Αντωνιος Σιτοκωνσταντινου – MTE1929

Ασφάλεια σε περιβάλλον νέφους

Περίληψη

Το υπολογιστικό νέφος (Cloud Computing – CC) αποτελεί ένα σύγχρονο μοντέλο δυναμικής παροχής υπολογιστικών πόρων προς τους τελικούς χρήστες. Οι υπολογιστικοί πόροι στην περίπτωση του CC φιλοξενούνται σε συστήματα μεγάλης κλίμακας που διέπονται από το καθεστώς της πολυμίσθωσης (multitenancy) λογισμικού και υπηρεσιών. Η παροχή των συγκεκριμένων πόρων προς τους πελάτες γίνεται κατόπιν αιτήματός τους, στοιχείο που θεωρείται οικονομικά αποδοτικό. Η συνολική φιλοσοφία λειτουργίας τους CC έχει μεταμορφώσει τον τρόπο δημιουργίας και παροχής των λύσεων στον τομέα της πληροφορικής.

Το βασικό κίνητρο, επομένως, στη χρήση του μοντέλου CC είναι η οικονομική αποδοτικότητά του, ένα κίνητρο που έχει οδηγήσει στη μεταφόρτωση κρίσιμων δεδομένων και υποδομών μεγάλου μέρους των οργανισμών Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) σε περιβάλλοντα cloud. Λόγω όμως της πολύπλοκης φύσης της υποκείμενης υποδομής του, το περιβάλλον ενός cloud έρχεται αντιμέτωπο με ένα μεγάλο αριθμό προκλήσεων, όπως οι κυβερνοεπιθέσεις, η έγχυση κακόβουλου λογισμικού κλπ., που αποτελούν σοβαρή απειλή για τα δεδομένα που φιλοξενούνται σε αυτό αλλά ακόμα και για την ίδια του την ύπαρξη. Η ύπαρξη τέτοιου είδους απειλών μπορούν να ελαχιστοποιήσουν την προσβασιμότητα σε ένα cloud, αλλά και να έχουν αισθητή αρνητική επίπτωση ως προς τη γενική εμπιστοσύνη και αξιοπιστία των πελατών προς την τεχνολογία.

Από τα παραπάνω προκύπτει το εύλογο συμπέρασμα ότι η ασφάλεια αποτελεί το κύριο μέλημα ενός μοντέλου υπηρεσίας cloud. Ωστόσο, οι μέχρι τώρα επιστημονικές μελέτες έχουν αποδείξει ότι τα περιβάλλοντα των cloud δεν είναι τόσο ασφαλή όσο θα περίμενε κανείς. Έχει επίσης διαπιστωθεί μια περιορισμένη κατανόηση σχετικά με την προσφορά ασφαλών cloud υπηρεσιών που να μπορούν να αντιμετωπίσουν τις προκλήσεις που αναφέρθηκαν παραπάνω. Κάτι τέτοιο αποδεικνύει τη σημασία της δυνατότητας εύρεσης όλων των εν δυνάμει απειλών κατά της ασφάλειας του cloud, αλλά και της προσπάθειας εύρεσης όλων των πιθανών λύσεων και τρόπων αντιμετώπισής τους.

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση των ζητημάτων ασφαλείας στον τομέα του CC, εστιάζοντας στην ταξινόμηση τους αλλά και στην ταξινόμηση των πιθανών λύσεων που έχουν παρουσιαστεί μέχρι τώρα στη βιβλιογραφία. Για το σκοπό αυτό, η παρούσα εργασία αποτελείται από πέντε κεφάλαια. Στο πρώτο, εισαγωγικό, κεφάλαιο αναπτύσσεται σε γενικές γραμμές το θεωρητικό υπόβαθρο σχετικά με το CC και την ασφάλειά του, καθώς και η οργάνωση και συμβολή της παρούσας εργασίας. Το δεύτερο κεφάλαιο ασχολείται με μια γενική περιγραφή της έννοιας του CC. Στο τρίτο κεφάλαιο αναπτύσσεται μια βιβλιογραφική ανασκόπηση των θεμάτων ασφάλειας που αντιμετωπίζει το cloud, ενώ το τέταρτο κεφάλαιο περιλαμβάνει πιθανούς τρόπους αντιμετώπισης των ζητημάτων ασφάλειάς του που έχουν προταθεί στη βιβλιογραφία. Στο πέμπτο κεφάλαιο περιγράφεται μια μελέτη περίπτωσης της ασφάλειας των συστημάτων υγείας που λειτουργούν σε περιβάλλον cloud. Η εργασία ολοκληρώνεται

με κάποια συμπεράσματα που προκύπτουν από την ανάλυση όλων των παραπάνω θεμάτων.

Λέξεις κλειδιά: Ασφάλεια, προκλήσεις, τρόποι αντιμετώπισης, Cloud Computing.

Περιεχόμενα

1 Εισαγωγή

1.1 Θεωρητικό υπόβαθρο

Στα παραδοσιακά υπολογιστικά μοντέλα, τα δεδομένα αποτελούν πολύτιμο πόρο. Η σωστή διαχείρισή τους αποτελεί μια πολύ σημαντική διαδικασία που στοχεύει στη διασφάλιση της ακεραιότητάς τους. Για δεκαετίες, η αποθήκευση των δεδομένων γινόταν με χρήση πολλών ειδών hardware υλικού, όπως σκληρούς δίσκους, DVD, CD, κλπ. Η εισαγωγή των συστημάτων βάσεων δεδομένων βελτίωσε τη διαχείριση των πληροφοριών, καθιστώντας την πιο αποτελεσματική [1]. Πρόσφατα, η επεξεργασία πληροφοριών μπορούσε να πραγματοποιηθεί ακόμα πιο αποτελεσματικά σε πλατφόρμες μεγάλης υπολογιστικής ισχύος και μεγάλου χώρου αποθήκευσης δεδομένων, οι οποίες είναι προσβάσιμες μέσω του Διαδικτύου [2]. Όλες αυτές οι εξελίξεις στα συστήματα βάσεων δεδομένων και στον τομέα των δικτύων, συμπεριλαμβανομένου του Διαδικτύου, επέτρεψαν την ανάπτυξη νέων υπολογιστικών μοντέλων. Τέτοια μοντέλα αφορούν την ανάπτυξη του grid computing, στις αρχές της δεκαετίας του 1990, καθώς και του utility computing και cloud computing, στα μέσα της δεκαετίας του 2000 [1].

Το Cloud Computing (CC) μπορεί να οριστεί ως ένα υπολογιστικό μοντέλο που επιτρέπει εύκολη και κατόπιν απαίτησης του χρήστη (on-demand) δικτυακή πρόσβαση σε κοινόχρηστο σύνολο διαμορφώσιμων υπολογιστικών πόρων, που μπορούν να παρασχεθούν γρήγορα με ελάχιστες προσπάθειες διαχείρισης ή αλληλεπιδράσεις παρόχων υπηρεσιών [3]. Το μοντέλο του CC περιλαμβάνει την παροχή και χρήση υποδομών πληροφορικής, πλατφορμών και εφαρμογών οποιουδήποτε είδους με τη μορφή υπηρεσιών που διατίθενται στο Διαδίκτυο [4]. Μερικές από ένα μεγάλο πλήθος εφαρμογών που χρησιμοποιούν υπηρεσίες cloud, αποτελούν η διαδικτυακή αποθήκευση αρχείων, οι ιστοσελίδες κοινωνικής δικτύωσης, το webmail και οι διαδικτυακές επιχειρηματικές εφαρμογές [2].

Καθώς οι επιχειρήσεις σε παγκόσμιο επίπεδο προσπαθούν να εντοπίσουν νέες μεθόδους προώθησής τους, το μεγαλύτερο βάρος αυτής της προσπάθειας έχει μετατοπιστεί σε λύσεις χαμηλότερου κόστους, όσον αφορά τη χρήση υπολογιστικών συστημάτων. Το κόστος αυτό αφορά την πρόσβαση σε υπολογιστικές υποδομές αλλά και το λειτουργικό κόστος. Αυτό είχε ως αποτέλεσμα την εκθετική ανάπτυξη του μοντέλου του CC, το οποίο θεωρείται αποτελεσματικότερο στην επίτευξη αυτών των στόχων σε σύγκριση με προηγούμενες λύσεις [4].

Η εικονικοποίηση (virtualization) αποτελεί μία από τις βασικές τεχνολογίες του μοντέλου CC και χρησιμοποιείται για τη συσσώρευση πολλαπλών αυτόνομων συστημάτων σε μία πλατφόρμα hardware υλικού. Η συγκεκριμένη τεχνολογία αποσκοπεί στην αφαίρεση του hardware υλικού, αποκρύπτοντας την πολυπλοκότητα της διαχείρισης της φυσικής υπολογιστικής πλατφόρμας, με αποτέλεσμα την απλοποίηση της επεκτασιμότητας των υπολογιστικών πόρων. Όλη αυτή η διαδικασία

της εικονικοποίησης υλοποιείται μέσω των υπερεποπτών (hypervisors), οι οποίοι αφορούν λογισμικά που είναι υπεύθυνα για την απομόνωση των εικονικών μηχανών (Virtual Machines - VM), έτσι ώστε να αποτρέπεται η άμεση πρόσβαση στους εικονικούς δίσκους, τη μνήμη ή εφαρμογές άλλων μηχανών VM στον ίδιο host [6]. Η εικονικοποίηση παρέχει επεκτασιμότητα και πολυχρηστικότητα (που επιτυγχάνεται όταν ένα και μόνο στιγμιότυπο μιας εφαρμογής λογισμικού εξυπηρετεί πολλούς πελάτες), δύο ιδιότητες που αποτελούν σημαντικά χαρακτηριστικά του μοντέλου CC και διευκολύνουν την κοινή χρήση και τη συγκέντρωση πόρων, προκειμένου να βελτιωθεί η ευκινησία, η ευελιξία, να μειωθεί το κόστος και να ενισχυθεί η επιχειρηματική αξία [7].

Οι πρακτικές πτυχές της εικονικοποίησης που σχετίζονται με τη διαμόρφωση, τη δικτύωση και το μέγεθος των συστημάτων cloud, αντιμετωπίζουν πολλές προκλήσεις [6]. Για παράδειγμα, η παροχή (provisioning) υπολογιστικών πόρων αποτελεί ένα βασικό μηχανισμό της διαδικασίας της εικονικοποίησης, που χρησιμοποιείται για την κατανομή των πόρων ενός παρόχου cloud σε έναν πελάτη. Όταν ένας πάροχος cloud λαμβάνει αίτημα από έναν πελάτη, πρέπει να δημιουργήσει τον κατάλληλο αριθμό μηχανών VM και να διαθέσει ανάλογους πόρους για την υποστήριξή τους. Η διαδικασία της παροχής υπολογιστικών πόρων μπορεί να διεξαχθεί με πολλούς διαφορετικούς τρόπους, όπως η εκ των προτέρων παροχή υπολογιστικών πόρων (advance provisioning), η δυναμική παροχή υπολογιστικών πόρων (dynamic provisioning) και η δυνατότητα αυτόνομης παροχής υπολογιστικών πόρων στον εκάστοτε χρήστη (user self-provisioning), καθένας από τους οποίους καλείται να αντιμετωπίσει διαφορετικές προκλήσεις [8]. Οι προκλήσεις αυτές μπορούν να αφορούν τη βέλτιστη διαμόρφωση των μηχανών VM και καθώς και τον περιορισμό στον αριθμό και τις δυνατότητες των επεξεργαστών, των μνήμων, των δίσκων και του εύρους ζώνης δικτύου που πρέπει να κατανεμηθούν μεταξύ των μηχανών αυτών. Λόγω αυτών των προκλήσεων, οι πάροχοι υπηρεσιών cloud καταβάλουν κάθε δυνατή προσπάθεια ώστε να εξασφαλίσουν την ασφάλεια των μηχανισμών εικονικοποίησης, προσπαθώντας να εξαλείψουν ή τουλάχιστον να μειώσουν τα τρωτά σημεία των συστημάτων cloud, αλλά και τις απειλές και τις επιθέσεις που θα μπορούσαν να δεχθούν [9]. Με τις συνεχιζόμενες τεχνολογικές εξελίξεις, η εμβέλεια και η επιρροή του CC συνεχίζει να αυξάνεται, με αποτέλεσμα τα ζητήματα ασφάλειας του να θεωρούνται κρίσιμα, όχι μόνο για τους παρόχους cloud αλλά και για τις επιχειρήσεις και τους μεμονωμένους χρήστες που μεταφορτώνουν τα δεδομένα και τις εφαρμογές τους σε αυτούς [10].

Με την ανάπτυξη των σύγχρονων τεχνολογιών ΤΠΕ, το ζήτημα της ασφάλειας και της προστασίας των δεδομένων παραμένει ένα από τα μεγαλύτερα προβλήματα του 21ου αιώνα. Επομένως αποτελεί και ένα πολύ ευαίσθητο ζήτημα και το μοντέλο CC και των υπηρεσιών που παρέχονται μέσω αυτού [11]. Σύμφωνα με τους Daimi και συν. (2018) με τον όρο ασφάλεια εννοείται *"το δικαίωμα που έχει ο οποιοσδήποτε ώστε να μην επηρεάζονται οι δραστηριότητές του από την παραβίαση των αντικειμένων του"* [12]. Ένας κλασικός ορισμός της ασφάλειας, που προκύπτει από την ανάδειξη των βασικών χαρακτηριστικών της, αφορά το ακρωνύμιο "CIA" (Confidentiality, Integrity, Availability). Ο συγκεκριμένος τρόπος ερμηνείας της ασφάλειας αναδεικνύει την

εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα, ως τις τρεις βασικές απαιτήσεις που θα πρέπει να πληροί ένα οποιοδήποτε σύστημα για να θεωρηθεί ασφαλές [13]. Οι απαιτήσεις αυτές ορίζονται ως εξής [14]:

1) Εμπιστευτικότητα: Είναι η δυνατότητα απόκρυψης πληροφοριών από άτομα που δεν έχουν εξουσιοδότηση να τα δουν. Είναι η βάση πολλών μηχανισμών ασφαλείας που προστατεύουν όχι μόνο τις πληροφορίες αλλά και άλλους πόρους.

2) Ακεραιότητα: Είναι η ικανότητα να διασφαλίζεται ότι τα δεδομένα αποτελούν ακριβή και αμετάβλητη αναπαράσταση των αρχικών πληροφοριών.

3) Διαθεσιμότητα: Διασφαλίζει ότι ένας πόρος είναι άμεσα προσβάσιμος στον εξουσιοδοτημένο χρήστη κατόπιν αιτήματός του.

Με βάση αυτήν την τριάδα απαιτήσεων, μπορεί να εξεταστεί η ασφάλεια όλων των σύγχρονων μοντέλων πληροφοριών. Ανάλογα με τις ανάγκες του εκάστοτε συστήματος, δίνεται μεγαλύτερη έμφαση στους ελέγχους ασφάλειας που αυξάνουν την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα, ή και τα τρία. Με άλλα λόγια, ο χώρος των δραστηριοτήτων είναι αυτός που εν μέρει προσδιορίζει της ανάγκες ασφάλειας του cloud [11].

Στη βιβλιογραφία μέχρι τώρα έχει εμφανιστεί ένα αρκετά μεγάλο πλήθος μελετών που ασχολείται αποκλειστικά με τα θέματα ασφάλειας των περιβαλλόντων cloud. Για την καλύτερη και πληρέστερη κατανόηση όλων των ζητημάτων ασφαλείας που καλούνται να αντιμετωπίσουν σήμερα τα περιβάλλοντα cloud, μελετητές και ερευνητές έχουν χρησιμοποιήσει διαφορετικά κριτήρια εξέτασης του θέματος, έτσι ώστε να δημιουργηθεί μια ολοκληρωμένη εικόνα του [15]. Στο πλαίσιο της παρούσας εργασίας θα γίνει μια αντίστοιχη προσπάθεια ανάλυσης της όλης κατάστασης και της παρουσίασης των αντίστοιχων λύσεων που έχουν εμφανιστεί τα τελευταία χρόνια στη βιβλιογραφία.

1.2 Σκοπός της πτυχιακής εργασίας

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση των ζητημάτων ασφάλειας που παρουσιάζουν το μοντέλο CC και τα περιβάλλοντα cloud. Η κύρια προσέγγιση της παρουσίασης αυτής είναι καθαρά από τεχνικής πλευράς, εστιάζοντας στην εύρεση και ταξινόμηση των ζητημάτων ασφάλειας του μοντέλου CC αλλά και των πιθανών λύσεων που έχουν παρουσιαστεί μέχρι τώρα στη βιβλιογραφία. Στην παρουσίαση αυτή εξαιρέθηκαν άλλες πλευρές ζητημάτων ασφάλειας, όπως νομική ή κανονιστική, που σχετίζονται με τα περιβάλλοντα cloud.

Η ερευνητική προσέγγιση της πτυχιακής εργασίας θα γίνει με χρήση των βάσεων δεδομένων Google Scholar και Google, για την ανεύρεση διαφόρων μελετών, άρθρων και πηγών. Η τεχνική πτυχή των περιβαλλόντων cloud θα διερευνηθεί μελετώντας ακαδημαϊκά έγγραφα. Η παρουσίαση και ανάλυση των μελετών αποσκοπεί στην εξαγωγή συμπερασμάτων και προτάσεων για μελλοντική έρευνα.

1.3 Δομή της πτυχιακής εργασίας

Στα πλαίσια της παρούσας πτυχιακής εργασίας, για την μελέτη των ζητημάτων ασφαλείας στο Cloud, επιλέχθηκε η ακόλουθη δομή.

Στο κεφάλαιο 2 δίνεται μια σύντομη επισκόπηση του μοντέλου CC και περιγράφονται τα μοντέλα ανάπτυξης των cloud καθώς και οι διαφορετικές υπηρεσίες που μπορούν να παρέχονται από αυτά.

Στο κεφάλαιο 3 γίνεται μια παρουσίαση και προσπάθεια ταξινόμησης των ζητημάτων ασφαλείας από τεχνικής άποψης που έχουν μελετηθεί κατά καιρούς στη βιβλιογραφία και αφορούν το Cloud.

Το κεφάλαιο 4 αφορά μια βιβλιογραφική ανασκόπηση των πιθανών λύσεων των ζητημάτων ασφαλείας που παρουσιάστηκαν στο προηγούμενο κεφάλαιο.

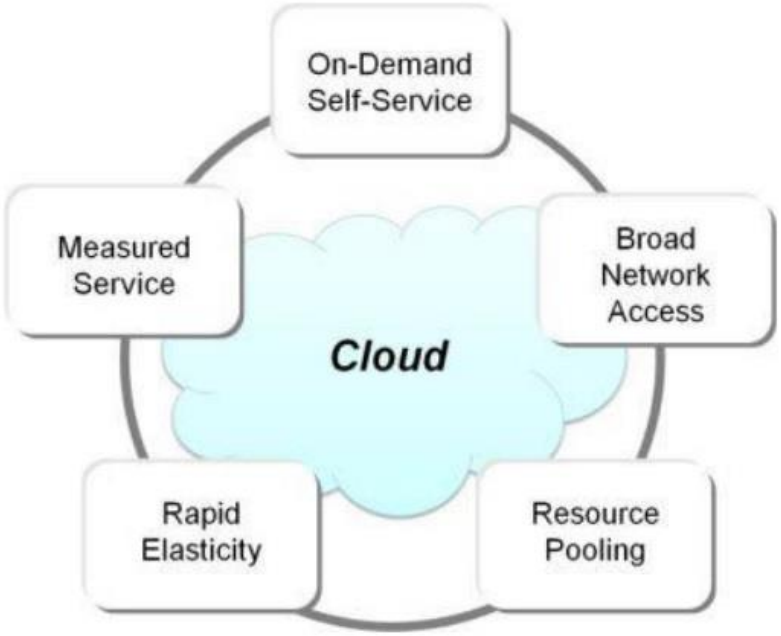
Το κεφάλαιο 5 αποτελεί μια μελέτη περίπτωσης των ζητημάτων ασφάλειας που παρουσιάζει το Cloud στον τομέα της υγείας.

Τέλος, η εργασία ολοκληρώνεται με κάποια συμπεράσματα που προκύπτουν από την ανάλυση όλων των παραπάνω θεμάτων.

2 Cloud Computing

2.1 Βασικά χαρακτηριστικά του Cloud Computing

Με βάση τα χαρακτηριστικά του, το CC διαφοροποιείται από τα υπόλοιπα υπολογιστικά πρότυπα ή μοντέλα. Κάποια από αυτά τα χαρακτηριστικά είναι κοινά για όλα τα υπολογιστικά μοντέλα. Στη βιβλιογραφία όμως έχουν παρουσιαστεί μελέτες που αποδίδουν στο CC πέντε βασικά χαρακτηριστικά, που τα ξεχωρίζουν από τα υπόλοιπα υπολογιστικά πρότυπα. Τα χαρακτηριστικά αυτά αφορούν (Εικ. 2.1) [16], [17]:



Εικόνα 2.1: **Τα 5 βασικά χαρακτηριστικά του μοντέλου CC [16]**

1) ***Αυτοεξυπηρέτηση κατ' απαίτηση (On-demand self-service)***: Επιτρέπει την μονομερή παροχή στο χρήστη υπολογιστικών δυνατοτήτων ως χρόνο διακομιστή και χώρο αποθήκευσης δικτύου. Μια τέτοια δυνατότητα είναι εφικτή χωρίς να απαιτείται καμία αλληλεπίδραση μεταξύ χρήστη και παρόχου υπηρεσιών. Οι υπολογιστικοί πόροι είναι άμεσα διαθέσιμοι στους χρήστες και ανάλογοι των απαιτήσεών τους.

2) ***Ευρεία πρόσβαση στο δίκτυο (Broad network access)***: Αφορά τη διαθεσιμότητα των υπολογιστικών πόρων στους χρήστες μέσω του δικτύου. Οι χρήστες μπορούν να έχουν πρόσβαση σε πόρους cloud μέσω τυπικών μηχανισμών που τους επιτρέπουν να χρησιμοποιούν ετερογενείς πλατφόρμες, δηλαδή μπορούν να έχουν πρόσβαση σε πόρους cloud μέσω κινητών τηλεφώνων, φορητών και σταθερών υπολογιστών. Επομένως, η πρόσβαση των χρηστών σε υπηρεσίες cloud δεν απαιτείται να γίνεται από συγκεκριμένες διαδικτυακές τοποθεσίες, αλλά από οποιαδήποτε και οποτεδήποτε.

3) ***Συγκέντρωση πόρων (Resource pooling)***: Οι πάροχοι υπηρεσιών συγκεντρώνουν διαφορετικούς φυσικούς και εικονικούς πόρους έτσι ώστε να

ικανοποιούν τις υπολογιστικές ανάγκες όλων των χρηστών. Οι συγκεντρωμένοι πόροι (όπως διακομιστές, συσκευές αποθήκευσης κλπ.) είναι κοινής χρήσης για όλους τους χρήστες. Η βελτιστοποίηση της ποιότητας των παρεχόμενων στους χρήστες υπηρεσιών γίνεται από τους παρόχους με κατάλληλη επιλογή των πόρων από αυτούς που έχουν συγκεντρωθεί ώστε να ικανοποιούν τις απαιτήσεις των πελατών τους. Η κοινή χρήση διευκολύνει τη μείωση του κόστους, καθώς επιτρέπει την εξυπηρέτηση περισσότερων εφαρμογών από το υπολογιστικό hardware υλικό του cloud σε σύγκριση με τον αριθμό των εφαρμογών που θα μπορούσαν να εξυπηρετηθούν αν χρησιμοποιούνταν αποκλειστικοί (dedicated) υπολογιστικοί πόροι.

4) ***Γρήγορη ελαστικότητα (Rapid elasticity)***: Αφορά την ταχεία και ελαστική δέσμευση για παροχή υπολογιστικών πόρων στους χρήστες (scale out), καθώς επίσης και τη γρήγορη αποδέσμευσή τους για διάθεση προς άλλους χρήστες (scale in). Οι υπολογιστικοί πόροι που παρέχονται στους καταναλωτές είναι (από την πλευρά του χρήστη) απεριόριστοι και μπορούν να χρησιμοποιηθούν σε οποιαδήποτε ποσότητα και ανά πάσα στιγμή. Η ελαστικότητα αυτή αυξάνει την ικανότητα εξυπηρέτησης των πελατών στις περιόδους αιχμής και μειώνει τη χωρητικότητα στις περιόδους εκτός αιχμής, επιτρέποντας έτσι την ελαχιστοποίηση για τους καταναλωτές του κόστους των υπηρεσιών cloud, πληρώντας ταυτόχρονα τις απαιτήσεις τους ως προς την ποιότητα των παρεχόμενων υπηρεσιών.

5) ***Τιμολόγηση βάσει χρήσης (Measured service)***: Αυτή η υπηρεσία ελέγχει και βελτιστοποιεί αυτόματα τη χρήση των πόρων. Γίνεται σε κάποιο επίπεδο αφαίρεσης κατάλληλο για τον εκάστοτε τύπο υπηρεσίας CC. Αυτό το χαρακτηριστικό επιτρέπει την παρακολούθηση, τον έλεγχο και την αναφορά της χρήσης των πόρων και, συνεπώς, τη δυνατότητα για δίκαιες τιμολογήσεις των υπηρεσιών.

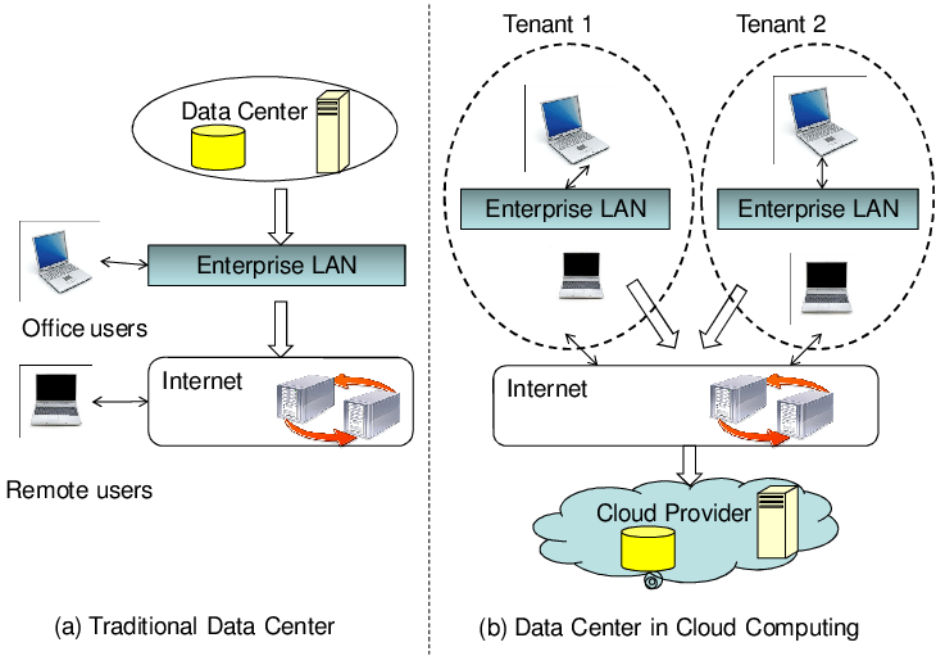
2.2 Σύγκριση Cloud Computing με άλλα υπολογιστικά μοντέλα

Το CC είναι μια τεχνολογία υπολογιστικής που δημιουργήθηκε για να ικανοποιήσει τις ανάγκες ύπαρξης ευέλικτων υποδομών πληροφορικής, ανάλυσης των Big Data και αυξημένης χρήσης των κινητών συσκευών [18]. Τα βασικά του χαρακτηριστικά, όπως παρουσιάστηκαν στην προηγούμενη ενότητα, το καθιστούν τελείως διαφορετικό από τις παραδοσιακές βάσεις δεδομένων αλλά και από άλλα υπολογιστικά μοντέλα.

2.2.1 Σύγκριση κέντρου δεδομένων Cloud με παραδοσιακά κέντρα δεδομένων

Όπως φαίνεται στην εικόνα 2.2, τα παραδοσιακά κέντρα δεδομένων διαφέρουν από αυτά των cloud ως προς τα χαρακτηριστικά τους. Η κύρια διαφορά των δύο κέντρων δεδομένων αφορά τη διαμόρφωση του hardware υλικού και του λογισμικού για την εκτέλεση των επιθυμητών από τους πελάτες τους διεργασιών, σε κάθε περίπτωση. Αυτό όμως σημαίνει ότι και το επίπεδο ασφάλειας σε κάθε περίπτωση είναι διαφορετικό. Στα παραδοσιακά κέντρα δεδομένων, κάθε διεργασία που εκτελείται από

συγκεκριμένη υποδομή έχει το δικό της επίπεδο ασφάλειας και είναι σχετικά εύκολο να αποτραπεί η αλληλεπίδραση μεταξύ των απομονωμένων μεταξύ τους υποδομών. Η απομόνωση των υποδομών κάθε διεργασίας διευκολύνει την πρόληψη των αλληλεπιδράσεων μεταξύ των στοιχείων δικτύωσης, υπολογισμού και αποθήκευσης διαφορετικών χρηστών [19].



Εικόνα 2.2: **Διαφορές μεταξύ (α) παραδοσιακών κέντρων δεδομένων και (β) κέντρων δεδομένων cloud [19]**

Αντίθετα, τα κέντρα δεδομένων cloud δεν χαρακτηρίζονται από την προσέγγιση της απομόνωσης των υποδομών, καθώς όλες οι διεργασίες που εκτελούνται σε ιδιωτικά cloud μοιράζονται την ίδια υποδομή διακομιστή, χώρου αποθήκευσης και δικτύου. Αυτό που επιτυγχάνεται όμως στα περιβάλλοντα cloud είναι η εκμετάλλευση κατάλληλα διαμορφωμένων λογισμικών, με σκοπό τη δημιουργία λογικής απομόνωσης [10].

Ένα κέντρο δεδομένων cloud θεωρείται καλύτερη επιλογή επειδή μπορεί να παρέχει όλες τις λειτουργίες και τις υπηρεσίες που παρέχει ένα παραδοσιακό κέντρο δεδομένων, αλλά με χαμηλότερο κόστος λόγω των οικονομιών κλίμακας (economies of scales), κάτι που αποτελεί και ένα από τα βασικά πλεονεκτήματα του μοντέλου [20]. Επίσης παρέχει μεγαλύτερη ευελιξία, καθώς η οποιαδήποτε εφαρμογή μπορεί να εκτελεστεί από έναν πελάτη, χωρίς αυτός να πρέπει να δημιουργήσει δική του υποδομή, αφαιρώντας κάθε βάρος συντήρησης και διαχείρισης. Τέλος, η πολυπλοκότητα των παραδοσιακών κέντρων δεδομένων αυξάνεται με την αύξηση των αποθηκευτικών χώρων, ενώ τα κέντρα δεδομένων cloud παρουσιάζουν ταχεία ελαστικότητα και επεκτασιμότητα καθώς οι εφαρμογές κάθε χρήστη μπορούν να εξυπηρετηθούν ανά πάσα στιγμή [17].

2.2.2 Σύγκριση Cloud Computing και Utility Computing

Το Utility Computing (UC) αναφέρεται σε έναν τύπο υπολογιστικών τεχνολογιών και επιχειρηματικών μοντέλων που παρέχουν υπηρεσίες και υπολογιστικούς πόρους στους πελάτες, όπως αποθήκευση, εφαρμογές και υπολογιστική ισχύ. Αυτό το μοντέλο έχει το πλεονέκτημα χρήσης υπολογιστικών πόρων χαμηλού κόστους. Η φιλοσοφία του αποτέλεσε το θεμέλιο λίθο της στροφής προς υπολογιστικά μοντέλα παροχής υπολογιστικής κατ' απαίτηση και παροχής λογισμικού ως υπηρεσία, που κατέληξαν στην μετέπειτα ιδέα της παροχής υπολογιστικής, εφαρμογών και δικτύου ως υπηρεσία. Το μοντέλο του UC περιλαμβάνει ένα είδος εικονικοποίησης, σύμφωνα με το οποίο χρησιμοποιούνται πολλαπλοί backend διακομιστές ιστού για να καταστεί δυνατή η παροχή υπηρεσιών ιστού. Επίσης, στο συγκεκριμένο μοντέλο οι πόροι λογισμικού και hardware υλικού συγκεντρώνονται σε μεγάλα κέντρα δεδομένων και οι χρήστες πληρώνουν ανά χρήση για υπηρεσίες αποθήκευσης και επικοινωνίας [21].

Υπάρχουν πολλές ομοιότητες μεταξύ UC και CC. Η λειτουργία του UC απαιτεί συχνά μια υποδομή που μοιάζει με cloud, αλλά η παροχή υπολογιστικών υπηρεσιών αφορά ως επί το πλείστο τις επιχειρήσεις. Η σημαντική διαφορά τους είναι ότι ενώ το UC περιλαμβάνει μια απλή ενοικίαση των υποδομών στους χρήστες, των οποίων έχουν πλήρη έλεγχο, στο CC, οι χρήστες πληρώνουν για τους πόρους που χρησιμοποιούν, αλλά η υποδομή και το λογισμικό ελέγχονται από τους ιδιοκτήτες και τους διαχειριστές του cloud [21].

2.2.3 Σύγκριση Cloud Computing και Grid Computing

Το Grid Computing (GC) είναι ένα δίκτυο με κατανεμημένους πόρους hardware υλικού και λογισμικού, το οποίο μπορεί να κατανεμηθεί σε μεγάλο αριθμό χρηστών και να ανήκει σε διάφορους οργανισμούς. Οι χρήστες του είναι υποχρεωμένοι να παρέχουν το hardware υλικό και το λογισμικό τους σε άλλους χρήστες σύμφωνα με πρόγραμμα που διαχειρίζεται ο διαχειριστής του δικτύου [22].

Η σύγκριση CC και GC αναδεικνύει αρκετές ομοιότητες. Θεωρητικά, η ιδέα πίσω από τα δύο μοντέλα αφορά την ομαδοποίηση διάφορων υπολογιστικών πόρων και η κλιμακωτή παροχή των δυνατοτήτων τους, με απώτερο σκοπό την επίτευξη μίας ή περισσοτέρων σύνθετων διεργασιών που θα ήταν δύσκολο ή ακόμη και αδύνατο να επιτευχθούν με έναν μόνο πόρο [23]. Οι υπολογιστικοί πόροι του GC μπορεί να περιλαμβάνουν κύκλους επεξεργασίας, χώρους δίσκων μνήμης, δίκτυα, εκτυπωτές, σαρωτές, άδειες χρήσης λογισμικού, απομακρυσμένες συσκευές κλπ. Το συγκεκριμένο μοντέλο χρησιμοποιείται περισσότερο για ακαδημαϊκούς και ερευνητικούς σκοπούς καθώς μπορεί να παρέχει μεγάλη υπολογιστική ισχύ σε δύσκολες διεργασίες, γρηγορότερα και φθηνότερα [23].

Σε ένα επιχειρηματικό μοντέλο, κάθε πελάτης διαπραγματεύεται με τους παρόχους για τη χρήση πόρων δικτύου, παρέχοντας μια λεπτομερή ανάλυση της διεργασίας που προτίθεται να πραγματοποιήσει και τους πόρους που θα πρέπει να χρησιμοποιήσει [24]. Στόχος της ανάπτυξης του GC ήταν να διευκολύνει τους χρήστες να χρησιμοποιούν από απόσταση την αδρανή υπολογιστική ισχύ σε άλλα υπολογιστικά κέντρα όταν το

τοπικό υπολογιστικό κέντρο είναι απασχολημένο ή δεν διαθέτει επαρκείς πόρους ώστε να εκτελέσει κάποια συγκεκριμένη διεργασία από μόνο του.

Η ανάλυση των βιβλιογραφικών μελετών πάνω στη λειτουργία των μοντέλων GC και CC έχει αναδείξει και μεγάλες διαφορές μεταξύ των δύο μοντέλων [23]. Το GC αφορά την ομαδοποίηση διαφόρων διάσπαρτων υπολογιστικών πόρων με σκοπό τη δημιουργία ενός συστήματος με μεγαλύτερη υπολογιστική ισχύ. Ενώ, το CC αφορά την παροχή cloud υπηρεσιών που χρησιμοποιούνται από τους πελάτες.

Το υπολογιστικό πλέγμα και το πλέγμα δεδομένων είναι δύο κύρια στοιχεία του GC που ασχολούνται με την επίτευξη υψηλότερης υπολογιστικής ισχύος ή μεγαλύτερης χωρητικότητας αποθήκευσης. Από την άλλη πλευρά, οι διάφοροι τύποι του μοντέλου CC περιλαμβάνουν την παροχή υποδομής ως υπηρεσία, πλατφόρμας ως υπηρεσία και λογισμικού ως υπηρεσία. Αυτοί οι τρεις τύποι CC παρέχουν αντίστοιχες υπηρεσίες υποδομών αποθήκευσης, πλατφορμών και εφαρμογών και συγκεκριμένων λογισμικών.

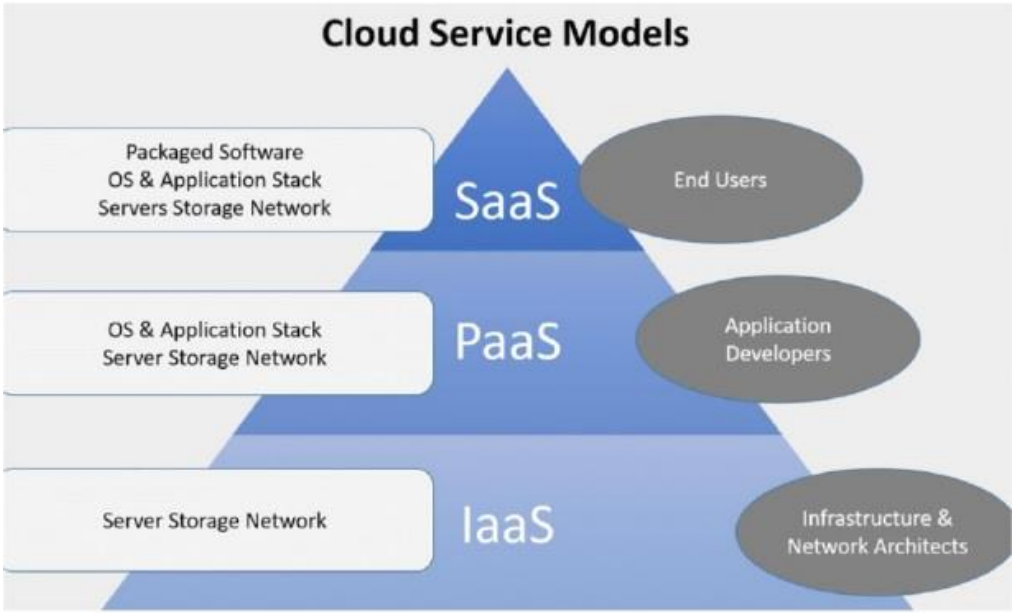
Τα βασικά μέρη του GC είναι οι πελάτες και οι διαχειριστές πλέγματος. Αντίθετα, τα βασικά μέρη του CC είναι οι πελάτες και οι διακομιστές cloud. Η λειτουργία του GC είναι τέτοια ώστε ο πελάτης να υποβάλλει την εκάστοτε διεργασία στον διαχειριστή πλέγματος που χρησιμοποιεί πόρους δεδομένων για την εκτέλεσή της. Στην περίπτωση αυτή, ο πελάτης δεν έχει γνώση για το πού εκτελείται η διεργασία. Μετά την εκτέλεσή της, οι πληροφορίες επιστρέφουν στον πελάτη και η χρέωση των χρησιμοποιούμενων πόρων γίνεται από τον διαχειριστή δικτύου. Από την άλλη πλευρά, η λειτουργία του CC είναι τέτοια που η εκάστοτε διεργασία υποβάλλεται από τον πελάτη στους διακομιστές cloud, οι οποίοι εκτελούν την διεργασία εντός του cloud και αποστέλλουν τις όποιες πληροφορίες στον πελάτη μετά την ολοκλήρωσή της. Ένας διακομιστής cloud είναι δυναμικής συνδεσμολογίας και μπορεί να δημιουργηθεί εντός του cloud από παράλληλους διακομιστές ή από κατανεμημένους διακομιστές, ανάλογα με τις ανάγκες τις εκάστοτε διεργασίας. Η χρέωση των παρεχόμενων υπηρεσιών γίνεται με βάση το μοντέλο UC που εμπεριέχεται στο CC.

Τέλος, ως προς τις εφαρμογές, το μοντέλο GC χρησιμοποιείται κυρίως σε υπηρεσίες εκπαίδευσης εξ αποστάσεως, αποθήκευσης δεδομένων βιοπληροφορικής και επεξεργασίας χημικών υπολογισμών. Αντίθετα, η εφαρμογή του CC αφορά κυρίως τα συστήματα ενδοεπιχειρησιακού σχεδιασμού (Enterprise Resource Planning – ERP) [25], [26].

2.3 Μοντέλα παροχής υπηρεσιών cloud

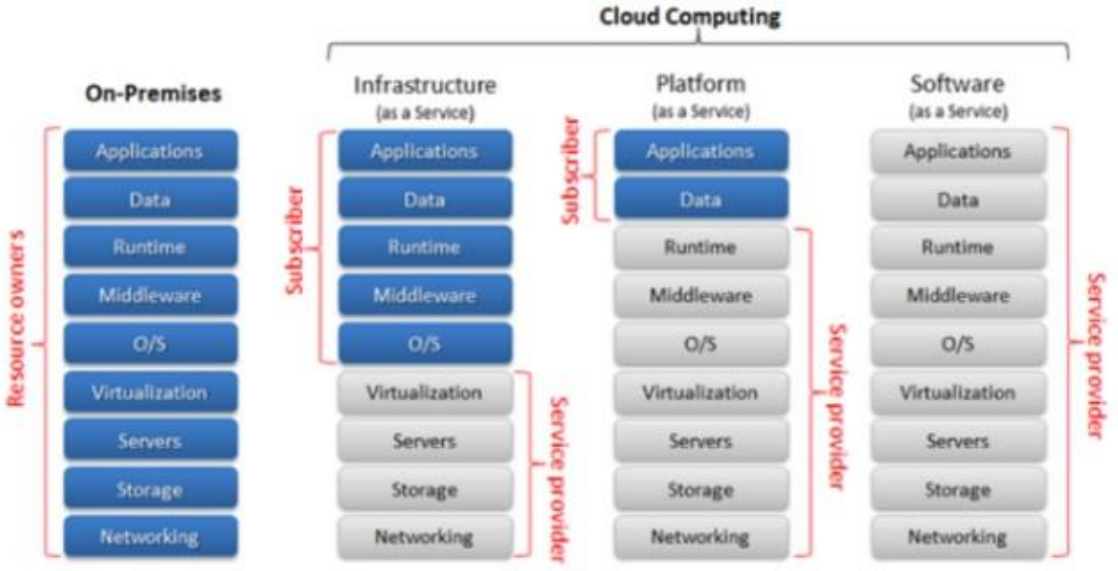
Ένα μοντέλο παροχής υπηρεσιών cloud αντιπροσωπεύει έναν συγκεκριμένο συνδυασμό πόρων πληροφορικής που προσφέρει ένας πάροχος. Ανάμεσα στα πολλά μοντέλα παροχής υπηρεσιών cloud, τρία έχουν καθιερωθεί ως τα πλέον βασικά. Πρόκειται για τα μοντέλα (Εικ. 2.3) [27]:

- Λογισμικό ως υπηρεσία (Software as a service - SaaS)
- Πλατφόρμα ως υπηρεσία (Platform as a service - PaaS)
- Υποδομή ως υπηρεσία (Infrastructure as a service - IaaS)



Εικόνα 2.3: **Τα τρία βασικά μοντέλα παροχής cloud [27]**

Παρόλο που συχνά αναφέρονται ως ένα ενιαίο μοντέλο SPI (που προέρχεται από τα αρχικά γράμματα των υπηρεσιών που παρέχει Software, Platform και Infrastructure) [28], ωστόσο, αυτά τα τρία μοντέλα διαφέρουν μεταξύ τους ως προς τη λειτουργικότητα και το επίπεδο διαχειριστικού ελέγχου που παρέχουν στους χρήστες cloud. Στην εικόνα 2.4 παρουσιάζεται η αλληλεξάρτηση των τριών αυτών μοντέλων και τα επίπεδα πόρων τους. Η αλληλεξάρτησή τους αφορά το γεγονός ότι το εύρος των πόρων του ενός μπορεί να καλύπτει αυτό του άλλου [27].



Εικόνα 2.4: **Σχέση υπηρεσιών και υποδομής των τριών βασικών μοντέλων παροχής υπηρεσιών cloud [28]**

2.3.1 Λογισμικό ως υπηρεσία (SaaS)

Με το μοντέλο SaaS, οι καταναλωτές CC έχουν τη δυνατότητα να χρησιμοποιούν τις εφαρμογές του παρόχου CC που εκτελούνται στην υποδομή cloud (σε αντίθεση με το μοντέλο PaaS, όπου εκτελούν τις δικές τους εφαρμογές). Στο μοντέλο SaaS, οι χρήστες του cloud δεν έχουν έλεγχο ή δικαίωμα διαχείρισης της υποκείμενης υποδομής cloud ή ακόμη και των μεμονωμένων εφαρμογών [28]. Όπως φαίνεται στην εικόνα 2.4, όμως, το μοντέλο τους δίνει κάποιες δυνατότητες περιορισμένης πρόσβασης στις ρυθμίσεις διαμόρφωσης κάποιων εφαρμογών. Οι υπηρεσίες SaaS περιλαμβάνουν εφαρμογές email και παραγωγικότητας γραφείου, διαχείριση πελατειακών σχέσεων (συστήματα Customer Relations Management – CRM), σχεδιασμό εταιρικών πόρων (συστήματα ERP), κοινωνική δικτύωση, διαχείριση δεδομένων κλπ. [29].

Τα βασικότερα χαρακτηριστικά του μοντέλου SaaS περιλαμβάνουν [29], [30]:

1) Λογισμικό που φιλοξενείται σε απομακρυσμένο διακομιστή και είναι πάντα προσβάσιμο μέσω ενός προγράμματος περιήγησης στο Διαδίκτυο.

2) Εφαρμογή που διαχειρίζεται από μια κεντρική τοποθεσία.

3) Οι χρήστες εφαρμογών δεν χρειάζεται να ανησυχούν για το hardware υλικό ή λογισμικό που χρησιμοποιούν (ενημερώσεις, patch, κλπ.)

4) Οποιαδήποτε ενσωμάτωση με εφαρμογές τρίτων γίνεται μέσω διεπαφών API

Η χρήση του μοντέλου SaaS από τους χρήστες συνίσταται για περιπτώσεις όπως [29], [30]:

1) Εφαρμογές όπου οι απαιτήσεις αυξάνονται ή μειώνονται σημαντικά. Για παράδειγμα, το λογισμικό της εφορίας παρουσιάζει μεγάλη ζήτηση κατά τη διάρκεια της περιόδου κατάθεσης των φορολογικών δηλώσεων, οι κρατήσεις στα ξενοδοχεία σημειώνουν άνοδο κατά τις περιόδους των διακοπών, κλπ.

2) Εφαρμογές που απαιτούν πρόσβαση στο Διαδίκτυο από σταθερές ή κινητές συσκευές. Παραδείγματα αποτελούν τα λογισμικά διαχείρισης πωλήσεων, συστήματα CRM, κλπ.

3) Βραχυπρόθεσμα project που απαιτούν συνεργασία. Το μοντέλο pay-as-you-go καθιστά εύκολη τη διαδικασία γρήγορης δημιουργίας και διάλυσης ενός συνεργατικού περιβάλλοντος.

4) Νέες επιχειρήσεις που θέλουν να δημιουργήσουν γρήγορα ιστότοπους ηλεκτρονικού εμπορίου χωρίς να ανησυχούν για τις διαμορφώσεις του διακομιστή και τις ενημερώσεις λογισμικού.

Παραδείγματα υπηρεσιών SaaS αποτελούν οι Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting και Cisco WebEx.

2.3.2 Πλατφόρμα ως υπηρεσία (PaaS)

Το μοντέλο PaaS δίνει στους καταναλωτές τη δυνατότητα να αναπτύξουν σε μια υποδομή cloud εφαρμογές που έχουν δημιουργήσει ή αποκτήσει, χρησιμοποιώντας

γλώσσες προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο CC. Όπως φαίνεται στην εικόνα 2.4, δεν παρέχεται στους καταναλωτές ο έλεγχος ή η δυνατότητα διαχείρισης της υποκείμενης υποδομής cloud, δηλαδή δίκτυα, διακομιστές, χώρο αποθήκευσης, εφαρμογές, δεδομένα κλπ. [29]. Ωστόσο, τους δίνεται η δυνατότητα διαχείρισης των εφαρμογών που έχουν αναπτύξει σε περιβάλλον φιλοξενίας εφαρμογών, κάτι που βοηθά στην γρήγορη και διαφανή εκτέλεση των εφαρμογών. Οι υπηρεσίες PaaS περιλαμβάνουν εικονική επιφάνεια εργασίας, πλατφόρμες παροχής και ανάπτυξης διαδικτυακών υπηρεσιών, υπηρεσίες βάσεων δεδομένων κλπ. [30].

Τα βασικότερα χαρακτηριστικά του μοντέλου PaaS περιλαμβάνουν [29], [30]:

1) Μια τεχνολογία εικονικοποίησης που βασίζεται στο PaaS επιτρέπει την απόκτηση πόρων κατ' απαίτηση και την προς τα πάνω ή προς τα κάτω κλιμάκωσή τους, όπως απαιτείται.

2) Διαφοροποίηση των υπηρεσιών ανάπτυξης και εκτέλεσης εφαρμογών για διευκόλυνση της ανάπτυξης, δοκιμής και φιλοξενίας εφαρμογών λογισμικού σε ένα ολοκληρωμένο περιβάλλον ανάπτυξης.

3) Κοινή χρήση του ίδιου περιβάλλοντος ανάπτυξης από πολλούς χρήστες.

4) Ολοκληρωμένες υπηρεσίες Διαδικτύου και βάσεις δεδομένων.

5) Τιμολόγηση και εγγραφή που διαχειρίζονται από εργαλεία CC.

Η χρήση του μοντέλου PaaS συνίσταται για περιπτώσεις όπως [29], [30]:

1) Πολλοί προγραμματιστές που εργάζονται για την ανάπτυξη του ίδιου προϊόντος ή εξωτερικά μέρη που συμμετέχουν στη διαδικασία ανάπτυξης. Το μοντέλο PaaS παρέχει ταχύτητα και ευελιξία στη διαδικασία ανάπτυξης.

2) Οργανισμοί που ακολουθούν την Ευέλικτη Μεθοδολογία για την ανάπτυξη λογισμικού. Το μοντέλο PaaS ορίζει τις δυσκολίες που σχετίζονται με την ταχεία ανάπτυξη και τις φάσεις επανάληψης μιας εφαρμογής.

3) Οργανισμοί που επιθυμούν να επεκτείνουν τις επενδύσεις κεφαλαίου τους. Το μοντέλο PaaS μειώνει τις δαπάνες που απαιτούνται για τη δημιουργία υποδομών υπολογιστικής, καθώς και για την ανάπτυξη και εκτέλεση εφαρμογών.

Παράδειγμα υπηρεσιών PaaS αποτελεί το Apprenda.

2.3.3 Υποδομή ως υπηρεσία (IaaS)

Το μοντέλο IaaS περιλαμβάνει την παροχή υπολογιστικών πόρων και υπηρεσιών όπως επεξεργασία, αποθήκευση, δίκτυα, δίκτυα παράδοσης περιεχομένου, δημιουργία αντιγράφων ασφαλείας και ανάκτησης, κλπ., στα οποία οι χρήστες μπορούν να αναπτύξουν και να εκτελέσουν το δικό τους λογισμικό [29]. Όπως φαίνεται στην εικόνα 2.4, το μοντέλο IaaS δεν δίνει στους καταναλωτές την δυνατότητα διαχείρισης ή ελέγχου της υποκείμενης υποδομής cloud ή των χαμηλότερων στρωμάτων του λειτουργικού συστήματος, αλλά τους επιτρέπει να έχουν τον πλήρη έλεγχο των

υψηλότερων επιπέδων του λειτουργικού συστήματος και των αναπτυγμένων εφαρμογών, όπως επίσης και περιορισμένο έλεγχο στοιχείων του δικτύου, όπως τα τείχη προστασίας του host [30].

Τα βασικότερα χαρακτηριστικά του μοντέλου IaaS περιλαμβάνουν [29], [30]:

1) Κάθε μέρος του hardware υλικού μπορεί να προσπελαύνεται από πολλαπλούς χρήστες.

2) Οι πόροι είναι διαθέσιμοι ως υπηρεσία.

3) Δυνατότητες δυναμικής κλιμάκωσης, βάσει των οποίων το κόστος ποικίλλει ανάλογα με την επιλογή της υποδομής.

Η χρήση του μοντέλου IaaS συνίσταται για περιπτώσεις όπως [29], [30]:

1) Οργανισμοί που χρειάζονται πλήρη έλεγχο του λογισμικού τους, π.χ. για εφαρμογές υψηλής απόδοσης.

2) Νέες επιχειρήσεις και μικρές εταιρείες που δεν επιθυμούν να ξοδέψουν χρήματα και χρόνο σε hardware υλικό και λογισμικό.

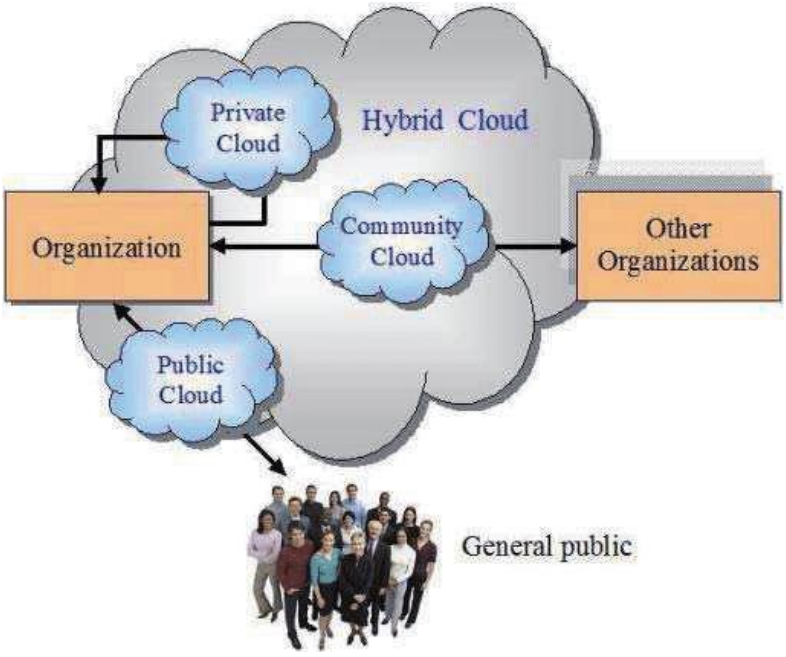
3) Αναπτυσσόμενοι οργανισμοί που δεν είναι ακόμη σίγουροι για το ποιες εφαρμογές θα χρειαστούν και ως εκ τούτου δεν θέλουν να δεσμευτούν σε συγκεκριμένες υποδομές.

4) Υπηρεσίες που αντιμετωπίζουν ασταθείς απαιτήσεις, όπου η εξαιρετικά δυναμική κλιμάκωση των πόρων σε συγχρονισμό με τις αιχμές ζήτησης είναι ζωτικής σημασίας.

Παραδείγματα υπηρεσιών IaaS αποτελούν οι Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure και Google Compute Engine (GCE).

2.4 Μοντέλα ανάπτυξης cloud

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) υπάρχουν τέσσερα μοντέλα ανάπτυξης cloud: (α) δημόσια, (β) ιδιωτικά, (γ) κοινοτικά και (δ) υβριδικά, όπως φαίνεται στην εικόνα 2.5. Ένα μοντέλο ανάπτυξης cloud ορίζεται ανάλογα με το σημείο πού βρίσκεται η υποδομή ανάπτυξης του cloud και το ποιος έχει τον έλεγχο της [31]. Κάθε ένα από αυτά τα μοντέλα έχει διαφορετικά χαρακτηριστικά και επιπτώσεις για τους πελάτες [32]. Η επιλογή του εκάστοτε κατάλληλου μοντέλου ανάπτυξης εξαρτάται από τους στόχους και τις επιχειρηματικές ανάγκες μιας εταιρείας ή ενός οργανισμού. Πριν από την επιλογή ενός μοντέλου ανάπτυξης, η επιχείρηση θα πρέπει να εξετάσει όλα τα ζητήματα ασφάλειας, αξιοπιστίας και απόδοσης που σχετίζονται με το μοντέλο που προτίθεται να υιοθετήσει [31].



Εικόνα 2.5: Μοντέλα ανάπτυξης cloud [31]

2.4.1 Δημόσιο cloud

Το δημόσιο (public) cloud είναι τα πιο ευρέως γνωστά, δημοφιλή και χρησιμοποιούμενα μοντέλα ανάπτυξης και αυτό που οι περισσότεροι άνθρωποι έχουν στο μυαλό τους ως "cloud". Στο συγκεκριμένο μοντέλο ανάπτυξης, οι πάροχοι cloud κατέχουν και διαχειρίζονται τις υποδομές, ενώ διαχειρίζονται και τις υπηρεσίες που είναι διαθέσιμες στο ευρύ κοινό. Ένα δημόσιο cloud έχει δυνατότητες πολλαπλής μίσθωσης και αποτελεί κοινή χρήση ενός μεγάλου αριθμού πελατών, που μεταξύ τους δεν έχουν τίποτα ή πολύ λίγα κοινά. Τα δεδομένα των χρηστών δεν είναι ορατά δημόσια [33].

Ανάμεσα στα πλεονεκτήματα ενός δημόσιου cloud, τα σημαντικότερα αφορούν τα εξής [34]:

1) ***Χαμηλό κόστος***: Η φύση του δημόσιου cloud αφορά την πληρωμή μόνο για ότι χρησιμοποιείται. Έτσι τα έξοδα μιας επιχείρησης από τη χρήση ενός δημόσιου cloud είναι ανάλογα του πλήθους των απαιτούμενων υπηρεσιών. Άλλα σημαντικά οικονομικά οφέλη που μπορεί να έχει η χρήση ενός δημόσιου cloud για μια επιχείρηση είναι η εξοικονόμηση μισθών που σχετίζονται με το μέγεθος και την εργασία της ομάδας πληροφορικής που απαιτείται να προσλάβει στην περίπτωση αυτή.

2) ***Αυξημένη αποδοτικότητα***: Δεδομένου ότι η συντήρηση της υποδομής των δημόσιων cloud εκτελείται από ειδικές ομάδες, ο χρόνος διακοπής παροχής υπηρεσιών σε ένα μοντέλο ανάπτυξης αυτού του είδους είναι λιγότερο πιθανό να αποτελέσει πρόβλημα. Επιπλέον, εάν οι εφαρμογές φιλοξενούνται από τον πάροχο CC, οι ενημερώσεις συνήθως διαχειρίζονται από τον ίδιο τον πάροχο, εξοικονομώντας τα όποια έξοδα αναβάθμισης.

Τα δημόσια cloud παρουσιάζουν όμως και κάποια μειονεκτήματα, τα σημαντικότερα από τα οποία αφορούν τα εξής [34]:

1) ***Λανθασμένη επιλογή παρόχου***: Στην περίπτωση λανθασμένης επιλογής παρόχου cloud, μπορούν να δημιουργηθούν πολλά προβλήματα για την επιχείρηση. Για παράδειγμα, εάν ένας πάροχος δεν αναβαθμίζει ή δεν ενημερώνει το hardware υλικό της υποδομής του, οι χρήστες ενδέχεται να αντιμετωπίσουν προβλήματα συμμόρφωσης και ταχύτητας εκτέλεσης.

2) ***Μειωμένος έλεγχος***: Καθώς το δημόσιο cloud ελέγχεται από τον πάροχο CC, οι χρήστες έχουν πολύ λιγότερο ή μηδενικό έλεγχο σε σύγκριση με την περίπτωση των ιδιωτικών cloud.

3) ***Αισθητά μικρότερη ασφάλεια***: Η ασφάλεια μπορεί να είναι ένα από τα βασικότερα μειονεκτήματα των δημόσιων cloud, αλλά, όπως αποδεικνύεται από το υψηλό επίπεδο υιοθέτησής τους από μερικούς από τους μεγαλύτερους οργανισμούς του κόσμου, οι ανησυχίες για την ασφάλεια είναι μικρές, εάν το δημόσιο cloud φιλοξενείται από παρόχους CC που γνωρίζουν τα θέματα ασφάλειας του μοντέλου και τον αντίκτυπό τους στην αντίληψη των πελατών.

2.4.2 Ιδιωτικό cloud

Ένα ιδιωτικό (private) cloud αφορά μια υπολογιστική υποδομή που είναι αποκλειστική μιας συγκεκριμένης επιχείρησης ή ομάδας. Το ιδιωτικό cloud μπορεί να αποτελεί ιδιοκτησία μιας επιχείρησης ή να μισθώνεται. Σε ιδιωτικό cloud, δεν υπάρχουν πρόσθετοι κανονισμοί ασφαλείας, νομικές απαιτήσεις ή περιορισμοί εύρους ζώνης [6]. Ωστόσο, οι πάροχοι υπηρεσιών και οι χρήστες έχουν βελτιστοποιήσει τον έλεγχο της υποδομής και της ασφάλειας. Μια επιχείρηση μπορεί να επιλέξει τη λύση του ιδιωτικού cloud, στην περίπτωση που η οργάνωσή της δεν της επιτρέπει να φιλοξενήσει εξ αποστάσεως τα δεδομένα της και ως εκ τούτου, η χρήση του cloud της επιτρέπει τη βελτίωση της χρήσης και της αυτοματοποίησης των πόρων της [10].

Ανάμεσα στα πλεονεκτήματα ενός ιδιωτικού cloud, τα σημαντικότερα αφορούν τα εξής [34]:

1) ***Ασφάλεια***: Η ασφάλεια του cloud είναι υπό τον έλεγχο της επιχείρησης. Όμως, παρόλο που το συγκεκριμένο μοντέλο ανάπτυξης cloud θεωρείται ως το πιο ασφαλές, η τεράστια ποικιλία διαφορετικών τύπων ανάπτυξης και επιπέδων ασφάλειας που υπάρχουν στα ιδιωτικά περιβάλλοντα φιλοξενίας, μπορεί να επηρεάσει την ασφάλεια των ιδιωτικών cloud. Στην πραγματικότητα, ένα ιδιωτικό cloud είναι εξίσου επιρρεπές σε κινδύνους ασφαλείας όσο ένα δημόσιο. Η μόνη διαφορά είναι ότι ένα δημόσιο cloud μπορεί να είναι πιο ελκυστικό για επίθεση από ένα ιδιωτικό, καθώς περιέχει μεγαλύτερη ποσότητα δεδομένων.

2) ***Απόδοση***: Εάν ένα ιδιωτικό cloud αναπτυχθεί εντός του τείχους προστασίας μιας επιχείρησης, η απόδοσή του είναι μεγαλύτερη σε σύγκριση με αυτή ενός cloud που αναπτύσσεται σε δημόσιο περιβάλλον.

3) ***Έλεγχος και ευελιξία***: Τα ιδιωτικά cloud είναι περισσότερο ελεγχόμενα από ότι τα δημόσια και ως εκ τούτου η ανάπτυξη νέων εφαρμογών και η πραγματοποίηση αλλαγών μπορεί να γίνει με γρήγορο τρόπο.

Τα ιδιωτικά cloud παρουσιάζουν όμως και κάποια μειονεκτήματα, τα σημαντικότερα από τα οποία αφορούν τα εξής [34]:

1) ***Πρόσθετη συντήρηση***: Εάν ένα ιδιωτικό cloud δεν συντηρείται από τον προμηθευτή λογισμικού, τότε είναι απίθανο η επιχείρηση να επωφεληθεί από τις τακτικές ενημερώσεις που συχνά σχετίζονται με τις σύγχρονες εφαρμογές SaaS.

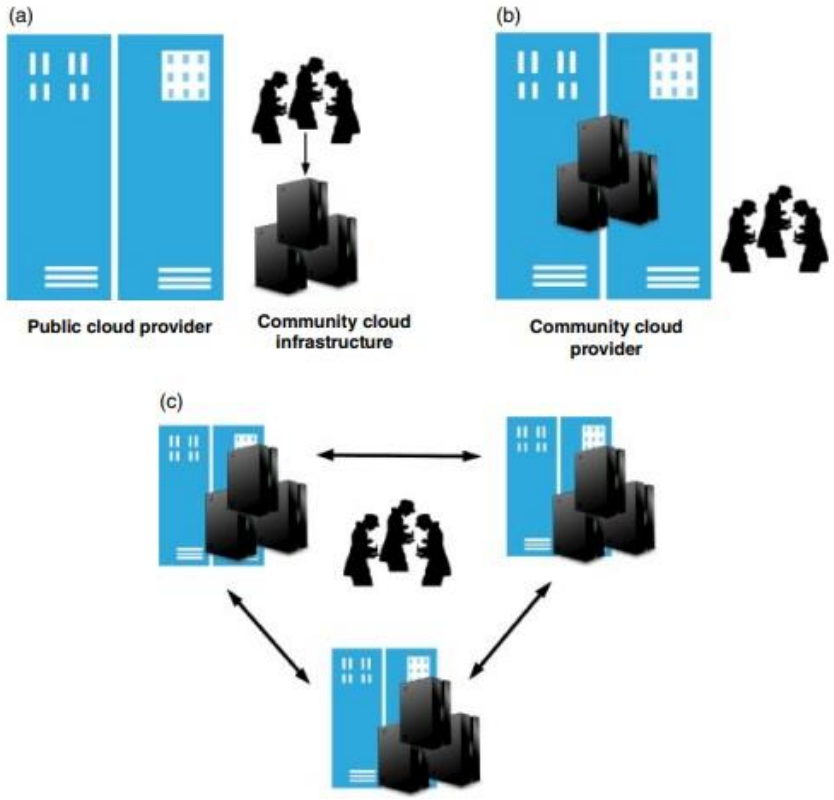
2) ***Υψηλότερο κόστος***: Όλα όσα σχετίζονται με ένα ιδιωτικό cloud είναι πιο ακριβά. Στην περίπτωση του ιδιωτικού cloud, η επιχείρηση πρέπει να αγοράσει την υποδομή ή αυτή να μισθωθεί από κάποιον προμηθευτή. Και στις δυο περιπτώσεις, τα έξοδα είναι μεγαλύτερα από ότι για το δημόσιο cloud. Επίσης το κόστος διαχείρισης του ιδιωτικού cloud είναι υψηλότερο.

2.4.3 Κοινοτικά cloud

Τα κοινοτικά (community) cloud δεν θα πρέπει να συγχέονται με τα δημόσια cloud. Στα κοινοτικά cloud, οι πόροι διατίθενται για πολλά άτομα ή ομάδες που έχουν κοινά ενδιαφέροντα, σε αντίθεση με τα δημόσια cloud, στα οποία οι χρήστες δεν έχουν κοινά ενδιαφέροντα. Η υπολογιστική υποδομή ενός κοινοτικού cloud μπορεί να είναι τοπική ή απομακρυσμένη. Οι πόροι του cloud, ανήκουν και διαχειρίζονται από έναν ή περισσότερους από τους συνεργάτες της κοινότητας, σε αντίθεση με ένα δημόσιο cloud, όπου οι πόροι ανήκουν και διαχειρίζονται από έναν μεμονωμένο πάροχο/ιδιοκτήτη [35].

Το πλεονέκτημα ενός κοινοτικού cloud έγκειται στο να μπορεί να προσφέρει βελτιστοποιημένες λύσεις cloud σε συγκεκριμένες κοινότητες χρηστών. Το πλεονέκτημα αυτό προκύπτει από το γεγονός ότι όλα τα μέλη της κοινότητας έχουν κοινά σημεία απαιτήσεων, όσον αφορά, για παράδειγμα, τις υπηρεσίες cloud που χρησιμοποιεί η κοινότητα ή τις ανάγκες απόδοσης του cloud [35].

Η υλοποίηση των κοινοτικών cloud μπορεί να επιτευχθεί με διάφορους τρόπους, ανάλογα με τις εκάστοτε απαιτήσεις. Στην εικόνα 2.6 παρουσιάζονται κάποιες από αυτές τις πιθανές αρχιτεκτονικές. Μια κοινή προσέγγιση αφορά τη δημιουργία μιας ξεχωριστής υποδομής από κάποιον πάροχο δημόσιου cloud και την ανάπτυξη ειδικών υπηρεσιών για μια συγκεκριμένη κοινότητα, παρέχοντας μια κάθετα ολοκληρωμένη λύση για αυτήν την αγορά. Μια άλλη επιλογή αφορά τη χρήση ενός παρόχου υπηρεσιών για τη δημιουργία λύσεων cloud αποκλειστικά για τη συγκεκριμένη κοινότητα. Τέλος μια τρίτη περίπτωση είναι τα ίδια τα μέλη της κοινότητας να έχουν τεχνογνωσία σε υποδομές cloud να ενώσουν τα ιδιωτικά τους cloud και να παρέχουν συλλογικά υπηρεσίες cloud στην κοινότητα [35].



Εικόνα 2.6: Αρχιτεκτονικές υλοποίησης κοινοτικού cloud (α) με χρήση παρόχου δημόσιου cloud, (β) με δημιουργία λύσεων cloud αποκλειστικά για την κοινότητα και (γ) από τα ίδια τα μέλη της κοινότητας [35]

2.4.4 Υβριδικό cloud

Ένα υβριδικό cloud αποτελεί συνδυασμό περισσότερων του ενός από τα παραπάνω μοντέλα ανάπτυξης [36]. Παρά τον υβριδικό χαρακτήρα του cloud, τα υβριδικά cloud περιλαμβάνουν ένα πλαίσιο διαχείρισης που διασφαλίζει ότι τα περιβάλλοντα εμφανίζονται ως ένα μόνο μοντέλο ανάπτυξης (δημόσιο, ιδιωτικό ή κοινοτικό). Η υιοθέτηση ενός υβριδικού cloud μπορεί να προκύψει από τις εκάστοτε απαιτήσεις για ασφάλεια, κόστος και απόδοση [35].

2.5 Οφέλη του Cloud Computing

Τα βασικά πλεονεκτήματα του μοντέλου CC, τα οποία ενισχύουν την επιλογή των χρηστών, αφορούν το μειωμένο κόστος κεφαλαίου και λειτουργίας, τη μεγάλη ευελιξία, την επεκτασιμότητα κατ' απαίτηση, την ευκολότερη και ταχύτερη ανάπτυξη εφαρμογών, την ευκολία στη χρήση και τη δυνατότητα διάθεσης ενός τεράστιου όγκου υπολογιστικών πόρων για κάθε είδους εφαρμογή ή χρήση [37]. Εξαιτίας όλων αυτών των οφελών που μπορεί να παρέχει η χρήση του cloud, πολλές εφαρμογές, όπως το email, η δημιουργία εγγράφων γραφείου και η αποθήκευση δεδομένων, έχουν κάνει ήδη στροφή προς το συγκεκριμένο μοντέλο υπολογιστικής [35].

Το CC απαλλάσσει τους χρήστες και τις επιχειρήσεις από τους περιορισμούς των τοπικών υπολογιστικών πόρων, επιτρέποντάς τους την πρόσβαση σε τεράστιο όγκο υπολογιστικών πόρων και υπολογιστικής ισχύος που μπορούν να βρεθούν σε ένα

περιβάλλον cloud. Για να κάνουν οι χρήστες χρήση των πόρων cloud από οπουδήποτε στον κόσμο και ανά πάσα στιγμή, το μόνο που χρειάζεται είναι μια σύνδεση στο Διαδίκτυο και ένα πρόγραμμα περιήγησης στον Ιστό. Ένα περιβάλλον cloud επιτρέπει στους χρήστες την εκτέλεση ακόμα και υπολογιστικά απαιτητικών εφαρμογών ή εφαρμογών που απαιτούν μεγάλους αποθηκευτικούς χώρους δεδομένων, καθώς όλες οι υπολογιστικές και αποθηκευτικές τους ανάγκες προέρχονται από το cloud [38].

Τα δημόσια cloud εξαλείφουν σημαντικά τα έξοδα για αγορά κατάλληλου hardware υλικού και για χρήση νόμιμων λογισμικών, όπως επίσης και τα ζητήματα συντήρησης και αναβάθμισης του hardware υλικού και λογισμικού από τους χρήστες. Οι εφαρμογές cloud μπορούν να αναπτυχθούν άμεσα και ταυτόχρονα σε χιλιάδες χρήστες σε διαφορετικές τοποθεσίες σε όλο τον κόσμο, ενώ παράλληλα μπορούν να ενημερώνονται τακτικά και εύκολα. Επιπλέον, καθώς τα cloud παρέχουν βελτιωμένη επιχειρηματική λειτουργία και ασφάλεια στα δεδομένα, είναι ιδιαίτερα ελκυστικά για μικρές και μεσαίες επιχειρήσεις, καθώς και για επιχειρήσεις σε επιρρεπείς σε καταστροφές περιοχές [39]. Οι νεοσύστατες εταιρείες και οι προγραμματιστές εφαρμογών μπορούν να χρησιμοποιήσουν τα περιβάλλοντα cloud για να δοκιμάσουν τις ιδέες τους, χωρίς να πρέπει να επενδύσουν για τη δημιουργία δικής τους υποδομής [35].

2.6 Εμπόδια που αποτρέπουν την ευρεία υιοθέτηση του Cloud Computing

Παρά τα όποια πλεονεκτήματα του μοντέλου CC, η ύπαρξη ορισμένων εμποδίων μπορεί να αποτρέπουν ή να καθυστερούν την ευρεία υιοθέτησή του από τις επιχειρήσεις. Ορισμένα από αυτά τα εμπόδια είναι τα εξής [40]:

1) ***Εσωτερικά επιχειρησιακά ζητήματα***: Ένα από τα πλεονεκτήματα του μοντέλου CC είναι ότι μπορεί να μειώσει τον αριθμό των εργασιών που εκτελούνται στα back-end συστήματα πληροφορικής. Αυτό σημαίνει ότι το τεχνικό προσωπικό μιας επιχείρησης ασχολείται περισσότερο με τις front-end εφαρμογές. Αποτέλεσμα όλων αυτών είναι η εν δυνάμει σημαντική μείωση του προσωπικού του τμήματος πληροφορικής της επιχείρησης. Ως εκ τούτου, οι τεχνικοί των τμημάτων πληροφορικής μιας επιχείρησης μπορούν να θεωρήσουν το CC ως απειλή για την ίδια τους την απασχόληση στην επιχείρηση [41].

2) ***Προκλήσεις για την ασφάλεια και την προστασία του απορρήτου***: Τα ζητήματα ασφάλειας και απορρήτου που σχετίζονται με το cloud αποτελούν σοβαρούς προβληματισμούς για πολλές επιχειρήσεις. Πολλές επιχειρήσεις θεωρούν τις προκλήσεις ασφάλειας ως εμπόδια που δεν μπορούν να εξαλειφθούν, αλλά ούτε δέχονται ότι υπάρχει κάποια αποτελεσματική λύση για την αντιμετώπισή τους. Τέτοιες επιχειρήσεις δεν λαμβάνουν υπόψη τους τα οφέλη από την υιοθέτηση της τεχνολογίας [4].

3) ***Αξιοπιστία και εμπιστοσύνη***: Οι διακοπές λειτουργίας του cloud που έχουν αντιμετωπίσει κατά καιρούς πάροχοι, όπως η Google και το Amazon, έχουν γίνει

γνωστές μέσω πολλών δημοσιεύσεων. Αυτό έχει αποθαρρύνει πολλές επιχειρήσεις από την υιοθέτηση της τεχνολογίας που είχαν μπει στη διαδικασία στροφής τους προς τα περιβάλλοντα cloud. Αυτή η έλλειψη εμπιστοσύνης προς το μοντέλο CC εμποδίζει την πλήρη υιοθέτησή του [42].

4) ***Υλοποίηση και διαλειτουργικότητα***: Παρά τα τόσα χρόνια ύπαρξης του μοντέλου, ακόμα υπάρχει έλλειψη κοινά αποδεκτών προτύπων διεπαφών, διαλειτουργικότητας και συναφών τεχνικών προτύπων που να επιτρέπουν τη διαλειτουργικότητα μεταξύ των ιδιωτικών cloud, των δημόσιων με τα ιδιωτικά cloud, κ.ο.κ. [29].

5) ***Συμφωνίες Επιπέδου Υπηρεσιών (SLA) και Ποιότητα Υπηρεσιών (QoS)***: Εκτός από κοινά αποδεκτά πρότυπα, η κατάλληλη ύπαρξη, από άκρο σε άκρο και καθόλη τη διάρκεια του κύκλου ζωής των υπηρεσιών cloud, συμφωνιών επιπέδου υπηρεσιών (Service Level Agreement – SLA) και ποιότητας υπηρεσιών (Quality of Service – QoS) απουσιάζει [43].

2.7 Παράγοντες απόδοσης και κόστους

Τα οφέλη του μοντέλου CC, όπως αυτά συνοψίσθηκαν σε προηγούμενη ενότητα, μπορούν να περιοριστούν από παράγοντες, όπως η απόδοση και το κόστος. Η απόδοση ενός cloud εξαρτάται από παραμέτρους, όπως οι εξής:

1) ***Ασφάλεια***: Η ασφάλεια βελτιώνει την αποδοτικότητα οποιουδήποτε συστήματος cloud και παρέχει καλύτερη απόδοση όσον αφορά την προστασία του συστήματος [44].

2) ***Ανάκτηση δεδομένων***: Τα δεδομένα που αποθηκεύονται ή διαχειρίζονται σε ένα cloud μπορεί να υπόκεινται σε σφάλματα ή απώλεια για διάφορους λόγους. Η ικανότητα και ο χρόνος που απαιτούνται για την ανάκτηση των δεδομένων επηρεάζουν την απόδοση [10].

3) ***Εύρος ζώνης δικτύου***: Όταν το εύρος ζώνης είναι πολύ μικρό, η απόδοση του cloud περιορίζεται όσον αφορά την παροχή των απαιτούμενων υπηρεσιών στον επιθυμητό χρόνο [13].

4) ***Αριθμός χρηστών***: Όταν ο αριθμός των χρηστών υπερβαίνει τη χωρητικότητα του cloud, η απόδοση των παρεχόμενων υπηρεσιών cloud επηρεάζεται [45].

5) ***Ανοχή σε σφάλματα***: Αφορά την ικανότητα των περιβαλλόντων cloud να παρέχουν υπηρεσίες ακόμη και όταν βιώνουν προβλήματα αξιοπιστίας ή ασφάλειας. Μια υψηλή ανοχή σε σφάλματα οδηγεί σε καλύτερη απόδοση του cloud [46].

6) ***Άλλοι παράγοντες***: Άλλοι παράγοντες που μπορούν να επηρεάσουν την απόδοση του cloud μπορεί να αφορούν προβλήματα κλιμάκωσης, καθυστέρησης, πλεονασμού, φόρτου εργασίας και ισχύος επεξεργαστή [47].

Όσον αφορά το κόστος των υπηρεσιών cloud, οι Rosati και συν. (2018) πρότειναν τον υπολογισμό του συνολικού κόστους ιδιοκτησίας (Total Cost of Ownership - TCO). Το κόστος TCO περιλαμβάνει όλα τα κόστη των υπηρεσιών cloud καθόλη τη διάρκεια

ζωής τους, από την αγορά έως τη διάθεση. Το κόστος TCO κατηγοριοποιείται ως άμεσο ή έμμεσο. Το άμεσο κόστος περιλαμβάνει τα τέλη αδειοδότησης του hardware υλικού και του λογισμικού, τα κόστη χρησιμότητας που σχετίζονται με το εύρος ζώνης και τους πόρους, καθώς και το κόστος που σχετίζεται με τη διαχείριση των υπηρεσιών. Το έμμεσο κόστος περιλαμβάνει το κόστος απασχόλησης του προσωπικού που συμμετέχει στο συντονισμό των εφαρμογών cloud και των τοπικών εφαρμογών, καθώς και τη διαπραγμάτευση και τη διαχείριση των συμβάσεων παροχής υπηρεσιών cloud [48].

3 Ζητήματα Ασφάλειας

3.1 Η σημασία της ασφάλειας για το Cloud Computing

Με βάση τα όσα αναφέρθηκαν στο προηγούμενο κεφάλαιο, προκύπτει το συμπέρασμα ότι ένα cloud μπορεί να είναι ευέλικτο και οικονομικά αποδοτικό. Σε μια υποδομή cloud, οι ευαίσθητες πληροφορίες των πελατών διατηρούνται σε γεωγραφικά διασκορπισμένες πλατφόρμες cloud, υπό τον άμεσο έλεγχο, όμως του cloud και όχι του πελάτη. Αυτό σημαίνει ότι η διατήρηση της ασφάλειας των δεδομένων των χρηστών στο πλαίσιο του cloud αποτελεί πολύ σημαντική διαδικασία, καθώς οι πόροι του cloud (λογισμικό, πλατφόρμες και υποδομές) παρουσιάζουν αρκετά τρωτά σημεία που μπορούν εύκολα να χρησιμοποιηθούν από κακόβουλα μέρη για παραβιάσεις, υποκλοπές, παράνομες διανομές ή ακόμη και καταστροφές τόσο των ίδιων των υποδομών όσο και των δεδομένων που περιλαμβάνουν [49]. Η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που είναι αποθηκευμένα στα περιβάλλοντα cloud, μπορεί να ελαχιστοποιηθεί μόνο μέσω της αύξησης της ασφάλειας [50].

Παρά τα όποια οφέλη του, τα ζητήματα ασφάλειας που παρουσιάζει το μοντέλο του CC αποτελούν και ένα από τα βασικότερα εμπόδια ως προς την πλήρη υιοθέτησή του από εταιρείες, επιχειρήσεις και οργανισμούς. Μετά την επιλογή του μοντέλου CC για χρήση σε επιχειρηματικές εφαρμογές, η ευθύνη για τη διαχείριση και προστασία των δεδομένων της επιχείρησης ανήκει αποκλειστικά στον εκάστοτε πάροχο υπηρεσιών [51]. Η απώλεια και ο χειρισμός δεδομένων από άγνωστες πηγές μπορεί να αποτραπεί μέσω της δημιουργίας ασφαλών υπολογιστικών περιβαλλόντων, τα οποία μπορούν να επιτευχθούν μέσω συστημάτων που εφαρμόζονται για τον έλεγχο της αποθήκευσης και της χρήσης των δεδομένων. Ένα ασφαλές υπολογιστικό περιβάλλον είναι σε θέση να μειώσει την όποια ζημιά μπορεί να προκληθεί από κακόβουλα λογισμικά [52]. Εκτός όμως από την αυξημένη ασφάλεια, ένα ασφαλές υπολογιστικό περιβάλλον μπορεί να μειώσει δραστικά και το κόστος χρήσης των υπηρεσιών cloud, καθώς σε ένα τέτοιο περιβάλλον η ύπαρξη μεγαλύτερης ασφάλειας βελτιώνει την απόδοση και μειώνει τις πιθανότητες ζημιάς σε δεδομένα, λογισμικό και hardware υλικό [10].

3.2 Απαιτήσεις ασφάλειας Cloud Computing

Δεδομένου ότι το μοντέλο CC επιτυγχάνει συγκέντρωση πόρων στους οποίους μπορούν να έχουν ταυτόχρονη πρόσβαση πολλοί χρήστες, με βάση τα όσα αναφέρθηκαν στην προηγούμενη ενότητα, τα δεδομένα που αποθηκεύονται ή διαχειρίζονται σε ένα cloud είναι πιθανό να αντιμετωπίσουν ζητήματα ασφάλειας. Επομένως, κάθε cloud θα πρέπει να περιλαμβάνει ένα μοντέλο ασφάλειας έτσι ώστε να είναι δυνατή η πλήρωση των βασικών χαρακτηριστικών της επεκτασιμότητας και της πολυμίσθωσης, σε συνδυασμό με την απαιτούμενη ύπαρξη εμπιστοσύνης [53].

Κατά την υιοθέτηση του CC από τις επιχειρήσεις, μέρος του ελέγχου των πληροφοριών και των υποδομών των επιχειρήσεων μεταφέρεται στα συστήματα CC

και τους παρόχους τους. Στην περίπτωση αυτή, η εκάστοτε επιχείρηση θα πρέπει να εμπιστεύεται στον αντίστοιχο πάροχο υπηρεσιών cloud αλλά ταυτόχρονα θα πρέπει να είναι σε θέση να επαληθεύει τις όποιες διαδικασίες πραγματοποιούνται στο cloud. Οι έννοιες της εμπιστοσύνης και της επαλήθευσης των διαδικασιών αποτελούν βασικές αρχές που θα πρέπει να ικανοποιούνται, ώστε να επιτυγχάνεται μεγαλύτερη ασφάλεια των δεδομένων [54].

Σύμφωνα με τους Hussain και συν. (2017), υπάρχει μία σχέση μεταξύ των παρεχόμενων υπηρεσιών cloud και των απαιτήσεων ασφαλείας του cloud (Πίνακας 3.1). Οι απαιτήσεις ασφαλείας περιλαμβάνουν τις έννοιες του ελέγχου ταυτότητας, της εξουσιοδότησης, της κρυπτογράφησης των δεδομένων, της διατήρησης του απορρήτου των δεδομένων και της πολυμίσθωσης και κρίνονται υποχρεωτικές για την επίτευξη ακεραιότητας και συνοχής στα συστήματα cloud [55].

Πίνακας 3.1: Αντιστοίχιση παρεχόμενων υπηρεσιών cloud και απαιτήσεις ασφάλειας cloud [55]

	Απαιτήσεις ασφάλειας				
Παρεχόμενες υπηρεσίες cloud	**Έλεγχος ταυτότητας**	**Εξουσιοδότηση**	**Κρυπτογράφηση δεδομένων**	**Διατήρηση απορρήτου δεδομένων**	**Πολυμίσθωση**
Προστασία δεδομένων	–	–	✓	✓	–
Διεπαφές API	✓	✓	–	–	–
Πύλες Ιστού	✓	✓	–	–	–
Υπηρεσίες ανάπτυξης	–	✓	✓	✓	–
Εικονικοποίηση hardware υλικού	–	–	–	✓	✓
Εικονικοποίηση λογισμικού	–	✓	–	–	✓
Εικονικοποίηση	–	✓	–	–	✓
Υπηρεσίες UC	–		–	–	✓

Στα κατανεμημένα συστήματα, η προστασία των δεδομένων επιτυγχάνεται μέσω των τεχνικών κρυπτογράφησης και κατακερματισμού των δεδομένων. Έτσι, η υπηρεσία προστασίας των δεδομένων εξαρτάται από τεχνικές κρυπτογράφησης και πολιτικές διατήρησης του απορρήτου. Εάν οι υπηρεσίες προστασίας των δεδομένων ή οι υπηρεσίες Διαδικτύου δεχθούν κάποια επίθεση, τότε υπάρχει κίνδυνος παραβίασης των τεχνικών αυτών, καθώς ο επίδοξος εισβολέας θα προσπαθήσει να σπάσει τις πολιτικές κρυπτογράφησης και κατακερματισμού. Ωστόσο, η φυσική αποθήκευση δεδομένων δεν απειλείται σε αυτήν την περίπτωση και έτσι ο παράγοντας κινδύνου που σχετίζεται με μια πιθανή επίθεση εναντίον της κρίνεται μεσαίας σπουδαιότητας.

Αν οι διεπαφές API και οι πύλες ιστού δεχθούν κάποιο είδος επίθεσης, θα παραβιαστούν οι απαιτήσεις ελέγχου ταυτότητας και εξουσιοδότησης. Οι διεπαφές API και οι πύλες ιστού παρέχουν μια πύλη πρόσβασης (gateway) στα συστήματα cloud και επομένως σε οποιαδήποτε επίθεση εναντίον τους, οι επιτιθέμενοι μπορούν εύκολα να παραβιάσουν τα συστήματα cloud. Ωστόσο, καθώς τα διαπιστευτήρια ελέγχου ταυτότητας και εξουσιοδότησης λήγουν μετά από κάθε συνεδρία, ο παράγοντας κινδύνου που σχετίζεται με αυτές τις υπηρεσίες κρίνεται σχετικά μικρός.

Οι υπηρεσίες ανάπτυξης παρέχουν έναν τρόπο δημιουργίας άλλων υπηρεσιών cloud από τους ίδιους τους πελάτες. Με κακόβουλη πρόσβαση σε αυτές τις υπηρεσίες, μπορούν να εκτελεστούν κακόβουλα script και κώδικες. Οι επιθέσεις κατά των υπηρεσιών ανάπτυξης μπορούν να παραβιάσουν τις απαιτήσεις κρυπτογράφησης δεδομένων, πολυμίσθωσης και ελέγχου ταυτότητας. Έτσι, κρίνεται ότι ο κίνδυνος από τις επιθέσεις κατά των υπηρεσιών ανάπτυξης είναι πολύ υψηλός.

Η εικονικοποίηση προσφέρει πολλά πλεονεκτήματα τα οποία όμως εξαρτώνται σε μεγάλο βαθμό από το είδος των απειλών κατά του cloud, για παράδειγμα τη μη εξουσιοδοτημένη πρόσβαση που μπορεί να έχει ένας μεγάλος αριθμός πελατών σε έναν μόνο πόρο. Η επίθεση κατά της εικονικοποίησης του hardware υλικού ενδέχεται να παραβιάσει τις απαιτήσεις πολυμίσθωσης και της διατήρησης του απορρήτου των δεδομένων και επομένως αποτελεί υψηλό παράγοντα κινδύνου. Εάν πραγματοποιηθούν επιθέσεις κατά της εικονικοποίησης του λογισμικού και των υπηρεσιών UC, θα υπάρξει σοβαρή απειλή για τις απαιτήσεις της πολυμίσθωσης και της εξουσιοδότησης. Οι επιθέσεις κατά τις πολυμίσθωσης θέτουν σε κίνδυνο το λογικό διαχωρισμό της πρόσβασης πολλών πελατών σε έναν μόνο πόρο, και ως εκ τούτου, ο κίνδυνος από την εξαπόλυσή τους είναι υψηλός [55].

3.3 Κατηγορίες ασφάλειας Cloud Computing

Σύμφωνα με τον Krishnan (2017), η ασφάλεια του CC μπορεί να ταξινομηθεί στις εξής κατηγορίες (Εικ.3.1) [10]: ταυτότητας, πληροφοριών, υποδομής, δικτύου και λογισμικού.

Εικόνα 3.1: Κατηγορίες ασφάλειας CC

3.3.1 Ασφάλεια ταυτότητας

Σύμφωνα με τους Indu, Anand & Bhaskar (2018), η ασφάλεια ταυτότητας (identity security) ορίζεται ως η ασφάλεια και η επιχειρησιακή πειθαρχία που επιτρέπει στα

σωστά άτομα να έχουν πρόσβαση στους σωστούς πόρους τις κατάλληλες στιγμές και για τους σωστούς λόγους [56]. Εξασφαλίζει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων και των εφαρμογών ενώ αυξάνει την προσβασιμότητά τους στους κατάλληλους χρήστες. Η ολοκληρωμένη διαχείριση ταυτότητας, οι υπηρεσίες ελέγχου ταυτότητας τρίτων και η ταυτότητα αποτελούν τα βασικά στοιχεία ασφάλειας ταυτότητας στο cloud. Η διαχείριση της ασφάλειας ταυτότητας διαθέτει δυνατότητες που θα πρέπει να διατίθενται τόσο στους χρήστες όσο και στα στοιχεία υποδομής του CC [57]. Οι ταυτότητες των χρηστών πρέπει να διαχειρίζονται με τέτοιο τρόπο που να δημιουργεί και το αίσθημα της εμπιστοσύνης.

Η ασφάλεια ταυτότητας στο μοντέλο CC απαιτεί την ύπαρξη ισχυρών μηχανισμών ελέγχου ταυτότητας και εξουσιοδότησης. Αυτό σημαίνει ότι οι μηχανισμοί αυτοί θα πρέπει να ελέγχουν πολλά περισσότερα στοιχεία από το όνομα χρήστη και τον κωδικό πρόσβασης. Για το λόγο αυτό, ενδέχεται να απαιτείται η υιοθέτηση μηχανισμών που να περιλαμβάνουν ισχυρή πιστοποίηση και έλεγχο ταυτότητας βάσει κινδύνων, αλλά και παρακολούθηση της συμπεριφοράς των χρηστών που θα επιτρέπει την εκτίμηση του επιπέδου επικινδυνότητας ενός αιτήματος χρήστη. Οι δυνατότητες ελέγχου ταυτότητας πρέπει να είναι σταθερές καθόλη τη διάρκεια του κύκλου ζωής της υποδομής και των δεδομένων του cloud. Ιδιαίτερα στην περίπτωση διαχείρισης ευαίσθητων δεδομένων και απαιτήσεων συμμόρφωσης, απαιτούνται ισχυρότερες δυνατότητες εξουσιοδότησης [10].

3.3.2 Ασφάλεια πληροφοριών

Σύμφωνα με τους Alhassan & Adjei-Quaye (2017), η ασφάλεια πληροφοριών (information security) ορίζεται ως ένα σύνολο στρατηγικών για τη διαχείριση των διαδικασιών, των εργαλείων και των πολιτικών που είναι απαραίτητες για την πρόληψη, τον εντοπισμό, την τεκμηρίωση και την αντιμετώπιση απειλών για ψηφιακές και μη ψηφιακές πληροφορίες [58]. Για την επίτευξη ασφάλειας των πληροφοριών απαιτείται η δημιουργία ενός συνόλου επιχειρηματικών διαδικασιών που θα προστατεύουν τις πληροφορίες ανεξάρτητα από τον τρόπο μορφοποίησης τους και την κατάσταση στην οποία βρίσκονται (μεταφορά, επεξεργασία ή αποθήκευση) [59]. Για το λόγο αυτό, οι έλεγχοι πρόσβασης στο hardware υλικό και λογισμικό των cloud αλλά και οι έλεγχοι ταυτότητας θα πρέπει να στοχεύουν στην προστασία των δεδομένων [10].

Η ασφάλεια των δεδομένων σε ένα cloud θα πρέπει επίσης να περιλαμβάνει την απομόνωσή τους, ιδιαίτερα στην περίπτωση των δημόσιων cloud. Διαφορετικοί βαθμοί απομόνωσης δεδομένων μπορούν να επιτευχθούν μέσω εικονικοποίησης, κρυπτογράφησης και ελέγχου πρόσβασης. Κάτι τέτοιο διασφαλίζει την προστασία των δεδομένων από μη εξουσιοδοτημένα άτομα [60]. Η απομόνωση των δεδομένων είναι επίσης απαραίτητη σε περιβάλλοντα cloud πολυμίσθωσης, όπου οι χρήστες δεν μπορούν να βλέπουν ή δεν μοιράζονται τα δεδομένα άλλων χρηστών, αλλά μπορούν να μοιράζονται μεταξύ τους πόρους ή εφαρμογές σε περιβάλλον εκτέλεσης, ακόμη και αν δεν ανήκουν στην ίδια επιχείρηση [10].

Οι τεχνολογίες Trusted Computing χρησιμοποιούνται για την οικοδόμηση εμπιστοσύνης σε υποδομές πολυμίσθωσης και επεκτείνονται για την υποστήριξη της εικονικοποίησης [61]. Η εικονικοποίηση χρησιμοποιείται στο μοντέλο CC για τον έλεγχο και την αναφορά της ακεραιότητας μιας συγκεκριμένης μηχανής VM [62]. Οι διάφορες αρχές που χρησιμοποιούνται για τη βελτίωση της ασφάλειας των πληροφοριών στην υποδομή cloud μέσω εικονικοποίησης και υπολογιστικής είναι [10]: μειωμένη αξιόπιστη υπολογιστική βάση, ξεχωριστά στοιχεία διαχείρισης και διαχωρισμό της επιβολής πολιτικής από τον χώρο εφαρμογών. Σύνθετα και πολυάριθμα στοιχεία κώδικα είναι πιθανό να υπόκεινται σε σφάλματα που δημιουργούν ευπάθειες. Επομένως, μια τελευταία απαίτηση της ασφάλειας πληροφοριών αφορά τη μείωση του μεγέθους του αξιόπιστου κώδικα. Με απλούστερο κώδικα και λιγότερες γραμμές κώδικα, θα εμφανιστούν λιγότερα σφάλματα [63].

3.3.3 Ασφάλεια υποδομής

Η εξασφάλιση ότι μια υποδομή cloud είναι ασφαλής είναι απολύτως απαραίτητη για μία επιχείρηση. Παρόλα αυτά, η υλοποίηση μιας αξιόπιστης εικονικής και φυσικής υποδομής ενός cloud αποτελεί πραγματική πρόκληση και η εύρεση ενός αξιόπιστου τρίτου μέρους δεν επαρκεί για τις κρίσιμες επιχειρηματικές διαδικασίες [64]. Η ασφάλεια της υποδομής θα πρέπει να διασφαλίζεται με τέτοιο τρόπο, ώστε η οποιαδήποτε τυχόν κακόβουλη εισβολή να μην επιτρέπει στον επίδοξο επιτιθέμενο να έχει πρόσβαση σε όλα τα συστήματα της επιχείρησης.

Στις αξιόπιστες υποδομές, το λογισμικό που διατηρεί τον διαχωρισμό και διαχειρίζεται κρίσιμα στοιχεία και πολιτικές του συστήματος θα πρέπει να ελαχιστοποιηθεί. Επίσης, θα πρέπει να καθοριστεί το ελάχιστο σύνολο υπηρεσιών που απαιτούνται για την υποστήριξη της διαχείρισης των μηχανών VM [65]. Η ασφάλεια υποδομής του cloud απαιτεί επίσης τη διατήρηση διαχωρισμού των βασικών μερών του, όπως είναι οι λογαριασμοί των χρηστών, οι διακομιστές, οι υπερεπόπτες, ο χώρος αποθήκευσης, οι βάσεις δεδομένων, το δίκτυο και οι περιέκτες (containers) [66]. Ο διαχωρισμός των συστατικών διαχείρισης επιτρέπει στα προγράμματα οδήγησης του δικτύου να αποτρέπουν την εύκολη πρόσβαση σε προγράμματα οδήγησης αποθήκευσης ή κλειδιά κρυπτογράφησης. Ο διαχωρισμός της επιβολής πολιτικών από τον χώρο εφαρμογών καθιστά δυνατή τη δημιουργία περιεκτών, εντός των οποίων οι εφαρμογές μπορούν να τρέχουν και να ελέγχουν τη φύση του εκάστοτε περιέκτη, μέσω καθορισμού πολιτικών εντός της υποδομής. Οι περιέκτες, σε κάθε περίπτωση, δημιουργούνται με δυνατότητες που δεν ελέγχονται από την εκτέλεση του λογισμικού εφαρμογών. Τέλος, ο διαχωρισμός του χώρου ελέγχου (audit) από τον χώρο της εφαρμογής προστατεύει τα αρχεία ελέγχου από παραβιάσεις [67]. Η επίτευξη όλων των παραπάνω, αποπνέει ένα αίσθημα εμπιστοσύνης προς τους καταναλωτές ότι το σύστημα είναι αξιόπιστο [68].

3.3.4 Ασφάλεια δικτύου

Η ασφάλεια δικτύου αποτελεί βασική απαίτηση του μοντέλου CC. Περιλαμβάνει τη λήψη προληπτικών μέτρων, σε φυσικό επίπεδο και επίπεδο λογισμικού, για την

προστασία της υποκείμενης υποδομής από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση, δυσλειτουργία, τροποποίηση ή καταστροφή, δημιουργώντας έτσι μια ασφαλή πλατφόρμα για υπολογιστές, χρήστες και προγράμματα, ώστε να εκτελέσουν τις επιτρεπόμενες λειτουργίες τους εντός ενός ασφαλούς περιβάλλοντος [69].

Τα ζητήματα του επιπέδου του δικτύου μπορούν να επηρεάσουν άμεσα ένα σύστημα cloud, μέσω μεταβολής του εύρους ζώνης και αύξησης της συμφόρησης της κυκλοφορίας δεδομένων. Στις πλατφόρμες κινητής τηλεφωνίας, πολλοί χρήστες cloud χρησιμοποιούν smartphone για πρόσβαση στις εφαρμογές και τις υπηρεσίες SaaS. Στην περίπτωση αυτή, η χρήση των κινητών συσκευών δημιουργεί περισσότερα τρωτά σημεία στο σύστημα τα οποία μπορούν να αποτελέσουν σημεία εισόδου επιβλαβών κακόβουλων λογισμικών [70].

Κατά τον σχεδιασμό της ασφάλειας του δικτύου cloud προκύπτουν διάφορα ζητήματα. Για παράδειγμα, ένα τείχος προστασίας περιέχει και διαχειρίζεται όλες τις συνδέσεις TCP του δικτύου. Αν υποτεθεί ότι μια μηχανή VM βρίσκεται έξω από το τείχος προστασίας και είναι προσβάσιμη από έναν εξωτερικό πελάτη. Οποιαδήποτε μετακίνηση της μηχανής VM σε άλλο μέρος του cloud θα αλλάξει τη διαδρομή δρομολόγησης του τείχους προστασίας. Σε αυτήν την περίπτωση και στα cloud πολυμίσθωσης, ένα κακόβουλο λογισμικό μπορεί να εξαπλωθεί από το ένα δίκτυο στο άλλο [70].

3.3.5 Ασφάλεια λογισμικού

Όλα τα λογισμικά που σχεδιάζονται και αναπτύσσονται απαιτούν εγγυήσεις ασφάλειας. Δεδομένου ότι η έννοια της εγγυημένης πλήρους ασφάλειας είναι ανύπαρκτη, στόχος κατά το σχεδιασμό είναι η δημιουργία ενός όσο το δυνατόν πιο ασφαλούς λογισμικού, που να του παρέχει έναν αρκετά υψηλό βαθμό προστασίας από επιθέσεις [71].

Οι εκτιμήσεις ασφαλείας ενός λογισμικού θα πρέπει να ξεκινούν ήδη από τη σύλληψη της ιδέας του και να συνεχίζουν στις φάσεις σχεδιασμού και ανάπτυξης, σχηματίζοντας με τον τρόπο αυτό έναν κύκλο ανάλυσης ασφαλείας. Κάθε μία από αυτές τις φάσεις εξαρτάται από την προηγούμενη, επιτυγχάνοντας το υψηλότερο επίπεδο ασφάλειας για το λογισμικό [72].

Οι προγραμματιστές πρέπει να ακολουθούν μια συγκεκριμένη διαδικασία ώστε να αναπτύσσουν λογισμικά με τη μέγιστη δυνατή ασφάλεια, η οποία θα πρέπει να περιλαμβάνει τη δημιουργία μιας αρχιτεκτονικής με σωστή παρακολούθηση και απομόνωση και τη δυνατότητα εξέτασης του σχεδιασμού και της εφαρμογής των λογισμικών όσον αφορά τα θέματα ασφάλειας [72]. Οι ομάδες ανάπτυξης εφαρμογών πρέπει να παράγουν έξυπνες ροές αρχείων καταγραφής. Παραδοσιακά, αυτά τα αρχεία καταγραφής χρησιμοποιούνται για την αντιμετώπιση προβλημάτων και τον εντοπισμό σφαλμάτων, αλλά ένα εξωτερικό σύστημα θα πρέπει να συνδυάσει πολλά αρχεία καταγραφής για να δημιουργήσει ένα συμβάν ασφαλείας. Μια πλήρης ροή αρχείων καταγραφής περιλαμβάνει περισσότερες λεπτομέρειες που αφορούν την ασφάλεια ως

προς παραδοσιακά συμβάντα αλλά και εκείνα που παράγονται με την ενσωμάτωση των ελέγχων ασφαλείας [10].

3.4 Ευπάθειες, τρωτά σημεία και επιθέσεις κατά του Cloud Computing

Το μοντέλο CC παρουσιάζει διάφορους κινδύνους για την επιχείρηση που το έχει υιοθετήσει. Τα ζητήματα ασφάλειας των περιβαλλόντων cloud καθορίζονται σε μεγάλο βαθμό από το μοντέλο παροχής υπηρεσιών και το μοντέλο ανάπτυξης cloud που χρησιμοποιούνται. Αυτό σημαίνει ότι, για παράδειγμα, επίπεδα υψηλής ασφάλειας μπορούν να επιτευχθούν πιο εύκολα σε ιδιωτικά cloud παρά σε δημόσια [40]. Τα ζητήματα ασφάλειας των περιβαλλόντων cloud σχετίζονται άμεσα με τις ευπάθειες και τα τρωτά σημεία που παρουσιάζει ένα cloud αλλά και με τις επιθέσεις που είναι δυνατόν να εξαπολυθούν εναντίον του. Τέτοια ζητήματα αφορούν τις εσωτερικές απειλές, τις ανασφαλείς διεπαφές API, κοινά προβλήματα της τεχνολογίας, παραβίαση λογαριασμού ή υπηρεσίας και προφίλ αγνώστου κινδύνου. Στις επόμενες υποενότητες θα αναλυθούν κάποια από αυτά τα ζητήματα, όπως επίσης και μερικές από τις σημαντικότερες επιθέσεις εναντίον των cloud, οι οποίες μπορεί να δημιουργήσουν σοβαρά προβλήματα ως προς την ασφάλειά τους.

3.4.1 Εσωτερικές απειλές

Ως εσωτερικές απειλές (malicious insider) θεωρούνται όλοι οι νυν ή πρώην υπάλληλοι μιας εταιρείας που είναι εξουσιοδοτημένοι να έχουν πρόσβαση στο δίκτυο, στο σύστημα ή στα δεδομένα της επιχείρησης και την χρησιμοποιούν για κακόβουλους σκοπούς [73]. Στην περίπτωση αυτή, τα τείχη προστασίας του δικτύου και τα συστήματα ανίχνευσης εισβολών δεν είναι σε θέση να εντοπίσουν τις δραστηριότητες μιας εσωτερικής απειλής, καθώς την θεωρούν εξουσιοδοτημένη. Στο μοντέλο CC, οι εσωτερικές απειλές με πρόσβαση σε πόρους cloud μπορούν να προκαλέσουν πολύ μεγαλύτερη ζημιά από ότι στα παραδοσιακά συστήματα αποθήκευσης δεδομένων μιας επιχείρησης, κυρίως επειδή μια τέτοιου είδους επίθεση μπορεί να επηρεάσει μεγάλο αριθμό πελατών cloud και όχι μόνο την εταιρεία του εισβολέα. Οι εσωτερικές απειλές μπορούν να επηρεάσουν σημαντικά τις παροχές υπηρεσιών, όπως η πρόσβαση σε εμπιστευτικά δεδομένα, και να αποκτήσουν τον έλεγχο των υπηρεσιών cloud χωρίς να γίνουν αντιληπτές [74].

Οι ζημιές στην επιχείρηση, ο νομισματικός αντίκτυπος και οι απώλειες παραγωγικότητας είναι μερικοί από τους τρόπους με τους οποίους μια εσωτερική απειλή μπορεί να επηρεάσει τις δραστηριότητες των εταιρειών που δέχτηκαν επίθεση. Σύμφωνα με τους Hassan και συν. (2019), οι εσωτερικές απειλές ευνοούνται από την απουσία διαφάνειας στις διεργασίες και τις διαδικασίες των παρόχων cloud [75]. Καθώς οι επιχειρήσεις υιοθετούν όλο και περισσότερο τις υπηρεσίες cloud, ο ανθρώπινος παράγοντας αποκτά ακόμη μεγαλύτερη σημασία. Επομένως, οι καταναλωτές των υπηρεσιών cloud είναι ζωτικής σημασίας να κατανοήσουν τι κάνουν οι πάροχοι για τον εντοπισμό και την άμυνα εναντίον των κακόβουλων εσωτερικών

απειλών [76]. Η απειλή μπορεί να αντιμετωπιστεί μέσω του περιορισμού της πρόσβασης σε υπηρεσίες και δεδομένα cloud, της αύξησης της διαφάνειας στις διαδικασίες ασφάλειας και διαχείρισης, συμπεριλαμβανομένης της αναφοράς συμμόρφωσης, και της ειδοποίησης σε στιγμές παραβίασης [77].

Στην περίπτωση που η εσωτερική απειλή αφορά εργαζόμενο στην εταιρεία παροχής cloud, η ζημιά που μπορεί να προκληθεί είναι μεγάλη τόσο στον πάροχο όσο και στους πελάτες του. Οι έλεγχοι που υπάρχουν για τη μείωση των επιπτώσεων των επιθέσεων από τις εσωτερικές απειλές αυτού του είδους χωρίζονται σε αυτούς στην πλευρά του πελάτη και σε αυτούς στην πλευρά του παρόχου. Οι έλεγχοι και λύσεις στην πλευρά του πελάτη περιλαμβάνουν αντίμετρα εμπιστευτικότητας και διαθεσιμότητας, ενώ αυτοί στην πλευρά του παρόχου περιλαμβάνουν μοντέλα εντοπισμού εσωτερικών απειλών, καταγραφή και νομική δέσμευση [10].

3.4.2 Ανασφαλείς διεπαφές API

Οι ανασφαλείς διεπαφές προγραμματισμού εφαρμογών (Application Programming Interface - API) αποτελούν ένα από τα πλέον κρίσιμα ζητήματα ασφάλειας του CC. Οι διεπαφές API ενδέχεται να αποτελούν έναν από τους κύριους στόχους των εγκληματιών στον κυβερνοχώρο στην προσπάθειά τους να παραβιάσουν το δίκτυο μιας εταιρείας, καθώς λειτουργούν ως δημόσια πόρτα σε οποιεσδήποτε εφαρμογές και από προεπιλογή η πρόσβαση σε αυτές θα πρέπει να επιτρέπεται εξωτερικά. Με τον τρόπο αυτό, οι επίδοξοι επιτιθέμενοι εκμεταλλεύονται τα τρωτά σημεία του συστήματος, όπως την ανεπαρκή πιστοποίηση, εξουσιοδότηση και κρυπτογράφηση [78].

Οι διεπαφές API χρησιμοποιούνται από παρόχους cloud και προγραμματιστές λογισμικού για να επιτρέπουν στους πελάτες τους να αλληλοεπιδρούν με τα δεδομένα των υπηρεσιών cloud. Αυτή τους η χρήση μπορεί να γίνει με τουλάχιστον τρεις τρόπους. Πρώτον, μπορούν να χρησιμοποιηθούν για τη συλλογή αρχείων καταγραφής από μια εφαρμογή. Δεύτερον, μπορούν να χρησιμοποιηθούν ως μέσο πρόσβασης σε μια βάση δεδομένων ή σε έναν χώρο αποθήκευσης. Τρίτον, μπορούν να χρησιμοποιηθούν για τον έλεγχο συγκεκριμένων πόρων cloud. Επιπλέον, αποτελούν τα κύρια κανάλια αλληλεπίδρασης των κινητών εφαρμογών με ιστότοπους ή υπηρεσίες back end [79]. Οι διεπαφές API μπορούν επίσης να διευκολύνουν τον έλεγχο ταυτότητας των χρηστών.

Εκτός από τις διεπαφές API, άλλες ευπάθειες που σχετίζονται με τον κώδικα περιλαμβάνουν κακές μεθοδολογίες κωδικοποίησης και δημιουργία ανεπαρκώς ασφαλή κώδικα [80].

3.4.3 Επιθέσεις υπερχείλισης buffer

Η υπερχείλιση του buffer αφορά την κατάσταση κατά την οποία τα δεδομένα που αποστέλλονται στο buffer είναι πολύ περισσότερα από τη χωρητικότητά του [81]. Κατά την εκτέλεση ενός προγράμματος, το σύστημα διαθέτει ένα τμήμα της παρακείμενης περιοχής μνήμης για την αποθήκευση διαφόρων τύπων δεδομένων, το οποίο ονομάζεται buffer. Κατά την υπερχείλιση του buffer, η οποία πραγματοποιείται με την

έλλειψη επικύρωσης των δεδομένων που είναι γραμμένα σε αυτό, το σύνολο των μη επικυρωμένων δεδομένων μεταφέρεται στην παρακείμενη μνήμη. Στην περίπτωση αυτή, το σύστημα καθίσταται πιο ευάλωτο σε επακόλουθες επιθέσεις, επιτρέποντας στους επιτιθέμενους να αναπτύξουν πιο εξελιγμένα προγράμματα που προκαλούν μεγαλύτερη ζημιά. Μια επιτυχημένη επίθεση υπερχείλισης του buffer μπορεί να τροποποιήσει τις τιμές των μεταβλητών στη μνήμη, να παραβιάσει τις διεργασίες που πραγματοποιούνται ή ακόμα και να εκτελέσει κακόβουλο κώδικα, οδηγώντας τελικά σε πλήρη έλεγχο του host [81].

Μία πιο απλή και συνηθισμένη μορφή επίθεσης υπερχείλισης του buffer αποτελεί μια τεχνική έγχυσης και ενεργοποίησης καταστροφής των εγγραφών. Ο εισβολέας εντοπίζει μια "υπερχειλίσιμη" μεταβλητή και στη συνέχεια τροφοδοτεί το πρόγραμμα με μια μεγάλη συμβολοσειρά που είναι σε θέση να υπερχειλίσει ταυτόχρονα το buffer, στην οποία έχει πραγματοποιηθεί έγχυση του κώδικα επίθεσης [10]. Οι επιτιθέμενοι χρησιμοποιούν κώδικα ειδικά σχεδιασμένο για να προκαλέσει υπερχειλίσεις του buffer [82]. Η υπερχείλιση του buffer είναι από τις χειρότερες επιθέσεις σφαλμάτων για ένα cloud, καθώς είναι δύσκολο να εντοπιστεί και να διορθωθεί. Ένας τρόπος αντιμετώπισής του είναι η έγκαιρη ανίχνευση και παρέμβαση για να διασφαλιστεί ότι προκαλείται ελάχιστη ζημιά [83].

3.4.4 Επιθέσεις ελέγχου ταυτότητας

Ο έλεγχος ταυτότητας είναι μια διαδικασία που διασφαλίζει και επιβεβαιώνει την ορθότητα και την εγκυρότητα των διαπιστευτηρίων ενός χρήστη. Η διαδικασία ξεκινά όταν ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε πληροφορίες. Ο χρήστης πρέπει να αποδείξει τα δικαιώματα πρόσβασής του και να διαθέτει την απαιτούμενη βασική ιδιότητα που έχει επιλεγεί για τη δεδομένη διαδικασία ελέγχου ταυτότητας [84]. Σε περιβάλλον cloud, ο χρήστης προσπαθεί να δημιουργήσει μια σύνδεση με υπηρεσίες cloud χρησιμοποιώντας τα δικά του διαπιστευτήρια που τον πιστοποιούν προκειμένου να του επιτραπεί η πρόσβαση σε αυτές [56].

Οι σημαντικότερες από τις επιθέσεις κατά του ελέγχου ταυτότητας σε περιβάλλον cloud είναι οι εξής [85]:

1) Επιθέσεις ωμής βίας (Brute Force Attacks): Αφορούν τις επιθέσεις εξαντλητικής δοκιμής κατά την οποία ο επιτιθέμενος αποκαλύπτει τα διαπιστευτήρια ενός χρήστη.

2) Επιθέσεις αναπαραγωγής cookie (Cookie Replay Attacks): Αφορούν τις επιθέσεις στις οποίες ο επιτιθέμενος αποκτά πρόσβαση στο σύστημα ενός χρήστη μέσω της επαναχρησιμοποίησης ενός cookie σε μια συνεδρία που έχει προηγουμένως υποκλέψει. Συνήθως τα cookies περιέχουν σημαντικές εμπιστευτικές πληροφορίες.

3) Επιθέσεις κλοπής διαπιστευτηρίων (Credential theft attacks): Αφορούν τις επιθέσεις στις οποίες ο επιτιθέμενος εκμεταλλεύεται το σύστημα και αποκτά πρόσβαση/διαπιστευτήρια μέσω υποκλοπής δεδομένων, π.χ. μέσω ηλεκτρονικού ψαρέματος (phising).

4) Επιθέσεις λεξικού (Dictionary attacks): Αφορούν τις επιθέσεις στις οποίες ο επιτιθέμενος μαντεύει τα διαπιστευτήρια του χρήστη δοκιμάζοντας μια σειρά από διαφορετικούς όρους από το λεξικό.

5) Επιθέσεις υποκλοπής δικτύου (Network eavesdropping): Αφορούν τις επιθέσεις στις οποίες ο επιτιθέμενος υποκλέπτει τα διαπιστευτήρια των χρηστών μέσω ανάγνωσης της κίνησης που δημιουργείται από τη μεταφορά δεδομένων εντός του δικτύου.

Καθώς το πρόγραμμα περιήγησης δεν μπορεί να δημιουργήσει κρυπτογραφικά έγκυρα XML token για τον έλεγχο της ταυτότητας ενός χρήστη πριν από την πρόσβασή του σε υπηρεσίες cloud, χρησιμοποιείται ένα πρωτόκολλο που περιλαμβάνει ένα αξιόπιστο τρίτο μέρος (Trusted Third Party - TTP). Ένα πρότυπο για τέτοια πρωτόκολλα είναι το Passport της Microsoft [86]. Το πρόγραμμα περιήγησης ενδέχεται να μην διαθέτει τα απαραίτητα διαπιστευτήρια, καθιστώντας αδύνατη την άμεση σύνδεση στον διακομιστή. Ο διακομιστής σύνδεσης του Passport λαμβάνει ένα HTTP μέσω ανακατεύθυνσης, επιτρέποντας στους χρήστες να εισάγουν τα διαπιστευτήριά τους. Κατόπιν, τα διακριτικά των χρηστών μεταφράζονται σε ένα Kerberos token και στη συνέχεια, η μετάφραση των διακριτικών του χρήστη αποστέλλεται στον διακομιστή διαχείρισης αιτημάτων μέσω άλλης ανακατεύθυνσης HTTP. Το κύριο ζήτημα ασφαλείας που παρουσιάζει το πρότυπο Passport είναι ότι τα token δεν είναι δεσμευμένα στο πρόγραμμα περιήγησης. Σε περίπτωση επίθεσης, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση όχι μόνο στα token αλλά και σε όλες τις υπηρεσίες του θύματος.

3.4.5 Επιθέσεις έγχυσης κακόβουλου λογισμικού

Οι επιθέσεις έγχυσης κακόβουλου λογισμικού στο μοντέλο CC στοχεύουν στην έγχυση κακόβουλων μηχανών VM (στην περίπτωση του IaaS) ή υλοποίησης υπηρεσιών (στις περιπτώσεις των PaaS ή SaaS) στο σύστημα του cloud. Αποτελέσματα αυτού του είδους επιθέσεων είναι η δυνατότητα υποκλοπών ή τροποποιήσεων των δεδομένων, πλήρων αλλαγών στη λειτουργικότητα του συστήματος, αποκλεισμών χρηστών ή υπηρεσιών, κλπ. [87].

Για να είναι μια επίθεση έγχυσης κακόβουλου λογισμικού επιτυχημένη, οι επιτιθέμενοι, αρχικά, δημιουργούν κακόβουλες μονάδες υλοποίησης υπηρεσιών ή μηχανές VM και τις προσθέτουν στο σύστημα του cloud. Στη συνέχεια, εξαπατούν το σύστημα ώστε να αντιμετωπίσουν τις κακόβουλες μονάδες ή τις μηχανές VM ως έγκυρες. Με τον τρόπο αυτό, το παραβιασμένο πλέον σύστημα του cloud ανακατευθύνει αυτόματα τα αιτήματα των έγκυρων χρηστών στο σύστημα στο οποίο εκτελείται ο κακόβουλος κώδικας [88].

3.4.6 Επιθέσεις DoS και κατά της ασφάλειας κινητών συσκευών

Η άρνηση παροχής υπηρεσιών (Denial of Service - DoS) και η κατανεμημένη άρνηση παροχής υπηρεσιών (Distributed DoS - DDoS) συγκαταλέγονται στις κύριες απειλές κατά της ασφαλείας του CC [89]. Κατά τις επιθέσεις DoS, ο επιτιθέμενος

αποσκοπεί στην άρνηση πρόσβασης σε πληροφορίες και υπηρεσίες cloud στους εξουσιοδοτημένους χρήστες. Μια επίθεση DDoS περιλαμβάνει τη χρήση πολλαπλών παραβιασμένων συστημάτων για τη στόχευση και την καταστροφή ενός συγκεκριμένου cloud, προκειμένου να προκληθούν επιθέσεις DoS [90].

Οι επιθέσεις DDoS εναντίον του επιπέδου εφαρμογών μπορούν να εκμεταλλεύονται τα τρωτά σημεία των Διαδικτυακών εφαρμογών. Επίσης, είναι συχνά δύσκολο ή αδύνατο να εντοπιστούν στο επίπεδο δικτύου, οπότε οποιοδήποτε μέτρο προστασίας ενδέχεται να μην μπορεί να τις αντιμετωπίσει, αναγκάζοντας τους χειριστές των ιστοτόπων να στηρίζονται σε συνδυασμό λύσεων που βασίζονται στο cloud ή σε διακομιστές μεσολάβησης (proxy), καθώς και σε βέλτιστες πρακτικές σχεδιασμού και διαχείρισης της αρχιτεκτονικής υποστήριξής των εφαρμογών (όπως οι HTTPD, διακομιστής MySQL, κλπ.). Κάτι τέτοιο απαιτεί τη σωστή επιλογή λογισμικού για χρήση αλλά και του τρόπου διαμόρφωσής του. Για παράδειγμα, μια εφαρμογή που αποστέλλει αιτήματα για μεγάλο αριθμό πόρων σε διακομιστή MySQL μπορεί εύκολα να δεχθεί επίθεση DoS, κατά την οποία δημιουργούνται σχετικά μικροί όγκοι μεταφοράς δεδομένων που αποσκοπούν στον αποσυντονισμό της λειτουργίας του διακομιστή SQL. Αυτό είναι ένα παράδειγμα μιας περίπτωσης κατά την οποία ο επίδοξος επιτιθέμενος μπορεί να εντοπίσει ένα ελάττωμα ή τρωτό σημείο σε μια Διαδικτυακή εφαρμογή και να το χρησιμοποιήσει για την εξαπόλυση επίθεσης DoS που δεν εντοπίζεται εύκολα στο επίπεδο δικτύου [91].

Σύμφωνα με τους Saxena & Dey (2019), οι επιθέσεις DoS και DDoS μπορούν να αντιμετωπιστούν μέσω μιας αποτελεσματικής τεχνικής πρόληψης και ανίχνευσης επιθέσεων DDoS, που βασίζεται στη χρήση ενός τρίτου μέρους για έλεγχο (Third Party Auditor - TPA) [92].

Οι Waseem, Lakhan & Jamali (2016) διαπίστωσαν ότι ιδιαίτερα οι χρήστες κινητών τηλεφώνων είναι συνήθως μη ενημερωμένοι σωστά ή αδιαφορούν για τα ζητήματα ασφάλειας και εμπιστευτικότητας. Οι συγγραφείς πιστεύουν ότι οι χρήστες κινητών τηλεφώνων δεν χρησιμοποιούν σωστά τις περισσότερες φορές τις συσκευές τους, εκθέτοντάς τες ως προς τους επίδοξους επιτιθέμενους. Οι επίδοξοι επιτιθέμενοι, από τη μεριά τους, ενδέχεται να εκμεταλλευτούν μια τέτοια χαλαρή ασφάλεια για να πραγματοποιήσουν επιθέσεις DoS, με σκοπό την άρνηση πρόσβασης των χρηστών στις υπηρεσίες τους στο cloud. Οι πάροχοι cloud, στην προσπάθειά τους να αντιμετωπίσουν τέτοιου είδους επιθέσεις, χρησιμοποιούν μεγάλο αριθμό πόρων cloud, αυξάνοντας περαιτέρω την πιθανότητα οι υπηρεσίες cloud να μην είναι διαθέσιμες στους πελάτες. Το τελικό αποτέλεσμα είναι οι επιτιθέμενοι να μπορούν να διαγράψουν ή να διαχειριστούν προς όφελός τους, τις πληροφορίες που έχουν αποθηκευτεί από τους χρήστες του cloud [54].

3.4.7 Επιθέσεις έγχυσης SQL

Κατά τις επιθέσεις έγχυσης SQL, ο επιτιθέμενος εγχέει στο cloud έναν κακόβουλο κώδικα, με στόχο την καταστροφή των διαδικασιών του. Συνήθως, στην προκειμένη περίπτωση, οι επιτιθέμενοι εκμεταλλεύονται τις ευπάθειες του κώδικα SQL, μέσω των

οποίων μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του cloud και να ανακτήσουν ή να παραποιήσουν ευαίσθητες πληροφορίες που είναι αποθηκευμένες στις βάσεις δεδομένων του [93].

Σε μια επίθεση έγχυσης SQL, ένας εισβολέας μπορεί επίσης να δημιουργήσει ένα εντελώς νέο κακόβουλο SQL query για να εκτελέσει μια μη εξουσιοδοτημένη λειτουργία της βάσης δεδομένων. Με τον τρόπο αυτό μπορεί να θέσει σε κίνδυνο την εμπιστευτικότητα και την ασφάλεια των ιστοτόπων που εξαρτώνται από βάσεις δεδομένων [94]. Ένας κατάλληλος επανασχεδιασμός του κώδικα που έχει γραφτεί για μια εφαρμογή PHP από τον προγραμματιστή της, μπορεί να προστατεύσει την εφαρμογή από επιθέσεις έγχυσης SQL. Η προστασία των πόρων του cloud από επιθέσεις έγχυσης SQL μπορεί επίσης να επιτευχθεί μέσω μηχανισμών ανίχνευσης και αναγνώρισης συγκεκριμένων τύπων επιθέσεων [93].

4 Έλεγχοι ασφάλειας

4.1 Η έννοια των ελέγχων ασφάλειας για το Cloud Computing

Η έννοια των ελέγχων ασφάλειας για το μοντέλο CC περιλαμβάνει όλες τις βέλτιστες πρακτικές, διαδικασίες και κατευθυντήριες γραμμές που πρέπει να εφαρμοστούν για την προστασία των περιβαλλόντων cloud από τις ευπάθειες και τα τρωτά σημεία που παρουσιάζουν, αλλά και για τη μείωση των επιπτώσεων από τις κακόβουλες επιθέσεις εναντίον τους. Οι έλεγχοι ασφάλειας βοηθούν τις εταιρείες να αντιμετωπίζουν τα όποια ζητήματα ασφαλείας, να αξιολογούν την κατάσταση επικινδυνότητας και να εφαρμόζουν τα κατάλληλα μέτρα προστασίας για την επίτευξη του μεγαλύτερου δυνατού επιπέδου ασφάλειας των κρίσιμων στοιχείων τους που φιλοξενούνται σε περιβάλλον cloud [95].

Δεδομένου ότι η φιλοσοφία του cloud διαφέρει από αυτήν των εσωτερικών επιχειρηματικών δικτύων, οι επιχειρήσεις είναι σημαντικό να κατανοήσουν ότι και η ασφάλειά του διαφέρει από αυτήν των κέντρων δεδομένων προτού το υιοθετήσουν. Εξίσου σημαντική είναι και η εφαρμογή των ελέγχων ασφάλειας μετά την υιοθέτηση της τεχνολογίας [96]. Το τεχνικό τμήμα της εκάστοτε επιχείρησης θα πρέπει να εφαρμόζει τους απαραίτητους ελέγχους ασφάλειας, τις περισσότερες φορές με τη βοήθεια των εργαλείων και των υπηρεσιών που παρέχονται από τους παρόχους cloud, για την ασφάλεια των δικτύων και των εφαρμογών των πελατών. Επίσης, καθώς η πρόσβαση των χρηστών στα ευαίσθητα δεδομένα και τις εφαρμογές των εταιρειών στο cloud γίνεται απομακρυσμένα, το τεχνικό τμήμα πρέπει να εφαρμόσει και ελέγχους πρόσβασης των χρηστών, έλεγχοι που και πάλι θα πρέπει να γίνουν με τα κατάλληλα εργαλεία που παρέχονται από τους παρόχους cloud [97].

Στη βιβλιογραφία έχουν παρουσιαστεί κατά καιρούς διάφορες προτάσεις ως προς την πραγματοποίηση ελέγχων ασφάλειας του cloud. Στα πλαίσια της παρούσας πτυχιακής εργασίας θα παρουσιαστούν στις επόμενες υποενότητες οι σημαντικότερες από αυτές.

4.2 Έλεγχοι των επιθέσεων κατά του hardware υλικού

Η πρώτη γραμμή άμυνας απέναντι στις επιθέσεις που στοχεύουν στο hardware υλικό αφορά την επίτευξη υψηλού επιπέδου φυσικής ασφάλειας των κέντρων δεδομένων [98]. Ωστόσο, στην περίπτωση των εσωτερικών απειλών ένα τέτοιο μέτρο θα μπορούσε εύκολα να παραβιαστεί μέσω παράκαμψης των μηχανισμών φυσικής ασφάλειας. Για την αποφυγή των επιθέσεων δευτερεύοντος καναλιού (side channel attacks), η εξαπόλυση των οποίων μπορεί να οδηγήσει σε απώλεια πληροφοριών, μπορούν να γίνουν αλλαγές στις φάσεις του αλγορίθμου κρυπτογράφησης, με σκοπό την τροποποίηση των μοτίβων προσωρινής και μόνιμης μνήμης [81].

Σύμφωνα με τον Sun (2019), οι διαδικασίες της κρυπτογράφησης, του ελέγχου πρόσβασης και του ελέγχου ταυτότητας αποτελούν βασικούς μηχανισμούς ελέγχου των επιθέσεων κατά του hardware υλικού [67]. Οι συνήθεις τεχνικές κρυπτογράφησης αφορούν την κρυπτογράφηση βάσει ταυτότητας (IDentity based Cryptography – IDC) και την ιεραρχική κρυπτογράφηση βάσει ταυτότητας (Hierarchical IDC – HIDC) [99]. Η κρυπτογράφηση IDC είναι μια τεχνολογία δημόσιου κλειδιού που επιτρέπει τη χρήση του δημόσιου αναγνωριστικού ενός χρήστη ως δημόσιου κλειδιού του. Η κρυπτογράφηση HIDC αποτελεί εξέλιξη της IDC και αναπτύχθηκε με σκοπό την επίλυση του ζητήματος της επεκτασιμότητας που παρουσιάζει η δεύτερη [100]. Προκειμένου να επιτευχθεί αποτελεσματικός έλεγχος ταυτότητας και έλεγχος πρόσβασης στα περιβάλλοντα cloud μέσω των διαδικασιών διαχείρισης ταυτότητας και χρήσης της κρυπτογράφησης HIDC, κάθε χρήστης και διακομιστής cloud έχει τη δική του μοναδική ταυτότητα, η οποία εκχωρείται από το σύστημα ιεραρχικά [101]. Η κρυπτογράφηση HIDC αποτελείται από πέντε αλγόριθμους. ρύθμιση ρίζας, ρύθμιση χαμηλότερου επιπέδου, εξαγωγή, κρυπτογράφηση και αποκρυπτογράφηση. Με τη χρήση της μοναδικής ταυτότητας και την ιεραρχική κρυπτογράφηση HIBC, η διανομή κλειδιών, ο έλεγχος ταυτότητας και ο έλεγχος πρόσβασης καθίστανται πιο ασφαλείς διαδικασίες [102].

4.3 Έλεγχοι των επιθέσεων κατά των υπερεποπτών

Ορισμένοι από τους μηχανισμούς κατά των επιθέσεων που στοχεύουν στο hardware υλικό του cloud μπορούν να εφαρμοστούν και να είναι επίσης αποτελεσματικοί για την εξασφάλιση της προστασίας των υπερεποπτών. Οι υπερεπόπτες αποτελούν ένα πολύ βασικό στοιχείο κάθε υπηρεσίας cloud, χαρακτηριστικό που τους καθιστά αυτόματα ως τους πρώτους πιθανούς στόχους των επιτιθέμενων. Η παρακολούθηση και ο έλεγχος των δραστηριοτήτων των υπερεποπτών μπορεί να επιτευχθούν με χρήση πολλών λύσεων που βασίζονται στο hardware υλικό ή στο λογισμικό και υφίστανται διαθέσιμες στην αγορά [103].

Η εικονικοποίηση με την υποβοήθηση του hardware υλικού (Hardware Assisted Virtualization - HAV), που αφορά μια προσέγγιση εικονικοποίησης πλατφόρμας, η οποία επιτυγχάνει αποτελεσματική πλήρη εικονικοποίηση μέσω χρήσης των δυνατοτήτων του hardware υλικού και κυρίως των κεντρικών επεξεργαστών, μπορεί να συνεισφέρει στην προστασία των υπερεποπτών, ενισχύοντας την ασφάλειά τους [104]. Η εικονικοποίηση HAV αποτρέπει τις όποιες απειλές ασφάλειας κατά της ακεραιότητας των υπερεποπτών και ενισχύει την απομόνωση των πόρων του hardware υλικού του συστήματος. Μέσω της εικονικοποίησης HAV καθίσταται επίσης δυνατή η εικονικοποίηση της φυσικής μνήμης του hardware υλικού [29]. Η εικονικοποίηση HAV παρέχει επίσης ασφάλεια στη μονάδα διαχείρισης εξόδου εισόδου της μνήμης (Input Output Memory Management Unit - IOMMU), κάτι που επιτρέπει στις μηχανές VM να έχουν άμεση πρόσβαση σε περιφερειακές συσκευές. Με τον τρόπο αυτό, είναι δυνατή η αντιμετώπιση των επιθέσεων από κακόβουλες συσκευές που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα των υπερεποπτών [105].

Οι τεχνικές ασφάλειας που βασίζονται σε λογισμικό προστατεύουν τις μηχανές VM είτε εκ των έσω (σε επίπεδο λειτουργικού συστήματος) ή εξωτερικά (σε επίπεδο υπερεποπτών). Στην περίπτωση αυτή η ασφάλεια των υπερεποπτών μπορεί να επιτευχθεί μέσω απομόνωσης της μνήμης, απομόνωσης των συσκευών και απομόνωσης του δικτύου. Περισσότερες λεπτομέρειες μπορούν να βρεθούν στην μελέτη των Chandramouli & Chandramouli (2016) [106].

4.4 Έλεγχοι μέσω Cloud Auditing

Όσον αφορά την ασφάλεια, στόχος του auditing είναι η αξιολόγηση των πολιτικών ασφαλείας καθώς και των πρακτικών και των τεχνικών ελέγχου που χρησιμοποιεί και ακολουθεί μια εταιρεία, αλλά και η αποτίμηση της συμμόρφωσης τους με τους κανονισμούς, της αποτελεσματικότητάς τους ως προς την ανίχνευση και τον εντοπισμό των επιθέσεων, της συνολικής προστασίας των διαδικασιών και επίτευξης ενός ικανοποιητικού επιπέδου ασφάλειας από τους κινδύνους του κυβερνοχώρου [107]. Οι έλεγχοι ασφαλείας μπορεί να είναι reactive και να πραγματοποιούνται περιστασιακά, δηλαδή μετά την εμφάνιση κάποιου ζητήματος ασφάλειας, ή proactive, που αποτελούν προληπτικούς ελέγχους που διενεργούνται έτσι ώστε να αξιολογείται η επάρκεια και η πρακτικότητα των ελέγχων ασφαλείας, των διαδικασιών, των διεργασιών και των λειτουργιών που πραγματοποιούνται, με στόχο την προστασία των ζωτικών περιουσιακών στοιχείων ενός πελάτη [108].

Η πραγματοποίηση διαδικασιών auditing στο μοντέλο CC εγείρει δύο σημαντικές ανησυχίες. Πρώτον, απαιτείται η ύπαρξη διαφάνειας προς τους πελάτες όλων των διαδικασιών auditing που πραγματοποιούνται από τους παρόχους υπηρεσιών cloud. Δεύτερον, το εύρος των ελέγχων ασφαλείας που πραγματοποιείται κατά το auditing θα πρέπει να συμμορφώνεται με τις απαιτήσεις που τίθενται από τους υφιστάμενους νόμους, κανονισμούς και πρότυπα, αλλά και να λαμβάνεται υπόψη όλη η γκάμα διαφορετικών πληροφοριών που επιβλέπονται από τους παρόχους υπηρεσιών cloud [109]. Λόγω αυτών των ζητημάτων, η χρήση του auditing ως διαδικασία ελέγχου των απαιτήσεων ασφάλειας σε περιβάλλον cloud, μπορεί να αποτελέσει σημαντική πρόκληση.

Σε μια προσπάθεια αντιμετώπισης αυτής της πρόκλησης, οι πάροχοι υπηρεσιών cloud έχουν αρχίσει τις προσπάθειας υποστήριξης της διαφάνειας κατά τη διαχείριση της ασφάλειας των πληροφοριών. Με τον τρόπο αυτό, προσπαθούν να βελτιώσουν τις πελατειακές τους σχέσεις, ενισχύοντας την εμπιστοσύνη των πελατών τους και ενημερώνοντάς τους σχετικά με όλες τις διαδικασίες ελέγχου (όσον αφορά την ποικιλία και το εύρος) που πραγματοποιούν [110].

Παρόλα αυτά, η διαφάνεια των ελέγχων ασφάλειας που πραγματοποιούνται από τους παρόχους cloud εγείρει νέες προκλήσεις, όσον αφορά τις πολιτικές ελέγχου αλλά και τις λειτουργίες, τις πρακτικές και τις τεχνικές ελέγχου, καθώς ο όγκος των δεδομένων που πρέπει να εποπτευθεί είναι τεράστιος. Δεδομένου ότι τα εγκλήματα στον κυβερνοχώρο και οι κακόβουλες επιθέσεις έχουν στόχο τις ψηφιακές συσκευές, τα συμβατικά συστήματα ελέγχου εξειδικεύονται στον εντοπισμό γνωστών απειλών,

κάτι που σημαίνει ότι η παροχή υποστήριξης για τον εντοπισμό άγνωστων απειλών είναι μια τάση ελέγχου που έχει μεγάλη σημασία για τα περιβάλλοντα cloud. Λόγω του μεγάλου όγκου δεδομένων και των αρχείων καταγραφής που υπάρχουν πλέον στα κέντρα δεδομένων των cloud, απαιτείται η χρήση νέων μεθόδων ελέγχου τους που να βασίζονται σε τεχνικές εξόρυξης δεδομένων, μηχανικής μάθησης και τεχνικών παρακολούθησης της συμπεριφοράς. Στο ίδιο πνεύμα, η αποθήκευση ακατέργαστων δεδομένων ελέγχου απαιτεί νέα αρχιτεκτονική και τεχνολογία βάσεων δεδομένων (όπως η NoSQL) ή υποστήριξη βάσεων δεδομένων επίπεδων αρχείων. Για λόγους επεκτασιμότητας, εξετάζονται νέες επιλογές ανάπτυξης που θα μεταβούν από τις συγκεντρωτικές αναλύσεις ελέγχου σε κατανεμημένες. Η χρήση του cloud auditing πρέπει να διερευνηθεί και να βελτιωθεί περαιτέρω, ώστε να είναι σε θέση να αντιμετωπίσει συγκεκριμένα χαρακτηριστικά του δυναμικού περιβάλλοντος ενός cloud [111].

4.5 Έλεγχοι μέσω αποτελεσματικής κρυπτογράφησης

Με την αύξηση της δημοτικότητας του CC, όλο και περισσότερες εταιρείες, οργανισμοί και μεμονωμένοι χρήστες παρακινούνται να μεταφέρουν τα δεδομένα τους στο cloud για αποθήκευση. Μία από τις τυπικές εφαρμογές περιλαμβάνουν συστήματα αποθήκευσης cloud ιατρικών αρχείων, στις οποίες η ηλεκτρονική ανταλλαγή δεδομένων υγείας μπορεί να βοηθήσει τους γιατρούς να αξιολογήσουν αποτελεσματικά την κατάσταση των ασθενών και να προβούν σε ανάλογες θεραπείες. Ωστόσο, καθώς οι διακομιστές cloud δεν είναι απόλυτα αξιόπιστοι και τα δεδομένα που μεταφορτώνονται σε περιβάλλον cloud μπορεί να περιέχουν ευαίσθητες πληροφορίες, η ασφάλεια των ευαίσθητων δεδομένων στο cloud αποτελεί ζήτημα μείζονος σημασίας για τους χρήστες. Προκειμένου να αντιμετωπιστεί αυτό το ζήτημα, τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφηθούν πριν από την μεταφόρτωσή τους στο cloud. Για να αποφευχθεί η διαρροή των πληροφοριών που αφορούν τους ασθενείς, στο cloud γίνεται μεταφόρτωση των κρυπτογραφημένων ιατρικών δεδομένων. Αν και η κρυπτογράφηση μπορεί να διασφαλίσει την εμπιστευτικότητα των δεδομένων, δημιουργεί ζητήματα όπως η δυσκολία πρόσβασης και επεξεργασίας τους. Για παράδειγμα, όταν οι γιατροί απαιτούν την πρόσβαση σε συγκεκριμένα ιατρικά δεδομένα, ο διακομιστής cloud πρέπει να εκτελέσει λειτουργίες αναζήτησης χωρίς να γνωρίζει το περιεχόμενο των δεδομένων. Ωστόσο, οι συμβατικές μέθοδοι ανάκτησης πληροφοριών που βασίζονται σε απλό κείμενο δεν μπορούν να χρησιμοποιηθούν απευθείας σε κρυπτογραφημένο κείμενο. Επομένως, ο ασφαλής τρόπος αναζήτησης κρυπτογραφημένων δεδομένων είναι σημαντικός και αποτελεί μια νέα πρόκληση, η οποία μπορεί να αντιμετωπιστεί με χρήση αλγορίθμων ενισχυμένης κρυπτογράφησης. Τέτοιοι αλγόριθμοι μπορεί να είναι οι εξής [112]: (1) κρυπτογράφησης βάσει χαρακτηριστικών (Attribute Based Encryption – ABE), (2) πλήρους ομομορφικής κρυπτογράφησης (Fully Homomorphic Encryption – FHE) και (3) συμμετρικής κρυπτογράφησης (Symmetric Encryption – SE).

Η κρυπτογράφηση ABE αποτελεί μια δημοφιλή μέθοδο επιβολής πολιτικών ελέγχου πρόσβασης μέσω κρυπτογράφησης. Ο συγκεκριμένος αλγόριθμος επιτρέπει σε οντότητες, με τα κατάλληλα διαπιστευτήρια, την αποκρυπτογράφηση κειμένου που κρυπτογραφήθηκε σύμφωνα με μια πολιτική ελέγχου πρόσβασης. Ανάλογα με τον τρόπο επιβολής της πολιτικής ελέγχου πρόσβασης, υπάρχουν δύο παραλλαγές της [113]: η κρυπτογράφηση ABE πολιτικής κλειδιού (Key Policy ABE – KP-ABE) και η κρυπτογράφηση ABE πολιτικής κρυπτοκειμένου (Ciphertext Policy ABE – CP-ABE). Η διαφορά των δύο αλγορίθμων αφορά την εκάστοτε τοποθέτηση των χαρακτηριστικών και της πολιτικής πρόσβασης κατά την κρυπτογράφηση. Στην κρυπτογράφηση KP-ABE, η πολιτική πρόσβασης κρυπτογραφείται στο μυστικό κλειδί του χρήστη και ένα κρυπτοκείμενο επισημαίνεται με ένα σύνολο περιγραφικών χαρακτηριστικών, ενώ στην κρυπτογράφηση CP-ABE, το μυστικό κλειδί του χρήστη σχετίζεται με μια λίστα χαρακτηριστικών και η πολιτική πρόσβασης καθορίζεται από ένα κρυπτοκείμενο. Η σύγκρισή τους αποδεικνύει ότι η κρυπτογράφηση CP-ABE παρουσιάζει μεγαλύτερη ευελιξία αλλά και πολυπλοκότητα, καθιστώντας την επίτευξη ασφάλειας του συστήματος πιο δύσκολη διαδικασία [114].

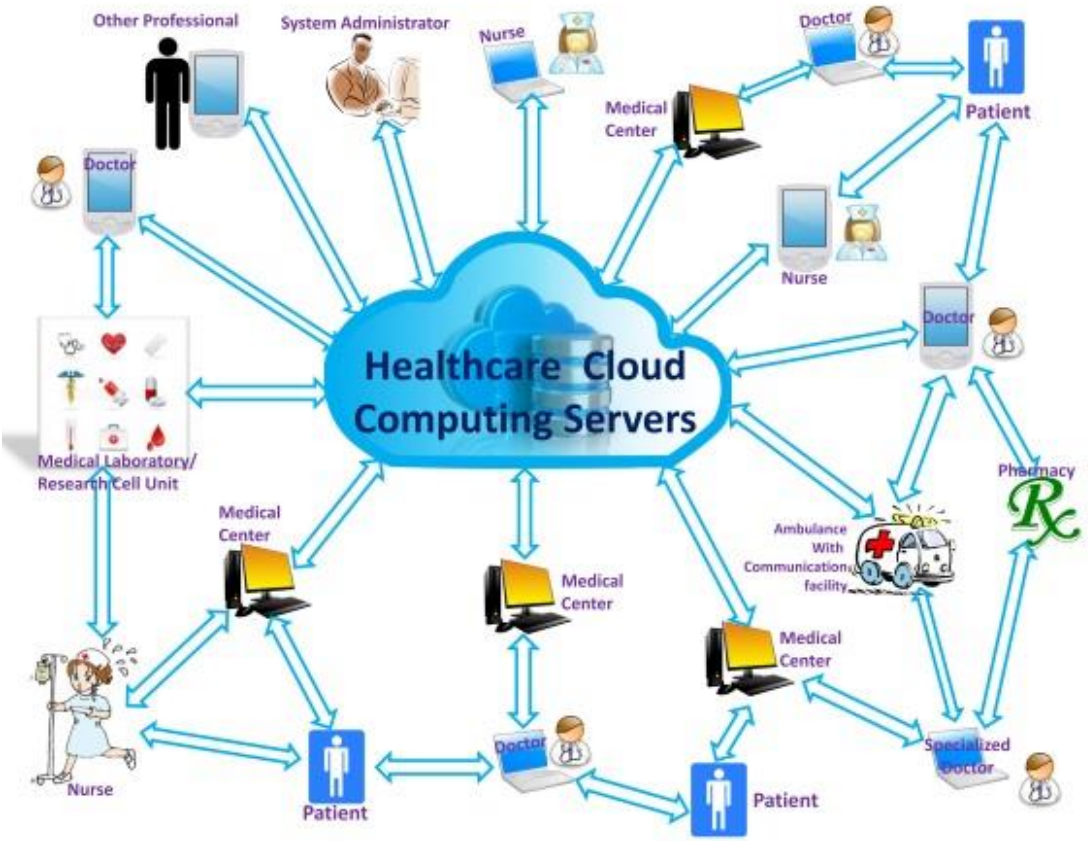
Η χρήση κρυπτογράφησης FHE στον μοντέλο CC επιτρέπει την πραγματοποίηση άμεσων υπολογισμών σε κρυπτογραφημένα δεδομένα. Παρά τα πλεονεκτήματά της, η πρακτική χρήση αυτής της μεθόδου περιορίζεται μόνο στην πολύ απλή επεξεργασία δεδομένων, όπως η πρόσθεση και ο πολλαπλασιασμός αριθμών [114]. Σε σύγκριση με απλούς αλγόριθμους κρυπτογράφησης, όπως η κρυπτογράφηση δημόσιου κλειδιού, που περιλαμβάνουν τρεις διαδικασίες ασφάλειας (παραγωγή κλειδιού, κρυπτογράφηση, αποκρυπτογράφηση), η κρυπτογράφηση FHE περιλαμβάνει και μια τέταρτη διαδικασία, αυτή της αξιολόγησης του αλγόριθμου. Αυτή της η ιδιαιτερότητα, την καθιστά προσιτή σε εφαρμογές cloud, ενισχύοντας την ασφάλεια και την προστασία του απορρήτου των χρηστών [115].

Η κρυπτογράφηση SE παρέχει τη δυνατότητα ασφαλών λειτουργιών αναζήτησης σε κρυπτογραφημένα δεδομένα. Για να ενισχυθεί η αποτελεσματικότητα της αναζήτησης, μια επέκτασή της, η συμμετρική κρυπτογράφηση με δυνατότητα αναζήτησης (Searchable SE – SSE), δημιουργεί ευρετήρια λέξεων-κλειδιών για την ασφαλή εκτέλεση ερωτημάτων από τους χρήστες και επιτρέπει την αποθήκευση δεδομένων σε ιδιωτικούς χώρους τρίτων μερών, διατηρώντας παράλληλα τη δυνατότητα αναζήτησης σε αυτούς. Με τον τρόπο αυτό επιτυγχάνεται μεγαλύτερη ασφάλεια των αναζητήσεων των χρηστών [116].

5 Ζητήματα ασφάλειας του cloud στον τομέα της υγείας

5.1 Σύνοψη των ζητημάτων και των απαιτήσεων ασφάλειας

Τη σύγχρονη εποχή, ο τομέας της υγείας επικεντρώνεται στην οποτεδήποτε και από οπουδήποτε πρόσβαση στα ιατρικά αρχεία των ασθενών. Η χρήση του μοντέλου CC στον τομέα της υγείας διευκολύνει την ενσωμάτωση των ιατρικών αρχείων σε μεγάλες βάσεις δεδομένων, δίνοντας τη δυνατότητα κοινής χρήσης τους. Όπως φαίνεται στην εικόνα 5.1, ένα σύστημα cloud υγείας αποτελεί μια υποδομή αρχιτεκτονικής cloud όπου όλοι οι πάροχοι υπηρεσιών υγείας μπορούν να επικοινωνούν μεταξύ τους μέσω των διακομιστών cloud. Παρά τα όποια όμως οφέλη του, μια τέτοια χρήση του CC στον τομέα της υγείας, δημιουργεί και κινδύνους για την ασφάλεια και τη διατήρηση του απορρήτου για τα δεδομένα υγείας. Στην περίπτωση του τομέα της υγείας, η αντιμετώπιση των ζητημάτων ασφαλείας θα πρέπει να γίνει με τέτοιο τρόπο ώστε να ενισχυθεί το επίπεδο εμπιστοσύνης μεταξύ των ασθενών και των παρόχων υγειονομικής περίθαλψης [49].



Εικόνα 5.1: Συνοπτική απεικόνιση ενός συστήματος cloud υγείας [49]

Στη βιβλιογραφία μέχρι στιγμής έχει παρουσιαστεί μια μεγάλη σειρά από μελέτες που ασχολούνται με τα ζητήματα ασφάλειας που παρουσιάζουν οι εφαρμογές cloud στον τομέα της υγείας. Για παράδειγμα, οι Rezaeibagha, Win & Susilo (2015) παρουσίασαν τα αποτελέσματα συστηματικής βιβλιογραφικής ανασκόπησης σχετικά με την ασφάλεια και τη διατήρηση του απορρήτου των συστημάτων ηλεκτρονικών ιατρικών αρχείων (Electronic Health Records – EHR) [117]. Ο Abdulhameed (2021) παρουσίασε μια ταξινόμηση 126 μελετών που ασχολούνται με την ασφάλεια και την προστασία του απορρήτου των αρχείων EHR σε περιβάλλοντα cloud, τις οποίες και κατέταξε σε δύο μεγάλες κατηγορίες. Η πρώτη περιλαμβάνει την εφαρμογή των διαδικασιών του ελέγχου ταυτότητας, της εξουσιοδότησης και του ελέγχου πρόσβασης στα αρχεία EHR, ενώ η δεύτερη την εφαρμογή των μηχανισμών ασφάλειας και προστασίας του απορρήτου στα δεδομένα των αρχείων αυτών. Ο συγγραφέας κατέληξε στο συμπέρασμα, ότι για την ενίσχυση της ασφάλειας θα πρέπει να υπάρξει ενσωμάτωση των διαδικασιών του ελέγχου ταυτότητας, της εξουσιοδότησης και του ελέγχου πρόσβασης στους μηχανισμούς ασφάλειας των αρχείων HER [118].

Οι Ibrahim, Mahmood & Singhal (2016) πρότειναν ένα πλαίσιο, το οποίο επιτρέπει την ασφαλή κοινή χρήση των αρχείων EHR που είναι αποθηκευμένα σε περιβάλλον cloud μεταξύ διαφορετικών παρόχων υγειονομικής περίθαλψης. Το προτεινόμενο πλαίσιο εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικότητα, τη διαθεσιμότητα και τη δυνατότητα ελέγχου των αρχείων EHR [119]. Παρόλα αυτά, τα ζητήματα ασφάλειας και διατήρησης του απορρήτου των συστημάτων υγείας σε περιβάλλοντα cloud δεν περιορίζονται μόνο στην τήρηση του μοντέλου ασφάλειας CIA [49]. Ο Koranga (2016) υποστήριξε ότι οι απειλές κατά της ασφάλειας των δεδομένων στα περιβάλλοντα cloud περιλαμβάνουν πλαστογράφηση της ταυτότητας του χρήστη, που πραγματοποιείται από επιτιθέμενο ώστε να θεωρηθεί νόμιμος χρήστης, παραβίαση των δεδομένων για κακόβουλη τροποποίηση του περιεχομένου, άρνηση της γνησιότητας της υπογραφής των χρηστών μετά την πραγματοποίηση κακόβουλης τροποποίησης των δεδομένων και αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένους χρήστες [120].

Η βελτίωση της εμπιστοσύνης των χρηστών ως προς την υιοθέτηση του μοντέλου CC στον τομέα της υγείας, μπορεί να επιτευχθεί μόνο μέσα από την πλήρωση των υπαρχόντων απαιτήσεων ασφαλείας. Στις επόμενες υποενότητες θα γίνει μια παρουσίαση αυτών των απαιτήσεων.

5.1.1 Μοντέλο ασφάλειας CIA

Όπως έχει ήδη αναφερθεί το μοντέλο CIA χρησιμοποιείται για να αναδείξει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα, ως τις τρεις βασικές απαιτήσεις που θα πρέπει να πληροί ένα οποιοδήποτε σύστημα για να θεωρηθεί ασφαλές.

Η εμπιστευτικότητα (Confidentiality), στην περίπτωση της ασφάλειας του cloud στον τομέα της υγείας, αποτελεί χαρακτηριστικό διασφάλισης των δεδομένων υγείας των ασθενών, όσον αφορά την πρόσβασή τους από μη εξουσιοδοτημένα άτομα ή

οντότητες. Η ανάθεση του ελέγχου των δεδομένων αυτών στο cloud οδηγεί σε αύξηση του κινδύνου παραβίασής τους, καθώς καθίστανται προσβάσιμα σε έναν αυξημένο αριθμό μερών, συσκευών και εφαρμογών. Η αποτελεσματική λειτουργία της σχέσης ασθενούς/γιατρού απαιτεί την ύπαρξη εμπιστοσύνης εκ μέρους του ασθενούς ως προς τα συστήματα υγείας στον τομέα της προστασία του απορρήτου των δεδομένων του. Αν ο ασθενής συνειδητοποιήσει ότι οι πληροφορίες που δίνει σχετικά με το ιατρικό ιστορικό του δεν προστατεύονται κατάλληλα και ότι μπορεί να υποκλαπούν, μπορεί να γίνει πιο επιλεκτικός στο τι δεδομένα δίνει στον θεράποντα ιατρό του στο μέλλον. Η απειλή της παραβίασης των δεδομένων υγείας μπορεί να βλάψει τη σχέση ασθενούς/γιατρού και να αποβεί μοιραία για τη σωστή ιατρική διάγνωση και θεραπεία [121]. Η εμπιστευτικότητα των ιατρικών δεδομένων μπορεί να επιτευχθεί μέσω της σωστής εφαρμογής των ελέγχων πρόσβασης σε αυτά και χρησιμοποιώντας τεχνικές κρυπτογράφησης [122].

Η ακεραιότητα (Integrity) διασφαλίζει ότι τα δεδομένα υγείας που συλλέγονται από το σύστημα ή παρέχονται σε οποιαδήποτε οντότητα είναι ακριβή, περιέχουν τις προβλεπόμενες πληροφορίες και δεν έχουν τροποποιηθεί με οποιονδήποτε τρόπο [118]. Η χρήση του cloud σε σημαντικές εφαρμογές όπως αυτές του τομέα της υγείας (π.χ. το eHealth cloud) απαιτεί εγγυήσεις καλής αξιοπιστίας των παρεχόμενων υπηρεσιών. Η αδυναμία εξασφάλισης της ακεραιότητας των ιατρικών δεδομένων μπορεί να έχει σοβαρές συνέπειες για την υγεία των ασθενών [117]. Κατά το σχεδιασμό ενός συστήματος υγείας, οι υπηρεσίες που αποθηκεύουν και διαχειρίζονται τα δεδομένα των ασθενών, μπορούν να διασφαλίσουν την ακεραιότητα των δεδομένων αυτών μέσω ένταξης στη λειτουργίας τους της έννοιας της επαλήθευσης των πληροφοριών. Ένας τρόπος πραγματοποίησης μιας τέτοιας επαλήθευσης είναι η χρήση τεχνικών ελέγχου αθροίσματος ή κατακερματισμού των δεδομένων. Στην περίπτωση που ο έλεγχος ακεραιότητας αποτύχει, η εφαρμογή πρέπει να αναφέρει το σφάλμα και να τερματίζει χωρίς να προχωρήσει στην επεξεργασία των δεδομένων [123].

Για να μπορεί να πληροί το σκοπό του οποιοδήποτε σύστημα cloud του τομέα της υγείας, οι πληροφορίες που είναι αποθηκευμένες σε αυτό θα πρέπει να είναι διαθέσιμες πάντοτε. Μια πολύ σημαντική, αλλά συχνά παραλειπόμενη, πτυχή των cloud συστημάτων υγείας είναι η συνεχής διαθεσιμότητα (Availability) των δεδομένων ανεξαρτήτως κατάστασης. Αυτό σημαίνει ότι το σύστημα θα πρέπει να λειτουργεί ακόμα και στις περιπτώσεις που έχει διαπιστωθεί παραβίαση της ασφάλειάς τους [124]. Τα συστήματα που παρουσιάζουν υψηλή διαθεσιμότητα θα πρέπει να είναι σε θέση να αποτρέπουν τις διακοπές παροχής υπηρεσιών λόγω διακοπών ρεύματος, αστοχιών υλικού (hardware και software), αναβάθμισης του συστήματος και ύπαρξης επιθέσεων DoS. Θα πρέπει επίσης να είναι σε θέση να διατηρούν τη χρηστικότητα των αρχείων EHR, αφού έχουν πρώτα εφαρμόσει όλους τους κανόνες τήρησης της ασφάλειας και διατήρησης του απορρήτου [125].

5.1.2 Αυθεντικότητα

Με τον όρο αυθεντικότητα (authenticity) γενικά εννοείται η επαλήθευση της προέλευσης, της προσφοράς, των δεσμεύσεων και των προθέσεων. Στον τομέα των

επικοινωνιών και της πληροφορίας διασφαλίζει ότι η οντότητα που ζητά πρόσβαση είναι αυθεντική [49]. Στα συστήματα υγείας, οι πληροφορίες που παρέχονται από τους παρόχους υπηρεσιών και οι ταυτότητες των οντοτήτων που κάνουν χρήση αυτών των πληροφοριών πρέπει να επαληθεύονται μέσω τεχνικών αυθεντικοποίησης ή ελέγχου ταυτότητας [124]. Η μη αυθεντικοποίηση των πληροφοριών μπορεί να δημιουργήσει διάφορα ζητήματα, όπως η ύπαρξη επιθέσεων man-in-the-middle, οι οποίες συχνά αντιμετωπίζονται με συνδυασμούς διακριτικών [126]. Τα περισσότερα κρυπτογραφικά πρωτόκολλα περιλαμβάνουν κάποια μορφή ελέγχου ταυτότητας, ειδικά για την πρόληψη ενάντια στις επιθέσεις man-in-the-middle [127].

5.1.3 Μη απόρριψη

Οι απειλές απόρριψης (repudiation) προέρχονται από τις περιπτώσεις στις οποίες οι χρήστες αρνούνται τη γνησιότητα της υπογραφής τους μετά την πρόσβασή τους σε δεδομένα [128]. Στην περίπτωση των δεδομένων που βρίσκονται σε cloud υγείας, κάτι τέτοιο δεν θα πρέπει να συμβαίνει αφού ούτε οι ασθενείς ούτε οι γιατροί μπορούν να αρνηθούν την γνησιότητα της υπογραφής τους μετά από πρόσβασή τους σε δεδομένα. Ακριβώς όπως συμβαίνει και στο ηλεκτρονικό εμπόριο, οι εφαρμογές cloud υγείας μπορούν να περιλαμβάνουν μηχανισμούς χρήσης ψηφιακών υπογραφών και κρυπτογράφησης ώστε να είναι σε θέση να πληρούν τις απαιτήσεις αυθεντικότητας και μη απόρριψης [129].

5.1.4 Auditing

Η διαδικασία του auditing αποτελεί ένα μέτρο που μπορεί να ενισχύσει την ασφάλεια ενός συστήματος υγείας. Στην περίπτωση των συστημάτων cloud υγείας, το auditing περιλαμβάνει καταχώρηση των δραστηριοτήτων των χρηστών στο σύστημα υγείας με χρονολογική σειρά. Τέτοιες δραστηριότητες μπορεί να αποτελούν τη διατήρηση αρχείου καταγραφής κάθε πρόσβασης και τροποποίησης των δεδομένων. Σύμφωνα με ήδη υπάρχοντες κανονισμούς, οι χρήστες των συστημάτων υγείας θα πρέπει να λογοδοτούν για τις ενέργειές τους, όταν χειρίζονται προστατευμένες πληροφορίες που αφορούν την υγεία ασθενών. Με βάση αυτούς τους κανονισμούς, οι διαδικασίες auditing θα πρέπει να περιλαμβάνουν ελέγχους που είναι σε θέση να αντιμετωπίζουν τις περιπτώσεις εσωτερικών απειλών, διασφαλίζοντας τον εντοπισμό μη εξουσιοδοτημένης πρόσβασης και παράνομης αποκάλυψης ιατρικών αρχείων. Οι διαδικασίες αυτές θα μπορούσαν επίσης να ενισχύσουν την ανίχνευση των προσπαθειών παράνομων εισβολών στα δημόσια cloud συστήματα υγείας ή τον εντοπισμό πιθανών ευπαθειών του συστήματος [49].

5.1.5 Έλεγχος πρόσβασης

Στην περίπτωση των συστημάτων cloud υγείας, ο έλεγχος πρόσβασης αποτελεί έναν μηχανισμό που ελέγχει και απαγορεύει την πρόσβαση στις πληροφορίες υγείας ενός ασθενούς, στην περίπτωση που ο χρήστης δεν κατέχει την απαιτούμενη εξουσιοδότηση ή δεν είναι νόμιμος. Η πολιτική ελέγχου πρόσβασης που χρησιμοποιείται βασίζεται συνήθως στο προνόμιο εξουσιοδότησης που λαμβάνει ο

ιατρός από τον ασθενή ή ένα έμπιστο τρίτο μέρος. Στη βιβλιογραφία έχουν προταθεί αρκετές λύσεις για την αντιμετώπιση των ζητημάτων ασφάλειας που μπορούν να παρουσιαστούν στους μηχανισμούς ελέγχου πρόσβασης και αφορούν τα συστήματα cloud υγείας. Για τις cloud εφαρμογές υγείας, τα δημοφιλέστερα μοντέλα ελέγχου πρόσβασης είναι ο έλεγχος πρόσβασης βάσει ρόλου (Role-Based Access Control-. RBAC) και ο έλεγχος πρόσβασης βάσει ιδιότητας (Attribute-Based Access. Control-ABAC) [130].

5.2 Βιβλιογραφική ανασκόπηση των προτεινόμενων λύσεων πάνω στα ζητήματα ασφάλειας

Στη βιβλιογραφία μέχρι στιγμής έχει παρουσιαστεί επίσης, μια μεγάλη σειρά από μελέτες που ασχολούνται με πιθανές λύσεις των ζητημάτων ασφάλειας που παρουσιάζουν οι εφαρμογές cloud στον τομέα της υγείας. Στην παρούσα ενότητα θα παρουσιαστούν κάποιες από αυτές τις μελέτες και οι προτάσεις τους για την υλοποίηση συστημάτων cloud υγείας με γνώμονα την ασφάλεια.

Οι Al Hamid και συν. (2017) έχοντας ως στόχο την αντιμετώπιση των ζητημάτων της εμπιστευτικότητας των δεδομένων των ασθενών στα συστήματα cloud υγείας, πρότειναν ένα πρωτόκολλο συμφωνίας μεταξύ τριών μερών που χρησιμοποιεί ένα κλειδί αυθεντικοποίησης και βασίζεται σε τεχνική κρυπτογράφησης διπλού ζεύγους. Το προτεινόμενο πρωτόκολλο μπορεί να δημιουργήσει ένα μοναδικό κλειδί συνεδρίας, το οποίο επιτρέπει την ασφαλή επικοινωνία μεταξύ των συμμετεχόντων. Η ασφαλής πρόσβαση των ιδιωτικών δεδομένων υγείας, αλλά και η αποθήκευσή τους, πραγματοποιείται μέσω υλοποίησης μιας τεχνικής δελεασμού (decoy technique) στην υποδομή ενός συστήματος Fog Computing. Παρά την επίτευξη ισχυρής ασφάλειας, η προτεινόμενη προσέγγιση συνεπάγεται μεγάλο υπολογιστικό κόστος επικοινωνίας [131].

Οι Marwan, Kartit & Ouahmane (2017) πρότειναν μια μέθοδο που βασίζεται στον αλγόριθμο κατανομής κλειδιών SSS (Secret Scheme Share) του Shamir και στην έννοια των multicloud, με σκοπό τη βελτίωση της αξιοπιστίας της αποθήκευσης δεδομένων σε περιβάλλον cloud. Με την έννοια της βελτίωσης της αξιοπιστίας, οι συγγραφείς ήθελαν ουσιαστικά να δημιουργήσουν μια μέθοδο ικανοποίησης των απαιτήσεων ασφάλειας της αποθήκευσης δεδομένων σε περιβάλλον cloud, που αφορούν την αποφυγή απώλειας δεδομένων και την αντιμετώπιση της μη εξουσιοδοτημένης πρόσβασης σε αυτά, αλλά και της αποκάλυψης ευαίσθητων πληροφοριών. Σύμφωνα με την προτεινόμενη μέθοδο, τα ευαίσθητα ιατρικά δεδομένα διαμοιράζονται σε πολλά μικρά μέρη (αρχιτεκτονική multicloud) αλλά και σε πολλά διαφορετικά συστήματα αποθήκευσης cloud, έτσι ώστε να μην είναι συγκεντρωμένα όλα μαζί. Σε ένα τέτοιο σενάριο, οι χρήστες του cloud κρυπτογραφούν τα δεδομένα τους χρησιμοποιώντας την τεχνική SSS, με σκοπό την επίτευξη εμπιστευτικότητας. Τα προβλήματα της μελέτης είναι ότι δεν αναφέρεται κανένα στοιχείο σχετικά με την ισοστάθμιση μεταξύ αποτελεσματικότητας και ασφάλειας, αλλά και για την ποιοτική ανάλυση των ανακτημένων δεδομένων υγείας [132].

Οι Galletta και συν. (2017) παρουσίασαν ένα σύστημα αντιμετώπισης των ζητημάτων ασφάλειας και διατήρησης του απορρήτου των δεδομένων των ασθενών. Το προτεινόμενο σύστημα βασίζεται σε δύο στοιχεία λογισμικού: τον ανωνυμοποιητή και τον διαχωριστή. Ο πρώτος συλλέγει ανώνυμα κλινικά δεδομένα, ενώ ο δεύτερος χρησιμοποιεί τεχνική συσκότισης (obfuscation) και αποθηκεύει τα δεδομένα σε πολλούς παρόχους αποθήκευσης cloud. Με τον τρόπο αυτό, πρόσβαση στα δεδομένα στο cloud έχουν μόνο οι υπεύθυνοι των κλινικών δοκιμών. Οι συγγραφείς απέδειξαν την αποτελεσματικότητά του συστήματός τους, δοκιμάζοντάς το σε αρχεία μαγνητικών τομογραφιών [133].

Οι Smithamol & Rajeswari (2017) παρουσίασαν μία νέα αρχιτεκτονική αντιμετώπισης των ζητημάτων εμπιστευτικότητας και πρόσβασης των ιατρικών δεδομένων που βρίσκονται σε περιβάλλον cloud. Στο προτεινόμενο μοντέλο χρησιμοποιεί κρυπτογράφηση CP-ABE με σκοπό την επίτευξη ελέγχου πρόσβασης στα δεδομένα. Επίσης, ελαχιστοποιεί το υπολογιστικό κόστος και το συνολικό χρόνο κρυπτογράφησης. Η ανάλυσή της απόδοσής του έδειξε μια τέτοια αποτελεσματικότητα που μπορεί να το καταστήσει κατάλληλο για πρακτική χρήση [134].

Οι Dhivya, Ibrahim & Kirubakaran (2017) παρουσίασαν μια ολοκληρωμένη λύση που επιτυγχάνει ασφαλή πρόσβαση σε ευαίσθητα δεδομένα EHR. Οι συγγραφείς χρησιμοποίησαν τρεις τεχνικές για το πετύχουν. Πρώτον, κρυπτογραφική τεχνική που βασίζεται σε ρόλους, για τη διανομή κλειδιών συνεδρίας χρησιμοποιώντας το πρωτόκολλο Kerberos, Δεύτερον, μεθόδους ελέγχου ταυτότητας που βασίζονται στην τοποθεσία και τη βιομετρία, για την εξουσιοδότηση των χρηστών. Τρίτον, τεχνική στεγανογραφίας για την ασφαλή ενσωμάτωση των δεδομένων EHR σε έναν αξιόπιστο χώρο αποθήκευσης cloud. Οι συγγραφείς μελέτησαν επίσης την ανθεκτικότητα της προτεινόμενης λύσης τους σε επιθέσεις αναπαραγωγής και man-in-the-middle. Ωστόσο, δεν ανέλυσαν την επεκτασιμότητά της, την ανθεκτικότητά της σε άλλους σημαντικούς κινδύνους ασφαλείας, όπως της ακεραιότητας και της διαθεσιμότητας των δεδομένων, αλλά και το υπολογιστικό κόστος [135].

Ο Shah & Prasad (2017) παρέθεσαν διάφορες μεθόδους κρυπτογράφησης και ανέπτυξαν ένα πλαίσιο στο οποίο χρησιμοποίησαν το μοντέλο ελέγχου πρόσβασης CPRBAC (Cloud based Privacy aware Role Based Access Control) για την αντιμετώπιση των προκλήσεων ασφάλειας και διατήρησης του απορρήτου που παρουσιάζουν τα συστήματα cloud υγείας. Ένας δευτερεύων στόχος της μελέτης ήταν η μείωση της υπολογιστικής πολυπλοκότητας και του κόστους επικοινωνίας. Οι συγγραφείς, ωστόσο, δεν παρουσίασαν καμία ποιοτική ανάλυση σχετικά με την αποτελεσματικότητα της προσέγγισης και των δυνατοτήτων της ως προς την αντιμετώπισης των επιθέσεων κατά της ασφάλειας των συστημάτων cloud υγείας [136].

5.3 Διαθέσιμες λύσεις ασφάλειας

Τα ζητήματα ασφάλειας θεωρούνται ως το πιο πολυσυζητημένο θέμα του τομέα των ΤΠΕ. Πολλοί πάροχοι υγείας χρησιμοποιούν την τεχνολογία του cloud με ιδιαίτερη

προσοχή λόγω των κινδύνων που ενέχει. Για την αντιμετώπιση των ζητημάτων ασφάλειας, οι ίδιοι οι πάροχοι υπηρεσιών cloud θα πρέπει να βρουν λύσεις και να δώσουν στους χρήστες τους τις απαραίτητες οδηγίες και συστάσεις [49]. Οι λύσεις που προτείνονται στη βιβλιογραφία από τις μέχρι τώρα εμφανιζόμενες μελέτες δεν έχουν ολιστικό χαρακτήρα και αντιμετωπίζουν εν μέρει τα προβλήματα ασφάλειας του cloud που έχουν μέχρι τώρα αναφερθεί. Οι διαθέσιμες λύσεις που αφορούν την ασφάλεια των συστημάτων cloud υγείας είναι περισσότερο κανονιστικού και τεχνικού χαρακτήρα και θα παρουσιαστούν εν συντομία στις επόμενες υποενότητες.

5.3.1 Κανονισμοί

Τα πρότυπα συνήθως δημιουργούνται από εμπειρογνώμονες οργανισμών και επιστημονικών ιδρυμάτων, με σκοπό την περιγραφή των αποδεκτών χαρακτηριστικών ενός προϊόντος ή μιας υπηρεσίας, όπως η ποιότητα, η ασφάλεια και η αξιοπιστία. Τα πρότυπα αυτά τεκμηριώνονται, δημοσιεύονται και θα πρέπει να παραμένουν σε εφαρμογή για μεγάλο χρονικό διάστημα. Στόχος της δημιουργίας τους είναι η υποστήριξη ατόμων και εταιρειών κατά την προμήθεια αγαθών και υπηρεσιών. Οι πάροχοι υπηρεσιών cloud μπορούν να ενισχύσουν τη φήμη τους δημιουργώντας τέτοια πρότυπα. Αντ' αυτού, πολλές χώρες ανέπτυξαν τα δικά τους πρότυπα με σκοπό την ύπαρξη εγγυήσεων σχετικά με την ασφάλεια των περιβαλλόντων cloud. Τέτοια πρότυπα αποτελούν τα HIPAA και HITECH Act των ΗΠΑ, αλλά και διεθνή πρότυπα, όπως η σειρά προτύπων ISO/IEC 27000 και το GDPR [49].

Ο κανονισμός HIPAA (Health Insurance Portability and Accountability Act) αποτελεί ουσιαστικά ένα νομικό πλαίσιο ασφάλειας των συστημάτων υγείας των ΗΠΑ και ορίζει κανόνες και οδηγίες για την προστασία και την ασφάλεια των δεδομένων υγείας. Ένας από τους κανόνες αυτούς, ο HIPAA Security Rule, αποσκοπεί στην προστασία των δεδομένων υγείας του ατόμου, επιτρέποντας παράλληλα στους τεχνολογικούς φορείς την υιοθέτηση των εξελίξεων των ΤΠΕ προς όφελος των υπηρεσιών υγείας και την δημιουργία ποιοτικών υπηρεσιών για ιδιώτες και για παρόχους υπηρεσιών υγείας. Πιο συγκεκριμένα, ο κανόνας ασφαλείας του HIPAA απαιτεί από τους τεχνολογικούς φορείς τη χρήση διαχειριστικών και τεχνικών μεθόδων προστασίας των δεδομένων υγείας, εξασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους, προστατεύοντάς τα έναντι όλων των απειλών για την ασφάλεια ή την ακεραιότητά τους αλλά και από μη εξουσιοδοτημένη χρήση τους [137].

Ο νόμος HITECH Act (Health Information Technology for Economic and Clinical Health Act) θεσπίστηκε με σκοπό τη διεύρυνση και την επιτάχυνση της υιοθέτησης των αρχείων EHR αλλά και τη βελτίωση της απόδοσης των συστημάτων υγείας των ΗΠΑ. Ο συγκεκριμένος νόμος παρακινεί και ανταμείβει τους παρόχους υγείας, προσφέροντάς τους κίνητρα και επιχορηγήσεις, που αυξάνουν την εμπιστοσύνη του κοινού στη χρήση των αρχείων EHR, μέσω λήψης των κατάλληλων μέτρων ασφάλειας. Απώτερος σκοπός του νόμου είναι ο καθορισμός προτύπων και πολιτικών που θα ενισχύουν την ασφάλεια κατά τη μεταφορά των ευαίσθητων ιατρικών δεδομένων στο Διαδίκτυο [138].

Η σειρά προτύπων ISO/IEC 27000 δημιουργήθηκε με σκοπό την αντιμετώπιση ζητημάτων ασφάλειας των πληροφοριών. Η σειρά περιλαμβάνει όλες τις βέλτιστες τεχνικές διαχείρισης της ασφάλειας των πληροφοριών. Πιο συγκεκριμένα, το πρότυπο ISO/IEC 27001 καθορίζει τις απαιτήσεις για τη δημιουργία, εφαρμογή, λειτουργία, παρακολούθηση, αναθεώρηση, διατήρηση και βελτίωση των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών και την ευθυγράμμιση τους με τους στρατηγικούς στόχους της κάθε επιχείρησης. Επίσης, το πρότυπο ασχολείται με την ασφάλεια των υποδομών των συγκεκριμένων συστημάτων, αποσκοπώντας στην αποκατάσταση της εμπιστοσύνης των ασθενών στους παρόχους υπηρεσιών cloud. Το πρότυπο ISO/IEC 27002 επικεντρώνεται στην ασφάλεια κατά τα στάδια σχεδιασμού και ανάπτυξης των συστημάτων και είναι λογικά δομημένο με βάση τις ομάδες των σχετικών ελέγχων ασφάλειας. Ασφαλείας [139], [140].

Ο κανονισμός GDPR (General Data Protection Regulation) καθορίζει τον τρόπο με τον οποίο επιχειρήσεις και οργανισμοί συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα κάθε μορφής, όπως επίσης και το σε ποιες περιπτώσεις επιτρέπεται να χρησιμοποιούνται, αποθηκεύονται, διαγράφονται, μεταβιβάζονται και εν γένει επεξεργάζονται τα προσωπικά δεδομένα, αλλά κυρίως, με ποιον τρόπο μπορούν να προστατευθούν. Ο κανονισμός GDPR έχει ευρωπαϊκή ισχύ αλλά ισχύει και για τις περιπτώσεις οποιασδήποτε συναλλαγής στην επικράτεια της Ευρωπαϊκής Ένωσης.

5.3.2 Λύσεις με κέντρο τους ασθενείς

Οι συγκεκριμένες λύσεις αφορούν συστήματα υγείας στα οποία οι ίδιοι οι ασθενείς μπορούν να αποθηκεύουν, να έχουν πρόσβαση, να ενημερώνουν και να διαμοιράζονται τα δεδομένα υγείας τους [142]. Οι λύσεις με κέντρο τους ασθενείς δίνουν τη δυνατότητα ασφαλούς αποθήκευσης και διαχείρισης των αρχείων EHR των ασθενών, τα οποία θα μπορούσαν να χρησιμοποιηθούν για τη θεραπεία τους, για έρευνα και άλλες εφαρμογές. Παραδείγματα τέτοιων λύσεων πραγματικού χρόνου και cloud χαρακτήρα αποτελούν οι εφαρμογές Google Health και Microsoft HealthVault. Και οι δύο εφαρμογές είναι κεντρικής αρχιτεκτονικής, σύμφωνα με την οποία, οι ασθενείς αποθηκεύουν και ενημερώνουν τα δεδομένα υγείας τους σε σύστημα αρχείων EHR, έχοντας τον πλήρη έλεγχό τους [143]. Για την επίτευξη μεγαλύτερης ασφάλειας των δεδομένων, πριν την μεταφόρτωσή τους στο cloud, χρησιμοποιούνται τεχνικές κρυπτογράφησης, όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο. Φυσικά. η κρυπτογράφηση δεδομένων απαιτεί χρόνο και μπορεί να επηρεάσει την απόδοση του συστήματος.

Η διαδικασία συγκέντρωσης των αρχείων υγείας από διαφορετικές πηγές σε ένα ενιαίο αποθετήριο είναι αρκετά πολύπλοκη, δεδομένου ότι η εφαρμογή ή το σύστημα συγκέντρωσής τους πρέπει να χρησιμοποιεί διαφορετικά πρότυπα και πρωτόκολλα, ώστε να επιτυγχάνεται διαλειτουργικότητα μεταξύ των διαφορετικών ενδιαφερομένων μερών. Η χρήση όμως διαφορετικών προτύπων δημιουργεί ζητήματα ασφάλειας στην εφαρμογή και την καθιστά επιρρεπή σε παραβιάσεις [144]. Το πρόβλημα των λύσεων που έχουν ως κέντρο τους ίδιους τους ασθενείς, όσον αφορά την αντιμετώπιση των

ζητημάτων ασφάλειας είναι οι αντικρουόμενες απαιτήσεις [145]. Δίνοντας τη δυνατότητα στους ασθενείς να αποφασίσουν ποιος μπορεί να έχει πρόσβαση στα αρχεία τους, υπάρχει η πιθανότητα να εμποδιστεί η πρόσβαση ενός γιατρού σε αυτά τα αρχεία σε περίπτωση έκτακτης ανάγκης. Η εφαρμογή πολυεπίπεδων μέτρων ασφάλειας ώστε να εξασφαλιστεί η πρόσβαση στο σύστημα μόνο σε εξουσιοδοτημένους χρήστες, μπορεί να μειώσει την απόδοση του συστήματος, κάτι που έρχεται σε αντίθεση με την ύπαρξη ανάγκης για γρήγορα και ευέλικτα συστήματα [146]. Τα πρόσθετα μέτρα ασφαλείας ενδέχεται επίσης να επηρεάσουν αρνητικά την εμπειρία των χρηστών [147]. Επιπρόσθετα, η θεμελιώδης ανάγκη για πρόσβαση στα δεδομένα των ασθενών από διαφορετικές οντότητες, τα καθιστά περισσότερο ευάλωτα σε παραβιάσεις ασφαλείας [148]. Τέλος, η δυνατότητα των ασθενών για επεξεργασία των δικών τους ιατρικών αρχείων, ενδέχεται να έρθει σε σύγκρουση με την απαίτηση των γιατρών για εγγύηση της γνησιότητας των ιατρικών αρχείων [49].

Συμπεράσματα

Το CC αποτελεί μια πολλά υποσχόμενη τεχνολογία που είναι σε θέση να βοηθήσει επιχειρήσεις και οργανισμούς στο να μειώσουν το λειτουργικό τους κόστος, αυξάνοντας παράλληλα την αποδοτικότητά τους. Ανάμεσα στα πολλά πλεονεκτήματά του, τα σημαντικότερα αποτελούν επίσης, η ταχύτατη ανάπτυξη εφαρμογών, ο μεγάλος χώρος αποθήκευσης δεδομένων και η ευκολία πρόσβασης οποτεδήποτε και από οπουδήποτε. Οι συνεχιζόμενες εξελίξεις της τεχνολογίας αναμένεται να δημιουργήσουν περισσότερα πλεονεκτήματα αλλά και να ελαχιστοποιήσουν τα μειονεκτήματά της.

Ανάμεσα στα μειονεκτήματα αυτά, η ασφάλεια των περιβαλλόντων cloud θεωρείται ίσως το σημαντικότερο. Όπως συμβαίνει και με τις περισσότερες αναδυόμενες τεχνολογίες, η ασφάλεια στο CC είναι ακόμα στα σπάργανα και χρειάζεται ακόμα περισσότερη ερευνητική προσπάθεια. Στις μέχρι τώρα εμφανιζόμενες μελέτες στην βιβλιογραφία, οι ερευνητές έχουν εντοπίσει πολλά κρίσιμα ζητήματα που αφορούν την αξιοπιστία των συστημάτων cloud και αρκετές μελέτες έχουν ασχοληθεί με τα γενικά ζητήματα της ασφάλειας τους.

Η ασφάλεια των δεδομένων αποτελούσε ανέκαθεν ένα μείζον ζήτημα στην τεχνολογία των πληροφοριών. Στο περιβάλλον του cloud γίνεται ιδιαίτερα σοβαρό επειδή τα δεδομένα βρίσκονται σε διαφορετικά μέρη ακόμη και σε ολόκληρο τον κόσμο. Τα θέματα ασφάλειας δεδομένων σχετίζονται με το hardware υλικό αλλά και με το λογισμικό της αρχιτεκτονικής του cloud. Αν και στη βιβλιογραφία έχουν παρουσιαστεί πολλές τεχνικές αντιμετώπισης των ζητημάτων της ασφάλειας των δεδομένων στο περιβάλλον του cloud, η ασφάλειά τους εξακολουθεί να αποτελεί κρίσιμο σημείο, όσον αφορά τη μελλοντική υιοθέτηση της τεχνολογίας από επιχειρήσεις και οργανισμούς.

Σκοπός της παρούσας εργασίας, ήταν η παρουσίαση των ζητημάτων ασφαλείας στον τομέα του CC, εστιάζοντας στην ταξινόμηση τους αλλά και στην ταξινόμηση των πιθανών λύσεων που έχουν παρουσιαστεί μέχρι τώρα στη βιβλιογραφία. Αρχικά, αναπτύχθηκε σε γενικές γραμμές το θεωρητικό υπόβαθρο σχετικά με το CC και την ασφάλειά του, καθώς και η οργάνωση και συμβολή της παρούσας εργασίας. Στη συνέχεια δόθηκε μια γενική περιγραφή της έννοιας του CC και αναπτύχθηκε μια βιβλιογραφική ανασκόπηση των θεμάτων ασφάλειας που αντιμετωπίζει το cloud. Κατόπιν, παρουσιάστηκαν κάποιοι πιθανοί τρόποι αντιμετώπισης των ζητημάτων ασφάλειάς του CC που έχουν προταθεί στη βιβλιογραφία. Η εργασία ολοκληρώθηκε με την παρουσίαση της ασφάλειας των συστημάτων υγείας που λειτουργούν σε περιβάλλον cloud, ένας τομέας ιδιαίτερα κρίσιμος ως προς την αντιμετώπιση των όποιων κινδύνων ασφάλειας μπορεί να προκύψουν από την πλήρη υιοθέτηση της τεχνολογίας.

Βιβλιογραφία

[1] Elmasri, R. & Navathe, S. B. (2016). Fundamentals of Database Systems. Pearson, 7th Edition

[2] Marinescu, D. (2017) Cloud Computing: Theory and Practice, Morgan Kaufmann, 2nd Edition

[3] Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. Journal of Network and Computer Applications, 60, 113-129.

[4] Attiya, I., & Zhang, X. (2017). Cloud computing technology: Promises and concerns. International Journal of Computer Applications, 159(9), 32-37.

[5] Biswash, S. K., & Addya, S. K. (Eds.). (2020). Cloud Network Management: An IoT Based Framework. CRC Press.

[6] Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.

[7] Tiwary, M., Kumar, S., Agrawal, P. K., Puthal, D., Rodrigues, J. J., Sahoo, K. S., & Sahoo, B. (2018, June). Introducing network multi-tenancy for cloud-based enterprise resource planning: An iot application. In 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE) (pp. 1263-1269). IEEE.

[8] Sridevi, S., & Katiravan, J. (2018). Enhanced Resource Provisioning Strategies for Scientific Workflows in Cloud Environment: A Survey. International Journal of Computer Applications (0975 – 8887), Volume 180, No.41, 27-33.

[9] Malathi, L., Malathi, S., & Ahamed, N. N. (2019). Hybrid Cloud Storage for Secure Authorization and Information Hiding. International Conference On Recent Trends In Electronics, Computing And Communication Engineering (ICRTECC 2019).

[10] Krishnan, R. (2017). Security and Privacy in Cloud Computing. Doctoral dissertation, Western Michigan University.

[11] Kashukeev, I., Denchev, S., & Garvanov, I. (2020). Data security model in cloud computing. Industry 4.0, 5(2), 55-58.

[12] Daimi, K., Francia, G., Ertaul, L., Encinas, L. H., & El-sheikh, E. (Eds.). (2018). Computer and network security essentials. Springer.

[13] Bulusu, S. T. (2019). Méthodologie d'ingénierie des exigences de sécurité réseau. Doctoral dissertation, Université Paul Sabatier-Toulouse III.

[14] Baker, A. (2020). A Survey of Information Security Implementations for Embedded Systems. Wind River Systems Inc.

[15] Selvam S. (2021). An Empirical Study on Security Issues in Cloud Computing Environments. International Journal of Engineering Research & Technology (IJERT). Volume 9, Issue 5, 450-454.

[16] McKelvey, N., Curran, K., Gordon, B., Devlin, E., & Johnston, K. (2015). Cloud computing and security in the future. In Guide to Security Assurance for Cloud Computing (pp. 95-108). Springer, Cham.

[17] Goralski, W. (2017). The illustrated network: how TCP/IP works in a modern network. Morgan Kaufmann.

[18] Khan, S., Shakil, K. A., & Alam, M. (2017). Big data computing using cloud-based technologies, challenges and future perspectives. arXiv preprint arXiv:1712.05233.

[19] Tsai, W. T., & Shao, Q. (2011, March). Role-based access-control using reference ontology in clouds. In 2011 Tenth International Symposium on Autonomous Decentralized Systems (pp. 121-128). IEEE.

[20] Board, F. S. (2019). Third-party dependencies in cloud services: Considerations on financial stability implications. FSB Publication, December, 9.

[21] Sharma, M., & Husain, S. (2017). Analyzing the Difference of Cluster, Grid, Utility & Cloud Computing. IOSR Journal of Computer Engineering, 19(1), 55-60.

[22] AlHakami, H., Aldabbas, H., & Alwada'n, T. (2012). Comparison between cloud and grid computing. International journal on cloud computing: services and architecture (IJCCSA), 2(4), 1-21.

[23] Sungkar, A. & Kogoya, T. (2020). A Review of Grid Computing. Computer Science & IT Research Journal. 1. 1-6.

[24] Ziegler, W. (2017). A framework for managing quality of service in cloud computing through service level agreements. Doctoral dissertation, Niedersächsische Staats-und Universitätsbibliothek Göttingen.

[25] Ochoa, R., Watowich, S. J., Flórez, A., Mesa, C. V., Robledo, S. M., & Muskus, C. (2016). Drug search for leishmaniasis: a virtual screening approach by grid computing. Journal of computer-aided molecular design, 30(7), 541-552.

[26] Sathish, K., & Reddy, A. R. (2017). Workflow scheduling in grid computing environment using a hybrid gaaco approach. Journal of The Institution of Engineers (India): Series B, 98(1), 121-128.

[27] Azam, M. G. (2019). Application of cloud computing in library management: innovation, opportunities and challenges. Int. J. Multidiscip., 4(1), 2-11.

[28] Alajmi, Q., Sadiq, A. S., Kamaludin, A., & Al-Sharafi, M. A. (2018). Cloud computing delivery and delivery models: opportunity and challenges. Advanced Science Letters, 24(6), 4040-4044.

[29] Salam, A., Gilani, Z., & Haq, S. U. (2015). Deploying and Managing a Cloud Infrastructure: Real-World Skills for the CompTIA Cloud+ Certification and Beyond: Exam CV0-001. John Wiley & Sons.

[30] Abdalla, P. A., & Varol, A. (2019, June). Advantages to Disadvantages of Cloud Computing for Small-Sized Business. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[31] Worku, J. (2017). Defining an Effective Security Policy for Companies using Cloud Computing. Doctoral dissertation, Preston University Kohat, Islamabad Campus.

[32] Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. International Journal of Computer Sciences and Engineering, 7(2), 421-426.

[33] Chakraborty, S., Das, S., & Patra, S. (2017). A Brief Study To Cloud. International Journal of Scientific & Engineering Research, 8(3), 50-54.

[34] Zhu, S. Y., Hill, R., & Trovati, M. (Eds.). (2016). Guide to security assurance for cloud computing. Springer.

[35] Murugesan, S., & Bojanova, I. (Eds.). (2016). Encyclopedia of cloud computing. John Wiley & Sons.

[36] Sharkh, M. A., Kanso, A., Shami, A., & Öhlén, P. (2016). Building a cloud on earth: A study of cloud computing data center simulators. Computer Networks, 108, 78-96.

[37] Frisardi, D. (2020). Cloud Computing Solutions and Business Model Innovation: A case study in the financial services industry. Master thesis, Delft University of Technology, Management of Technology, Faculty of Technology, Policy and Management.

[38] Almajalid, R. (2017). A survey on the adoption of cloud computing in education sector. arXiv preprint arXiv:1706.01136.

[39] Jorrigala, V. (2018). Business Continuity and Disaster Recovery Plan for Information Security. Faculty of Saint Cloud State University, Master of Science in Information Assurance.

[40] Rad, B. B., Diaby, T., & Rana, M. E. (2017, June). Cloud computing adoption: a short review of issues and challenges. In Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government (pp. 51-55).

[41] Aljawarneh, S. (Ed.). (2015). Advanced research on cloud computing design and applications. IGI Global.

[42] Gritzalis, S., Weippl, E. R., Kotsis, G., Tjoa, A. M., & Khalil, I. (Eds.). (2020). Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings (Vol. 12395). Springer Nature.

[43] Rizvi, S., Roddy, H., Gualdoni, J., & Myzyri, I. (2017). Three-step approach to qos maintenance in cloud computing using a third-party auditor. Procedia computer science, 114, 83-92.

[44] Zanoon, N. (2015). Toward Cloud Computing: Security and Performance. International Journal on Cloud Computing: Services and Architecture, 5(5/6), 17-26.

[45] Duan, Q. (2017). Cloud service performance evaluation: status, challenges, and opportunities–a survey from the system modeling perspective. Digital Communications and Networks, 3(2), 101-111.

[46] Kumari, P., & Kaur, P. (2018). A survey of fault tolerance in cloud computing. Journal of King Saud University-Computer and Information Sciences.

[47] Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A systematic review on cloud storage mechanisms concerning e-healthcare systems. Sensors, 20(18), 5392.

[48] Rosati, P., Fowley, F., Pahl, C., Taibi, D., & Lynn, T. (2018, March). Right scaling for right pricing: A case study on total cost of ownership measurement for cloud migration. In International Conference on Cloud Computing and Services Science (pp. 190-214). Springer, Cham.

[49] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

[50] Ismail, M., & Yusuf, B. (2016). Ensuring data storage security in cloud computing with advanced encryption standard (AES) and authentication scheme (AS). Int. J. Inf. Syst. Eng, 4(1), 18-39.

[51] Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., ... & Kim, K. I. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. Electronics, 10(15), 1811.

[52] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6(1), 1-22.

[53] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[54] Waseem, M., Lakhan, A., & Jamali, I. A. (2016). Data security of mobile cloud computing on cloud server. Open Access Library Journal, 3(4), 1-11.

[55] Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57-65.

[56] Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.

[57] Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and access management as security-as-a-service from clouds. Procedia Computer Science, 79, 170-174.

[58] Alhassan, M., & Adjei-Quaye, A. (2017). Information Security in an Organization. International Journal of Computer (IJC). pp 100-116.

[59] Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. NIST special publication, 800(12), 101.

[60] Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global.

[61] Hosseinzadeh, S., Sequeiros, B., Inácio, P. R., & Leppänen, V. (2020). Recent trends in applying TPM to cloud computing. Security and Privacy, 3(1), e93.

[62] Di Pietro, R., & Lombardi, F. (2018). Virtualization Technologies and Cloud Security: advantages, issues, and perspectives. In From Database to Cyber Security (pp. 166-185). Springer, Cham.

[63] Safonov, V. O. (2016). Trustworthy cloud computing. John Wiley & Sons.

[64] Movahedisefat, M. R., Farshchi, S. M. R., & Mohammadpur, D. (2014). Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure. In Emerging Trends in ICT Security (pp. 379-393). Morgan Kaufmann.

[65] Boutaba, R., Zhang, Q., & Zhani, M. F. (2014). Virtual machine migration in cloud computing environments: Benefits, challenges, and approaches. In Communication Infrastructures for Cloud Computing (pp. 383-408). IGI Global.

[66] Alenezi, M. (2021). Safeguarding Cloud Computing Infrastructure: A Security Analysis. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 37(2), 159-167.

[67] Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. IEEE Access, 7, 147420-147452.

[68] Ibrahim, F. A., & Hemayed, E. E. (2019). Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review. Computers & Security, 82, 196-226.

[69] Chakraborty, M., Singh, M., Balas, V. E., & Mukhopadhyay, I. (2021). The "Essence" of Network Security: An End-to-End Panorama. Springer Nature.

[70] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[71] Simpson, S. (2018). SAFECode whitepaper: Fundamental practices for secure software development 3rd edition. In ISSE 2018 Securing Electronic Business Processes (pp. 1-38). Springer Vieweg, Wiesbaden.

[72] Williams, L. (2019). Secure software lifecycle knowledge area. The National Cyber Security Centre.

[73] Samani, R., Reavis, J., & Honan, B. (2014). CSA guide to cloud computing: Implementing cloud privacy and security. Syngress.

[74] Pitropakis, N. (2015). Detecting malicious insider threat in cloud computing environments. Doctoral dissertation, Πανεπιστήμιο Πειραιώς. Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών. Τμήμα Ψηφιακών Συστημάτων.

[75] Hassan, W., Chou, T. S., Li, X., Appiah-Kubi, P., & Tamer, O. (2019). Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks. Int J Inf & Commun Technol ISSN, 2252(8776), 8776.

[76] Legg, P. A. (2015, October). Visualizing the insider threat: challenges and tools for identifying malicious user activity. In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 1-7). IEEE.

[77] Callejas, J. T., & Flores & Dumitriu, P. (2019). Managing cloud computing services in the United Nations system. report of the Joint Inspection Unit.

[78] Turuk, A. K., Sahoo, B., & Addya, S. K. (Eds.). (2016). Resource Management and Efficiency in Cloud Computing Environments. IGI Global.

[79] Mendoza, A., & Gu, G. (2018, May). Mobile application web api reconnaissance: Web-to-mobile inconsistencies & vulnerabilities. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 756-769). IEEE.

[80] Black, P., Badger, M., Guttman, B., & Fong, E. (2016). Dramatically reducing software vulnerabilities: Report to the white house office of science and technology policy (No. NIST Internal or Interagency Report (NISTIR) 8151 (Draft)). National Institute of Standards and Technology.

[81] Bhunia, S., & Tehranipoor, M. (2018). Hardware security: a hands-on learning approach. Morgan Kaufmann.

[82] Conrad, E., Misenar, S., & Feldman, J. (2016). Eleventh Hour CISSP®: Study Guide. Syngress.

[83] Kumar, K. S., & Kisore, N. R. (2014, December). Protection against buffer overflow attacks through runtime memory layout randomization. In 2014 International Conference on Information Technology (pp. 184-189). IEEE.

[84] Vacca, J. R. (2017). Computer and information security handbook. 3rd Edition. Newnes.

[85] Sumitra, B., Pethuru, C. R., & Misbahuddin, M. (2014). A survey of cloud authentication attacks and solution approaches. Int. J. Innov. Res. Comput. Commun. Eng, 2(10), 6245-6253.

[86] Xu, L. (2017). Pseudonymization and its Application to Cloud-based eHealth Systems. Doctoral dissertation. Mathematisch-Naturwissenschaftlichen, Fakultät der Rheinischen Friedrich Wilhelms Universität Bonn.

[87] Shaikh, A. A. (2016, October). Attacks on cloud computing and its countermeasures. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 748-752). IEEE.

[88] Sharma, S., & Singh, R. P. (2019). A Critical Survey on: Cloud Security and privacy issues and its associated solutions. International Journal of Computer Sciences and Engineering, Vol.-7, Issue-8 (pp. 288-296).

[89] Bonguet, A., & Bellaiche, M. (2017). A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. Future Internet, 9(3), 43.

[90] Deka, R. K., Bhattacharyya, D. K., & Kalita, J. K. (2021). Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment. Big Data Analytics for Internet of Things, 285-319.

[91] Papadie, R., & Apostol, I. (2017, June). Analyzing websites protection mechanisms against DDoS attacks. In 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-6). IEEE.

[92] Saxena, R., & Dey, S. (2019). DDoS prevention using third party auditor in cloud computing. Iran Journal of Computer Science, 2(4), 231-244.

[93] Mavromoustakos, S., Patel, A., Chaudhary, K., Chokshi, P., & Patel, S. (2016, December). Causes and prevention of SQL injection attacks in web

applications. In Proceedings of the 4th International Conference on Information and Network Security (pp. 55-59).

[94] Yasin, A. F., & Zidan, N. (2016). SQL injection prevention using query dictionary based mechanism. International Journal of Computer Science and Information Security, 14(6), 479.

[95] Kaplan, J., Richter, W., & Ware, D. (2019). Cybersecurity: Linchpin of the digital enterprise. As Companies Digitize Businesses and Automate Operations, Cyberrisks Proliferate.

[96] Garcia, T. (2019, December). What is Cloud Security Control? Reciprocity. https://reciprocity.com/resources/what-is-cloud-security-control/ (Πρόσβαση στις 28 ΣΕΠ 2021).

[97] Casetto, O. (2021, March). Cloud Security: Principles, Solutions, and Architectures. exabeam.com. https://www.exabeam.com/information-security/cloud-security/ (Πρόσβαση στις 28 ΣΕΠ 2021).

[98] Sahana, S., & Sarddar, D. (2019). Application Safety and Service Vulnerability in Cloud Network. Security Designs for the Cloud, Iot, and Social Networking, 77-95.

[99] Germouty, P. (2018). Identity-based cryptography. Doctoral dissertation, Limoges.

[100] Phaneendra, H. D. (2014). Identity-based cryptography and comparison with traditional public key encryption: A survey. International Journal of Computer Science and Information Technologies, 5(4), 5521-5525.

[101] Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1-37.

[102] Thales Blog. (2019, September). Identity-based Cryptography. https://cpl.thalesgroup.com/blog/access-management/identity-based-cryptography (Πρόσβαση στις 28 ΣΕΠ 2021).

[103] Aalam, Z., Kumar, V., & Gour, S. (2021, August). A review paper on hypervisor and virtual machine security. In Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012027). IOP Publishing.

[104] Huang, D., & Wu, H. (2017). Mobile cloud computing: foundations and service models. Morgan Kaufmann.

[105] Morgan, B., Alata, E., Nicomette, V., & Kaâniche, M. (2018). IOMMU protection against I/O attacks: a vulnerability and a proof of concept. Journal of the Brazilian Computer Society, 24(1), 1-11.

[106] Chandramouli, R., & Chandramouli, R. (2016). Secure virtual network configuration for virtual machine (vm) protection. NIST Special Publication, 800, 125B.

[107] Sabillon, R. (2021). Audits in Cybersecurity. Research Anthology on Business Aspects of Cybersecurity, 1-18.

[108] Gangolly, J. S. (2016). American institute of certified public accountants, INC., Audit analytics and continuous audit: Looking towards the future. Journal of Emerging Technologies in Accounting, 13(1), 187-188.

[109] Ismail, U. M., Islam, S., Ouedraogo, M., & Weippl, E. (2016). A framework for security transparency in cloud computing. Future Internet, 8(1), 5.

[110] Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., & Dubois, E. (2015). Security transparency: the next frontier for security research in the cloud. Journal of Cloud Computing, 4(1), 1-14.

[111] Jarraya, Y., Zanetti, G., Pietikäinen, A., Obi, C., Ylitalo, J., Nanda, S., ... & Pourzandi, M. (2017). Securing the cloud with compliance auditing. Ericsson Review, 95(2), 38-47.

[112] Zhou, Y., Zheng, S., & Wang, L. (2020). Privacy-preserving and efficient public key encryption with keyword search based on cp-abe in cloud. Cryptography, 4(4), 28.

[113] Zheng, Q., Xu, S., & Ateniese, G. (2014, April). VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. In IEEE INFOCOM 2014-IEEE conference on computer communications (pp. 522-530). IEEE.

[114] Mascia, C., Sala, M., & Villa, I. (2021). A survey on Functional Encryption. arXiv preprint arXiv:2106.06306.

[115] Shrestha, R., & Kim, S. (2019). Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities. In Advances in Computers (Vol. 115, pp. 293-331). Elsevier.

[116] Liu, C., Zhu, L., & Chen, J. (2017). Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud. Journal of Network and Computer Applications, 86, 3-14.

[117] Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal, 44(3), 23-38.

[118] Abdulhameed, I. S. (2021). The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 1979-1992.

[119] Ibrahim, A., Mahmood, B., & Singhal, M. (2016, May). A secure framework for sharing electronic health records over clouds. In 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH) (pp. 1-8). IEEE.

[120] Koranga, M. (2016). Advanced Cyber Security Techniques. Post-Graduate Diploma in Cyber Security. Uttarakhand Open University, New Delhi.

[121] Matheny, M., Israni, S. T., Ahmed, M., & Whicher, D. (2019). Artificial intelligence in health care: the hope, the hype, the promise, the peril. NAM Special Publication. Washington, DC: National Academy of Medicine, 154.

[122] Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). A secure cloud computing system by using encryption and access control model. Journal of Information Processing Systems, 15(3), 538-549.

[123] Wu, F., & Eagles, S. (2016). Cybersecurity for medical device manufacturers: ensuring safety and functionality. Biomedical instrumentation & technology, 50(1), 23-34.

[124] Hansen, J., Wilson, P., Verhoeven, E., Kroneman, M., Kirwan, M., Verheij, R., & van Veen, E. B. (2021). Assessment of the EU Member States' rules on health data in the light of GDPR.

[125] Zhao, X., Garg, S., Queiroz, C., & Buyya, R. (2017). Software Architecture for Big Data and the Cloud. Morgan Kaufmann.

[126] Obaidat, M., Brown, J., Obeidat, S., & Rawashdeh, M. (2020). A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication. Sensors, 20(15), 4212.

[127] Bertram, L.A., & van Dooble, G. (2019) Nomenclatura - Encyclopedia of modern Cryptography and Internet Security: From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys. BoD – Books on Demand.

[128] Zhang, K., & Shen, X. S. (2015). Security and privacy for mobile healthcare networks. Springer.

[129] Sarkar, B. K. (2017). Big data for secure healthcare system: a conceptual design. Complex & Intelligent Systems, 3(2), 133-151.

[130] Mukherjee, S., Ray, I., Ray, I., Shirazi, H., Ong, T., & Kahn, M. G. (2017, March). Attribute based access control for healthcare resources. In Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control (pp. 29-40).

[131] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 5, 22313-22328.

[132] Marwan, M., Kartit, A., & Ouahmane, H. (2017, July). Protecting medical data in cloud storage using fault-tolerance mechanism. In Proceedings of the 2017 international conference on smart digital environment (pp. 214-219).

[133] Galletta, A., Bonanno, L., Celesti, A., Marino, S., Bramanti, P., & Villari, M. (2017, July). An approach to share MRI data over the Cloud preserving patients' privacy. In 2017 IEEE Symposium on Computers and Communications (ISCC) (pp. 94-99). IEEE.

[134] Smithamol, M. B., & Rajeswari, S. (2017). Hybrid solution for privacy-preserving access control for healthcare data. Advances in Electrical and Computer Engineering, 17(2), 31-38.

[135] Dhivya, B., Ibrahim, S. P. S., & Kirubakaran, R. (2017). Hybrid cryptographic access control for cloud based electronic health records systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(2).

[136] Shah, K., & Prasad, V. (2017). Security for healthcare data on cloud. International Journal on Computer Science and Engineering (IJCSE), 9(5).

[137] Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. International Journal of Healthcare Management, 10(2), 135-146.

[138] Ruley, M., Walker, V., Studeny, J., & Coustasse, A. (2018). The nationwide health information network: the case of the expansion of health information exchanges in the United States. The health care manager, 37(4), 333-338.

[139] ISO/IEC 27001 (2016). Information Technology: Security Techniques, Systems Requirements, ISO/IEC 27001, Geneva, Switzerland.

[140] ISO/IEC 27002 (2016). Information Technology: Security Techniques - Code of Practice for Information Security Management, ISO/IEC 27001, Geneva, Switzerland.

[141] Gibbs, S. (2016). European parliament approves tougher data privacy rules. The Guardian, 14.

[142] Minniti, M. J., Blue, T. R., Freed, D., & Ballen, S. (2016). Patient-interactive healthcare management, a model for achieving patient experience excellence. In Healthcare Information Management Systems (pp. 257-281). Springer, Cham.

[143] Azarm, M. (2020). A Patient-Centered Framework for System-Level Sharing of Health Records. Doctoral dissertation, Université d'Ottawa/University of Ottawa.

[144] Riefa, C., & Saintier, S. (Eds.). (2020). Vulnerable Consumers and the Law: Consumer Protection and Access to Justice. Routledge.

[145] Hermes, S., Riasanow, T., Clemons, E. K., Böhm, M., & Krcmar, H. (2020). The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. Business Research, 13(3), 1033-1069.

[146] Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. Symmetry, 12(7), 1191.

[147] Ramji, S. (2021, March). The evolving role of user experience in security. Security magazine. https://www.securitymagazine.com/articles/94909-the-evolving-role-of-user-experience-in-security (Πρόσβαση την 01 ΟΚΤ 2021).

[148] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.