'12).* Hangzhou: s.n., pp. 647-151.

Chou, T. S., 2013. Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, 5(3), p. 79.
Chow , R. και συν., 2009. *Controling Data in the Cloud: Outsourcing Computation without Outsourcing Control.* New York, ACM New York, pp. 85-90.
Cohen, J., 2013. *What Privacy Is For.* s.l.:Harvard Law Review.
Digital Trends Staff, 2009. *EPIC Complains to the FTC About Google Cloud.* [Ηλεκτρονικό] Available at: https://www.digitaltrends.com/web/epic-complains-to-the-ftc-about-google-cloud/
Dongwan Shin, G.-J. A., 2005. Role-based Privilege and Trust Management. *Computer Systems Science and Engineering*, Νοέμβριος, 20(6), pp. 401-410.
Federal Trade Commission, 2010. *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* s.l.: s.n.
Feldman, A., Zeller, W., Freedman, M. & Felden, E., 2010. SPORC: group collaboration using untrusted cloud resources. Στο: *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implenentation (OSDI '10).* s.l.:s.n., pp. 337-350.
Griffith, E., 2016. *PCMag.com.* [Ηλεκτρονικό] Available at: http://www.pcmag.com/article2/0,2817,2372163,00.asp
Gurpreet, . K. & Manish, . M., 2013. *Analyzing Data Security for cloud computing using cryptographic Algorithms.,* s.l.: s.n.
Hassan Takabi, J. B. D. J. G. J. A., 2010. Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security and Privacy*, Νοέμβριος, 8(6), pp. 24-31.
Hassan Takabi, J. B. J. G.-J. A., 2010. *Security and Privacy Challenges in Cloud Computing Environments.* [Ηλεκτρονικό] Available at: https://www.cs.ru.nl/~jhh/pub/secsem/takabi2012security-privacy-cloud-challenges.pdf
Hietala, J., 2008. *Don't cloud your vision.* [Ηλεκτρονικό] Available at: https://www.ft.com/content/303680a6-bf51-11dd-ae63-0000779fd18c
Hogan, M. & Shepherd, T., 2015. Information Ownership and Materiality in an Age of Big Data Surveillance. Στο: *Journal of Information Policy.* s.l.:Pen State University Press, pp. 6-31.

Hurwitz, J., Bloor, R. & Kaufman, M., 2012. *How to Design a Cloud Computing Strategy.* [Ηλεκτρονικό]
Available at: http://www.dummies.com/programming/networking/how-to-design-a-cloud-computing-strategy/
[Πρόσβαση 10 3 2018].
Johnston, S., n.d. *Wikipedia.* [Ηλεκτρονικό] Available at: https://en.wikipedia.org/wiki/Cloud_computing
Joshi, J., 2004. *Access-Control Language for Multidomain Environments.* s.l.:IEEE.
Konstantinou, A. και συν., 2009. An Architecture for Virtual Solution Composition and Deployment in Infrastructure Clouds. Στο: *Proceedings of the 3rd International Workshop on Virtualization Technologies in Distributed Computing (VTDC '09).* s.l.:s.n., pp. 9-18.
Linthicum, D., 2018. *InfoWorld.* [Ηλεκτρονικό] Available at: https://www.infoworld.com/article/3299296/the-biggest-risk-in-cloud-computing-is-not-doing-it.html
Lo, H., Wang, R. & Garbini, J. P., 2009. The state of enterprise software. *Forrester Research.*
Mearian, L., 2009. *Latest cloud storage hiccups prompts data security questions.* [Ηλεκτρονικό]

Available at: http://www.computerworld.com/article/2523339/cloud-computing/latest-cloud-storage-hiccups-prompts-data-security-questions.html
Mitchell, C., 2005. *Trusted Computing.* s.l.:IET.
Pandith, M. Y., 2014. Data Security and Privacy Concerns in Cloud Computing. *Internet of Things and Cloud Computing,* Τόμος II, pp. 6-11.
Paterson, N., 2014. End User Privacy and Policy-Based Networking. Στο: *Journal of Information Policy.* s.l.:s.n., pp. 28-43.
Pearson, S., 2009. Taking Account of Privacy when Designing Cloud Computing Services . Στο: *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing.* s.l.:s.n., pp. 44-52.
Ramokapane, K. M., Rashid, A. & Such, J. M., n.d. Assured Deletion in the Cloud: Requirements, Challenges.
Ranchal, R., Bhargava, B. & Othmane, L., 2010. Protection of Identity Infrmation in Cloud Computing without Trusted Third Party. Στο: *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS'10).* s.l.:s.n., pp. 368-372.
Rastogi, N., Gloria, M. J. K. & Hendler, J., 2015. Security and Privacy of Performing Data Analytics in the Cloud: A Three-way Handshake nof Technology, Policy and Management. Στο: *Journal of Information Policy.* s.l.:Penn State University Press, pp. 129-154.
Report, I.-T. T. W., 2012. *Privacy in Cloud Computing,* s.l.: ITU.
Richardson, F., n.d. *GNews Entertainment.* [Ηλεκτρονικό] Available at: https://gwcaia.com/cloud-computing/banks-are-responsible-for-confidentiality-of-information-when-using-the-cloud
Rouse, M., 2014. *Trusted Platform Module (TPM),* s.l.: s.n.
SAS 70, n.d. *SAS 70 Service Organization Auditing Standards, Public Accounting Information.* [Ηλεκτρονικό] Available at: http://sas70.com/
Sen, J., 2013. Security and privacy issues in cloud computing. *Architectures and protocols for secure information technology infrastructures,* pp. 1-45.
Sen, J., 2013. Security and Privacy Issues in Cloud Computing. Στο: *Architectures and Protocols for Secure Information Technology Infrastructures.* Kolkata: s.n., pp. 1-45.
Shukla, P. & Dixit, M., 2015. *Big Data: An Emerging Field of Data Engineering,* s.l.: s.n.
Squicciarini, A., Sundareswaran, S. & Lin, D., 2010. Preventing Information Leakagefrom Indexing in the Cloud. Στο: *Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD'10).* s.l.:s.n., pp. 188-195.
Stephen Biggs, S. V., 2009. *Cloud Computing: The impact on digital forensic investigations.* London, UK: IEEE.
Sun, D., Chang, G., Sun, L. & Wang, X., 2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. Στο: *Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS '11).* s.l.:s.n., pp. 2852-2856.
Sun, Y., Zhang, J., Xiong, Y. & Zhu, G., 2014. *Data Security and Privacy in Cloud Computing,* Beijing: s.n.
Tracey, P. B. &. B., 2009. *Cloud Computing: Privacy, Security Challenges. Bureau of National Affers.* s.l.:s.n.
Viswav, P., 2017. *MSPoweruser.* [Ηλεκτρονικό] Available at: https://mspoweruser.com/microsoft-azure-finally-catches-amazon-availability-zones/
Wang, S., Yan, K., Wang, S. & Huang, C., 2009. Achieving High Efficient Agreement with Malicious Faulty Nodes on a Cloud Computing Environment. Στο: *Proceedings of the 2nd*

International Conference on Interaction Sciences: Information Technology, Culture and Human (ICIS '09). s.l.:s.n., pp. 468-473.
Ward, M., 2009. *Facebook Users Suffer Viral Surge.* [Ηλεκτρονικό] Available at: http://news.bbc.co.uk/2/hi/technology/7918839.stm
Yanpei Chen, V. P. R. H. K., 2010. *What's New About Cloud Computing Security?*, s.l.: s.n.
Zhang, Y., 2011. *An Access Control and Trust Management Framework for Loosely-Coupled Multidomain Environment.* s.l.:(Unpublished).
Zissis, D. & Lekkas, D., 2010. Addressing Cloud Computing Security Issues. Στο: *Future Generation Computer Systems.* Syros: s.n., pp. 583-592.
Γκιούρδας, 2001. Στο: *Χάκερ Επίθεση και Άμυνα.* s.l.:s.n., p. 555.
Λαγουμντζής, Γ., Βλαχόπουλος, Γ. & Κουτσογιάννης, Κ., 2015. *Μεθοδολογία της Έρευνας στις Επιστήμες Υγείας*. s.l.:Εκδόσεις Κάλλιπος.

Μουρίκη, Μ. Ε., 2014. *DSpace HEAL*. [Ηλεκτρονικό] Available at: http://dspace.lib.ntua.gr/dspace2/bitstream/handle/123456789/39901/mourikie_apis.pdf?sequence=1
Ομάδα Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων , 2014. *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης*, s.l.: s.n.

ΠΑΡΑΡΤΗΜΑ Α

Παρουσιάζεται το ερωτηματολόγιο που χρησιμοποιήθηκε για την συλλογή των πρωτογενών δεδομένων της παρούσας εργασίας.

Προστασία και Ασφάλεια στο Cloud

Το παρόν ερωτηματολόγιο δημιουργήθηκε με σκοπό τη συλλογή δεδομένων για την πτυχιακή εργασία με θέμα "Προστασία και Ασφάλεια στο Cloud". Σκοπός μας είναι η διεξαγωγή μίας έγκυρης έρευνας πάνω στον τύπο νέφους που επιλέγουν οι ελληνικές επιχειρήσεις, καθώς και η συλλογή στοιχειών για τη χρήση και την ασφάλεια των υπηρεσιών νέφους που επιλέγονται. Η συμπλήρωση είναι γρήγορη και γίνεται ανώνυμα.

Ευχαριστούμε πολύ για τον χρόνο σας.

Γαλιατσάτου Μαργαρίτα
Μηλιώνη Δήμητρα
(Τμήμα Διοίκησης Επιχειρήσεων Πάτρας - Τ.Ε.Ι. Δυτικής Ελλάδας)

ΓΛΩΣΣΑΡΙ

Cloud computing = σύνολο online υπηρεσιών διάθεσης υπολογιστικών πόρων, όπως αποθηκευτικοί χώροι, δίκτυα, applications.

Δημόσιο Νέφος (Public Cloud) = υπηρεσία διαθέσιμη για το κοινό, όπου οι πόροι παρέχονται στους χρήστες μέσω του Internet και οι υπηρεσίες είναι είτε δωρεάν, είτε επί πληρωμή, ανάλογα με τις δυνατότητες που προσφέρονται.

Ιδιωτικό Νέφος (Private Cloud) = ανήκει σε μία εταιρεία, συνίσταται από πολλαπλούς καταναλωτές και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων. Αποτελείται από το δίκτυο, τον hardware διακομιστή, αποθηκευτικό χώρο και τα εργαλεία διαχείρισης. Συνήθως διοικείται εσωτερικά, αλλά μπορεί επίσης να «φιλοξενηθεί» και εξωτερικά από Παρόχους Διαχειριζόμενων Υπηρεσιών (MSP).

Υβριδικό Νέφος (Hybrid Cloud) = υπηρεσία η οποία συνδυάζει τα πλεονεκτήματα του δημόσιου και ιδιωτικού νέφους.

Κοινοτικό Νέφος (Community Cloud) = παρέχεται για αποκλειστική χρήση σε κάποια συγκεκριμένη κοινότητα πελατών από οργανώσεις που έχουν κοινές ανησυχίες (π.χ. αποστολή, ανάγκες ασφαλείας, πολιτική, και παραμέτρους συμμόρφωσης).

Λογισμικό ως Υπηρεσία Νέφους (Applications/Software as a Service – SaaS) = εφαρμογές που προσφέρονται δωρεάν ή με συνδρομή και είναι προσβάσιμες από οποιονδήποτε ηλεκτρονικό υπολογιστή συνδεδεμένο στο διαδίκτυο, π.χ. Dropbox, Microsoft Office 365.

Πλατφόρμα ως Υπηρεσία Νέφους (Platform as a Service – PaaS) = προσφέρει εργαλεία και περιβάλλον στους χρήστες για να δημιουργήσουν εφαρμογές cloud, π.χ. Python Anywhere, Google App Engine.

Υποδομή ως Υπηρεσία Νέφους (Infrastructure as a Service – IaaS) = επιτρέπει στους χρήστες να τρέξουν οποιαδήποτε ήδη υπάρχουσα εφαρμογή στο hardware του παρόχου του cloud. Ο πελάτης δεν διαχειρίζεται ούτε ελέγχει τις υποκείμενες υποδομές του νέφους, αλλά έχει τον έλεγχο του λειτουργικού συστήματος, της αποθήκευσης και των ανεπτυγμένων εφαρμογών, π.χ. Google Compute Engine (GCE), Amazon Web Services (AWS).

* Απαιτείται

Χρησιμοποιείτε υπηρεσίες Cloud Computing; *

- ○ Ναι
- ○ Όχι

Ποιο μοντέλο ανάπτυξης cloud χρησιμοποιείτε; *

- ○ Δημόσιο Νέφος (Public Cloud)
- ○ Ιδιωτικό Νέφος (Private Cloud)
- ○ Υβριδικό Νέφος (Hybrid Cloud)
- ○ Κοινοτικό Νέφος (Community Cloud)

Ποιο μοντέλο υπηρεσιών cloud computing χρησιμοποιείτε; *

- ○ Λογισμικό ως Υπηρεσία Νέφους (Applications/Software as a Service – SaaS)
- ○ Πλατφόρμα ως Υπηρεσία Νέφους (Platform as a Service – PaaS)
- ○ Υποδομή ως Υπηρεσία Νέφους (Infrastructure as a Service – IaaS)

Πόσο ικανοποιημένοι είστε από την χρήση υπηρεσιών cloud ; *

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα Πολύ

Αισθάνεστε ασφάλεια κατά τη χρήση του Cloud; *

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα Πολύ

Πώς θα βαθμολογούσατε την εμπιστευτικότητα στις υπηρεσίες Cloud; *

	1	2	3	4	5	
Πολύ Κακή	○	○	○	○	○	Άριστη

Πώς θα βαθμολογούσατε την ακεραιότητα στις υπηρεσίες Cloud; *

	1	2	3	4	5	
Πολύ Κακή	○	○	○	○	○	Άριστη

Πώς θα βαθμολογούσατε τη διαθεσιμότητα στις υπηρεσίες Cloud; *

	1	2	3	4	5	
Πολύ Κακή	○	○	○	○	○	Άριστη

Είναι επαρκής η προστασία από ανεπιθύμητους εισβολείς; *

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα Πολύ