ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ (ΕΔΡΑ ΣΠΑΡΤΗ)

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
«ΑΝΑΛΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΟΥ ΔΙΚΤΥΟΥ ΠΟΥ ΒΑΣΙΖΕΤΑΙ ΣΕ CLOUD ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΗ ΜΕΘΟΔΟ ΤΟΥ SECRET SHARING»

ΕΠΙΜΕΛΕΙΑ ΕΡΓΑΣΙΑΣ:

ΕΥΜΟΡΦΙΑ-ΜΑΡΙΑ ΜΑΚΡΑΝΔΡΕΟΥ Α.Μ. : 2012021

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΙΩΑΝΝΗΣ ΠΙΚΡΑΜΜΕΝΟΣ

ΣΠΑΡΤΗ 2018

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Α
2. Β
3. Γ

Τόπος_____

Ημερομηνία_____

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνουμε ενυπογράφως ότι είμαστε αποκλειστικοί συγγραφείς της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχουμε αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνουμε την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαστε υπόλογοι έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μας Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνουμε, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμάς προσωπικά και αποκλειστικά και ότι, αναλαμβάνουμε πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μας ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Όνομα και Επώνυμο Συγγραφέων (Με Κεφαλαία):

……

Υπογραφή (Ολογράφως, χωρίς μονογραφή):

……

Ημερομηνία (Ημέρα – Μήνας – Έτος):

……

Πίνακας περιεχομένων

Ιστορικό 7

Εισαγωγή 9

1ο Κεφάλαιο: Cloud computing 11

1.1 Τι είναι το Cloud computing και ποια τα βασικά χαρακτηριστικά του 11

1.2 Βασικά είδη μοντέλων υπηρεσιών που μας προσφέρει το cloud computing 16

1.2.1 Βασικά είδη εφαρμογών που μας προσφέρει το cloud computing 20

1.2.2 Άλλα μοντέλα ανάπτυξης 23

1.3 Αρχιτεκτονική του cloud computing 26

1.3.1 Μέθοδοι και συστήματα για την παροχή αρχιτεκτονικών ανάπτυξης σε περιβάλλοντα υπολογιστικού νέφους 27

1.4 Πως δουλεύει το cloud computing 36

1.5 Συστήματα και μέθοδοι για την ανάπτυξη δεδομένων cloud με βάση προτιμώμενες και / ή υπάρχουσες σχέσεις συνδρομής 37

2ο Κεφάλαιο: Ασφάλεια στο cloud computing 44

2.1 Περιορισμοί και μειονεκτήματα 46

2.2 Προκλήσεις ασφάλειας υπολογιστών cloud 47

2.3 Μυστική κοινή χρήση 52

2.4 Το σχέδιο του Adi Shamir 53

2.5 Το σχέδιο του George Blakley 57

2.6 Μυστική κοινή χρήση χρησιμοποιώντας το θεώρημα του κινέζικου υπολοίπου 58

2.7 Μοντέλο Πολλαπλών Σύννεφων 62

2.8 Προληπτική μυστική κοινή χρήση 65

2.9 Επαληθεύσιμη μυστική κοινή χρήση 66

2.10 Υπολογιστικά ασφαλής μυστική κοινή χρήση 66

2.11 Πολλαπλή μυστική και αποτελεσματική διανομή (διαδοχικά) μυστική κοινή χρήση 67

2.12 Ασφαλής έναντι ανασφαλής μυστική κοινή χρήση 68

3ο Κεφάλαιο: MULTI CLOUD 72

3.1 Αρχιτεκτονική multi- cloud για την παροχή απορρήτου δεδομένων και ακεραιότητας. 73

3.2 Προσέγγιση ασφάλειας για την αποθήκευση δεδομένων σε multi-cloud 77

3.3 Συγκριτική μελέτη των μηχανισμών ασφαλείας σε multi-cloud περιβάλλον 78

3.4 Συνδυασμός μυστικής κοινής χρήσης και υπολογιστικού νέφους 79

3.5 Λειτουργία μυστικής κοινής χρήσης για εξασφάλιση multi-clouds στο cloud computing και τις εφαρμογές στην κρυπτογραφία κατωφλίου 80
4ο Κεφάλαιο: Ασφάλεια ηλεκτρονικών αρχείων υγείας που βασίζονται σε cloud 84
4.1 Ανάλυση των απαιτήσεων ασφάλειας και ιδιωτικού απορρήτου των συστημάτων ηλεκτρονικών αρχείων υγείας που βασίζονται σε cloud 84
4.2 Ηλεκτρονικό αρχείο καταγραφής της υγείας και θέματα ιδιωτικότητας 85
4.3 Απαιτήσεις ασφάλειας ηλεκτρονικών δεδομένων υγείας και ιδιωτικού απορρήτου 86
4.3.1 Τα κύρια χαρακτηριστικά της ηλεκτρονικής υγείας 89
4.4 Θέματα ασφάλειας και ιδιωτικού απορρήτου λύσεων υγείας που βασίζονται σε σύννεφα 91
4.5 Πρόσβαση βάσει ρόλων 92
4.6 Μηχανισμοί ασφάλειας δικτύων 93
4.7 Κρυπτογράφηση δεδομένων και Ψηφιακή υπογραφή 94
4.8 Παρακολούθηση της πρόσβασης στο σύστημα 97
4.9 Προτάσεις πριν γίνει μετακίνηση ηλεκτρονικών αρχείων υγείας στο Cloud 98
4.10 Διάφορα ζητήματα ασφάλειας που πρέπει να λαμβάνει υπόψη ο πελάτης κατά την επιλογή του καταλληλότερου παροχέα 99
4.11 Μετακίνηση Ηλεκτρονικών Αρχείων Υγείας στο Σύννεφο: Παράδειγμα Απαιτήσεων Ασφαλείας της Εταιρείας Cloud 101
5ο Κεφάλαιο: Μυστική κοινή χρήση δεδομένων υγείας 111
5.1 Μυστική κοινή χρήση δεδομένων υγείας σε πολλούς παρόχους υπηρεσιών σύννεφου 111
5.1.1 Στόχοι στην ασφάλεια και την ιδιωτικότητα 113
5.2 Μυστική κοινή χρήση των δεδομένων Υγείας του Internet of Things(IoT) 114
5.2.1 Αρχιτεκτονική υγειονομικής υποστήριξης βάση το IoT 114
5.2.2 Ροή εργασιών υγειονομικής περίθαλψης 116
5.3 Ηλεκτρονικά αρχεία υγείας: Πώς μοιράζονται τα συστήματα 117
5.4 Προκλήσεις διαλειτουργικότητας των EHR(ηλεκτρονικών αρχείων υγείας)που πρέπει να επικεντρωθούν στις εταιρίες πληροφορικής: 118
5.5 Μέτρα ασφαλείας 120
5.5.1 Συστήματα και μέθοδοι για ασφαλή κοινή χρήση δεδομένων 121
5.6 Super Users - το μυστικό όπλο για την εκπαίδευση InfoSec για την παροχή ασφάλειας στην υγειονομική περίθαλψη 124
Συμπεράσματα 126
Λύση/Πρόταση Βελτίωσης 127

Βιβλιογραφία 129

Ιστορικό

Οι έννοια του Cloud Computing υπάρχει εδώ και πολλά χρόνια.

Η εξέλιξή του άρχισε να ξεκινάει από το 1950, με τη χρήση υπολογιστών mainframe.

Πολλοί χρήστες είχαν την δυνατότητα να έχουν πρόσβαση σε έναν κεντρικό υπολογιστή μέσω τερματικών σταθμών, των οποίων η μόνη λειτουργία ήταν η πρόσβαση στο mainframe. Λόγω του κόστους για να αγοραστούν και να διατηρηθούν οι υπολογιστές mainframe, δεν ήταν πρακτικό για έναν οργανισμό να αγοράσει και να διατηρήσει έναν για κάθε εργαζόμενο. Ούτε ο απλός χρήστης χρειάζεται την μεγάλη ικανότητα αποθήκευσης και την ισχύ επεξεργασίας που παρείχε ένα mainframe. Η παροχή κοινής πρόσβασης σε έναν και μοναδικό πόρο ήταν η λύση που έκανε οικονομικά λογική αυτή την προηγμένη τεχνολογία.

Μετά από λίγο καιρό, περίπου το 1970, δημιουργήθηκε η έννοια των εικονικών μηχανών (VM). Χρησιμοποιώντας λογισμικό virtualization όπως το VMware, κατέστη δυνατή η ταυτόχρονη εκτέλεση ενός ή περισσοτέρων λειτουργικών συστημάτων σε απομονωμένο περιβάλλον.

Το λειτουργικό σύστημα VM πήρε το mainframe κοινής πρόσβασης της δεκαετίας του '50 στο επόμενο επίπεδο, επιτρέποντας σε πολλά διαφορετικά περιβάλλοντα υπολογιστών να διαμένουν σε ένα φυσικό περιβάλλον. Ο εικονικοποιητής γνώριζε την τεχνολογία, που αποτελούσε τον ευρύτερο καταλύτη στην επικοινωνία και την πληροφορική εξέλιξη.

Τη δεκαετία του 1990 οι εταιρίες τηλεπικοινωνιών άρχισαν να προσφέρουν εικονικές διασυνδέσεις ιδιωτικού δικτύου.

Ιστορικά, οι εταιρείες τηλεπικοινωνιών προσέφεραν μόνο μοναδικές συνδέσεις δεδομένων από σημείο σε σημείο. Αντί να δημιουργήσουν φυσική υποδομή για να επιτρέψουν σε περισσότερους χρήστες να έχουν τις δικές τους συνδέσεις, οι εταιρείες τηλεπικοινωνιών ήταν πλέον σε θέση να παρέχουν στους χρήστες κοινή πρόσβαση στην ίδια φυσική υποδομή.

Η παρακάτω λίστα λοιπόν, εξηγεί συνοπτικά την εξέλιξη του cloud computing:

- Grid computing: Επίλυση σημαντικών προβλημάτων με τον παράλληλο υπολογισμό
- Υπολογιστική χρησιμότητα: Προσφορά υπολογιστικών πόρων
- SaaS: Συνδρομές σε εφαρμογές βάσει δικτύου
- Cloud computing: Οποτεδήποτε και οπουδήποτε πρόσβαση στους πόρους πληροφορικής που παρέχονται δυναμικά ως υπηρεσία

Εισαγωγή

Για χρόνια το Διαδίκτυο έχει εκπροσωπηθεί από το cloud έως το 2008, όταν άρχισαν να εμφανίζονται διάφορες νέες υπηρεσίες που επέτρεψαν την πρόσβαση σε υπολογιστικούς πόρους μέσω του Διαδικτύου που ονομάζονταν cloud computing. Το Cloud Computing μπορεί να χαρακτηριστεί από ένα σύνολο κινούμενων ή υπολογιστικών στοιχείων, όπως την επεξεργασία των στοιχείων του ενεργητικού ισχύος, δικτύου και αποθήκευσης από επιτραπέζιους υπολογιστές και servers για να εντοπίζονται γεγονότα και τα στοιχεία των κόμβων που φιλοξενείται από εταιρείες όπως η Amazon, η Google, η Microsoft, κ.λπ. Το Cloud computing περιλαμβάνει δραστηριότητες όπως η χρήση ιστότοπων κοινωνικής δικτύωσης και άλλων μορφών πληροφορικής. Το Cloud computing είναι ένας τρόπος για να αυξήσετε τη δυναμικότητα ή να προσθέσετε δυνατότητες χωρίς να επενδύσετε σε νέες υποδομές, να εκπαιδεύσετε νέο προσωπικό ή να χορηγήσετε άδεια χρήσης νέου λογισμικού. Επεκτείνει τις υπάρχουσες δυνατότητες της τεχνολογίας πληροφοριών (IT).

Γνωστό για τα πολλαπλά οφέλη, το υπολογιστικό νέφος υιοθετείται όλο και περισσότερο μεταξύ των επιχειρήσεων. Η σχετικά νέα τεχνολογία μπορεί να απλοποιήσει την ανταλλαγή πληροφοριών μεταξύ των διαφορετικών επιχειρηματικών εταίρων όπως επίσης και στον τομέα της υγείας. Τα ηλεκτρονικά αρχεία υγείας (ΕΓΔ) σε ένα περιβάλλον υπολογιστικού νέφους προσελκύουν τόσο τον ακαδημαϊκό χώρο όσο και τους επαγγελματίες.

Αποτελεί πρόκληση ο τομέας της υγειονομικής περίθαλψης που βασίζεται στο cloud και ταυτόχρονα έχει γίνει ένα δύσκολο πεδίο εξέτασης η ασφάλεια των πληροφοριών, λόγω της πολύπλοκης φύσης των δεδομένων και της ιδιωτικής ζωής. Από τότε που τα συστήματα υγειονομικής περίθαλψης έχουν εφαρμοστεί , η ασφάλεια τους εξετάζεται ως ένα σημαντικό θέμα, ιδίως το γεγονός ότι τα δεδομένα περιλαμβάνουν εξαιρετικά ευαίσθητες πληροφορίες. Η προοπτική της αποθήκευσης πληροφοριών υγείας σε ηλεκτρονική μορφή εγείρει ανησυχίες για

τη προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Οποιαδήποτε προσπάθεια να δημιουργηθούν ηλεκτρονικά πληροφοριακά συστήματα υγειονομικής περίθαλψης θα πρέπει να διασφαλίζεται από ικανοποιητική και πλήρη προστασία εμπιστευτικότητας και ακεραιότητας των πληροφοριών του ασθενούς. Επίσης οι πληροφορίες του ασθενή πρέπει να είναι άμεσα διαθέσιμες σε όλους τους εξουσιοδοτημένους παρόχους υπηρεσιών υγειονομικής περίθαλψης, προκειμένου να εξασφαλίσουν τη σωστή θεραπεία-νοσηλεία του ασθενούς.

Επίσης, προκειμένου να δημιουργηθούν εξαιρετικά αξιόπιστες εφαρμογές, είναι κατάλληλη μια αρχιτεκτονική multi-cloud. Στόχος είναι να γίνει η μετεγκατάσταση των συστημάτων cloud-based που τρέχουν σε πολλαπλά ανεξάρτητα σύννεφα.

1ο Κεφάλαιο: Cloud computing

1.1 Τι είναι το Cloud computing και ποια τα βασικά χαρακτηριστικά του

Cloud computing : είναι ένα παράδειγμα τεχνολογίας πληροφορική (IT) που επιτρέπει τη πρόσβαση σε κοινόχρηστες δεξαμενές διαμορφωμένων πόρων συστήματος και υπηρεσιών υψηλότερου επιπέδου όπου μπορούν γρήγορα να παρέχονται με ελάχιστη προσπάθεια διαχείρισης, συχνά μέσω του διαδικτύου . Το Cloud computing βασίζεται στην ανταλλαγή πόρων για την επίτευξη συνοχής και την οικονομίας κλίμακας. Τα σύννεφα τρίτων μερών επιτρέπουν στους οργανισμούς να επικεντρωθούν στις βασικές τους επιχειρήσεις, αντί να δαπανήσουν πόρους για την υποδομή και τη συντήρηση των υπολογιστών. Επίσης επιτρέπει στις εταιρείες να αποφεύγουν ή να ελαχιστοποιούν τα αρχικά κόστη υποδομής πληροφορικής. Οι υποστηρικτές ισχυρίζονται ότι το cloud computing επιτρέπει στις επιχειρήσεις να κάνουν πιο γρήγορες τις εφαρμογές τους με βελτιωμένη διαχειρισιμότητα και λιγότερη συντήρηση και επιτρέπει στις ομάδες τεχνολογίας πληροφορικής να προσαρμόζουν ταχύτερα τους πόρους για να ανταποκριθούν στη διακυβευόμενη και απρόβλεπτη επιχειρηματική ζήτηση. Οι προμηθευτές σύννεφων συνήθως χρησιμοποιούν ένα μοντέλο "pay-as-you-go", το οποίο μπορεί να οδηγήσει σε μη αναμενόμενα λειτουργικά έξοδα ,εάν οι διαχειριστές δεν εξοικειωθούν με τα μοντέλα τιμολόγησης νέφους.

Η διαθεσιμότητα δικτύων υψηλής χωρητικότητας, χαμηλού κόστους υπολογιστές και συσκευές αποθήκευσης καθώς και η ευρεία υιοθέτηση του virtualization υλικού, της προσανατολισμένης και αυτόνομης αρχιτεκτονικης στις υπηρεσίες χρησιμότητας υπολογιστών οδήγησαν στην ανάπτυξη του cloud computing.

Χαρακτηριστικά:

- Virtual
- Βάση δεδομένων, λειτουργικά συστημάτων, λογισμικό, web servers, αποθήκευση και δικτύωση ως εικονικοί servers.

- Κόστος: Οι μειώσεις κόστους απαιτούνται από τους παρόχους cloud. Ένα μοντέλο παροχής δημόσιου cloud μετατρέπει τις κεφαλαιουχικές δαπάνες (π.χ. αγορές διακομιστών) στις επιχειρησιακές δαπάνες. Αυτό στην ουσία μειώνει τα εμπόδια στην είσοδο, καθώς η υποδομή παρέχεται συνήθως από τρίτο μέρος και δεν χρειάζεται να αγοραστεί για ενίοτε ή σπάνια εντατικά υπολογιστικά καθήκοντα. Η τιμολόγηση σε βάση υπολογιστικής χρησιμότητας είναι λεπτής σημασίας με επιλογές χρέωσης που βασίζονται στη χρήση. Επίσης,δεν απαιτούνται μέγιστες δεξιότητες πληροφορικής για την υλοποίηση έργων που χρησιμοποιούν cloud computing.Αρκετά άρθρα που εξετάζουν λεπτομερός τις πτυχές κόστους, τα περισσότερα από τα οποίας καταλήγουν στο συμπέρασμα ότι το κόστος, η εξοικονόμηση εξαρτάται από τον τύπο των υποστηριζόμενων δραστηριοτήτων και από τον τύπο της διαθέσιμης υποδομής στο εσωτερικό της επιχείρησης.
- Η πολυεθνική επιτρέπει την ανταλλαγή πόρων και κόστους σε μια μεγάλη ομάδα χρηστών, επιτρέποντας έτσι:
- Αύξηση χωριτικότητας μέγιστου φορτίου(οι χρήστες δεν χρειάζεται να κατασκευάζουν μηχανήματα και να πληρώνουν τους πόρους και τον εξοπλισμό για να καλύψουν τα υψηλότερα δυνατά φορτία),συγκέντρωση της υποδομής σε τοποθεσίες με χαμηλότερο κόστος και αξιοποίηση και βελτίωση της αποδοτικότητας για συστήματα που χρησιμοποιούνται συχνά μόνο κατά 10-20%.
- Συντήρηση: Η συντήρηση των εφαρμογών του cloud computing είναι ευκολότερη, διότι δεν χρειάζεται να εγκατασταθεί στον υπολογιστή του κάθε χρήστη και μπορεί να προσεγγιστεί από διαφορετικά μέρη.

- Η ανεξαρτησία της συσκευής και της τοποθεσίας επιτρέπει στους χρήστες να έχουν πρόσβαση σε συστήματα χρησιμοποιώντας ένα πρόγραμμα περιήγησης ιστού, ανεξάρτητα από την τοποθεσία τους ή τη συσκευή που χρησιμοποιούν (π.χ. PC, κινητό τηλέφωνο) και δεδομένου ότι η υποδομή είναι εκτός τοποθεσίας (συνήθως παρέχεται από τρίτο μέρος) και προσπελάζεται μέσω του Διαδικτύου, οι χρήστες μπορούν να συνδεθούν με αυτό από οπουδήποτε.
- Παραγωγικότητα: μπορεί να αυξηθεί όταν πολλοί χρήστες μπορούν να εργάζονται ταυτόχρονα για τα ίδια δεδομένα, αντί να περιμένουν να αποθηκευτούν και να αποσταλούν μέσω ηλεκτρονικού ταχυδρομείου. Ο χρόνος μπορεί να αποθηκευτεί, καθώς οι πληροφορίες δεν χρειάζεται να εισαχθούν ξανά όταν τα πεδία αντιστοιχούν, ούτε οι χρήστες πρέπει να εγκαταστήσουν αναβαθμίσεις λογισμικού εφαρμογών στον υπολογιστή τους.
- Απόδοση: παρακολουθείται από έμπειρους ειδικούς πληροφορικής, από τον πάροχο υπηρεσιών και οι συνεπείς και χαλαρά συζευγμένες αρχιτεκτονικές κατασκευάζονται χρησιμοποιώντας υπηρεσίες ιστού ως διεπαφή συστήματος.
- Συγκέντρωση πόρων: είναι ο υπολογιστικός πόρος του παροχέα, που συγχρηματοδοτείται για την εξυπηρέτηση πολλών καταναλωτών χρησιμοποιώντας ένα μοντέλο πολλαπλών μισθωτών, με διαφορετικούς φυσικούς και εικονικούς πόρους δυναμικά εκχωρημένους και ανακαθορισμένους σύμφωνα με τη ζήτηση των χρηστών. Υπάρχει μια αίσθηση ανεξαρτησίας ως προς την τοποθεσία, όμως δεδομένου ότι ο καταναλωτής γενικά δεν έχει κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία του παρεχόμενου πόρου.
- Αξιοπιστία: βελτιώνεται με τη χρήση πολλαπλών πλεονάζοντων τοποθεσιών, γεγονός που καθιστά το σχεδιασμό cloud κατάλληλα σχεδιασμένο για συνεχή λειτουργία και ανάκτηση καταστροφών.
- Εξοικονόμηση και ελαστικότητα: μέσω δυναμικής ("κατ' απαίτηση") προμήθειας πόρων σε λεπτομερή αυτοεξυπηρέτηση σχεδόν σε πραγματικό χρόνο (όπου σημειώνουμε ότι ο χρόνος εκκίνησης του VM ποικίλλει ανάλογα

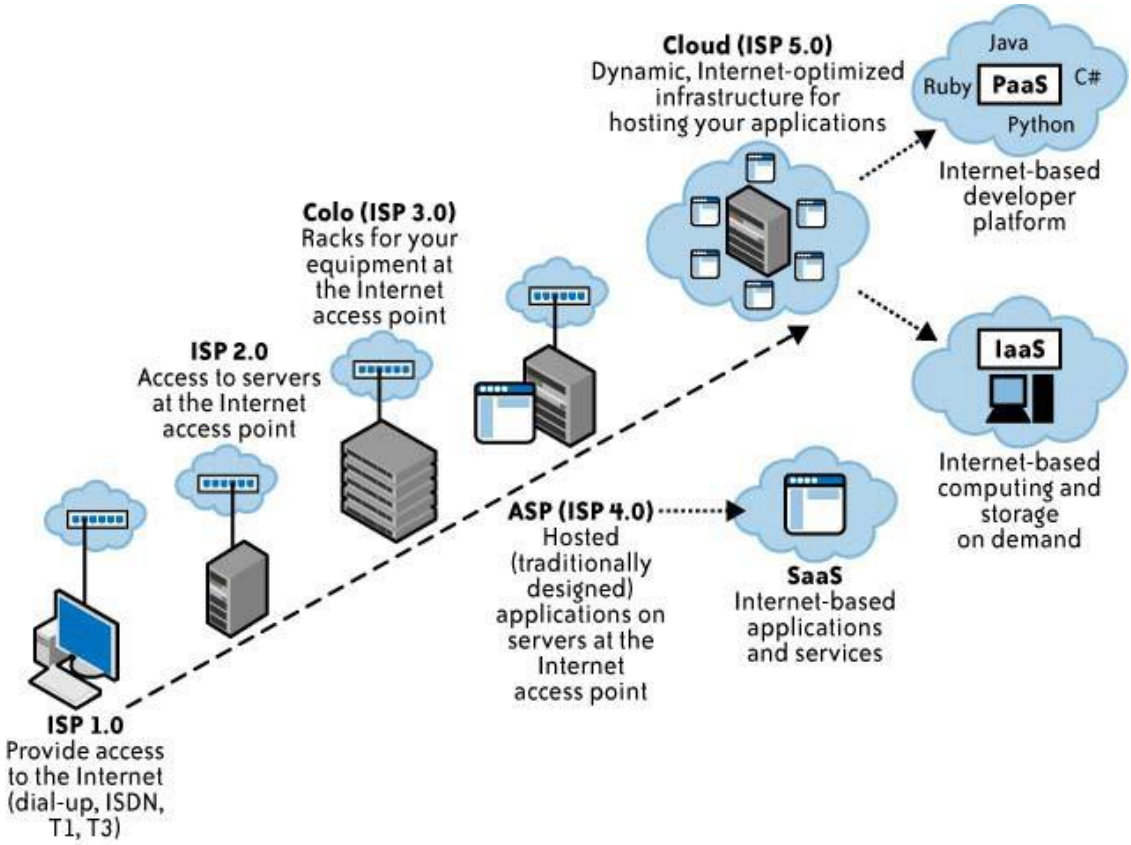
με τον τύπο VM, την τοποθεσία, τους OS και τους παρόχους cloud),χωρίς τους χρήστες να χρειαστεί μηχανική για φορτία αιχμής. Αυτό δίνει τη δυνατότητα να κλιμακωθεί όταν η ανάγκη χρήσης αυξάνεται ή μειώνεται εάν οι πόροι δεν χρησιμοποιούνται.

- Ασφάλεια: μπορεί να βελτιωθεί εξαιτίας της συγκέντρωσης δεδομένων, των αυξημένων πόρων που σχετίζονται με την ασφάλεια κ.λπ., αλλά οι ανησυχίες μπορούν να εξακολουθήσουν να αφορούν την απώλεια ελέγχου ορισμένων ευαίσθητων δεδομένων και την έλλειψη ασφάλειας για τους αποθηκευμένους πυρήνες. Η ασφάλεια είναι συχνά μέγιστη από άλλα παραδοσιακά συστήματα. Εν μέρει επειδή οι πάροχοι υπηρεσιών είναι σε θέση να αφιερώσουν πόρους για την επίλυση ζητημάτων ασφάλειας που πολλοί πελάτες δεν έχουν την οικονομική δυνατότητα αντιμετώπισης ή για τους οποίους δεν διαθέτουν τις τεχνικές ικανότητες που πρέπει να αντιμετωπιστούν, αυξάνεται σημαντικά όταν τα δεδομένα διανέμονται σε ευρύτερη περιοχή ή σε μεγαλύτερο αριθμό συσκευών, καθώς και σε συστήματα πολλαπλών μισθωτών που μοιράζονται μη συνδεδεμένοι χρήστες. Επιπλέον, η πρόσβαση των χρηστών σε αρχεία καταγραφής ελέγχου ασφαλείας μπορεί να είναι δύσκολη ή αδύνατη. Οι ιδιωτικές εγκαταστάσεις cloud ενθαρρύνονται εν μέρει από την επιθυμία των χρηστών να διατηρούν τον έλεγχο της υποδομής και να αποφεύγουν να χάσουν τον έλεγχο της ασφάλειας των πληροφοριών.

Ο ορισμός του cloud computing του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας προσδιορίζει "πέντε βασικά χαρακτηριστικά":

- Αυτοεξυπηρέτηση κατά παραγγελία: Ένας καταναλωτής μπορεί μονομερώς να παρέχει δυνατότητες υπολογιστών, όπως χρόνο διακομιστή και αποθήκευση δικτύου, όπως απαιτείται αυτόματα χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με κάθε πάροχο υπηρεσιών.
- Ευρεία πρόσβαση στο δίκτυο: Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσπελάζονται μέσω τυποποιημένων μηχανισμών που προωθούν τη χρήση από ετερογενείς λεπτές ή παχές πλατφόρμες πελατών (π.χ. κινητά τηλέφωνα, tablet, φορητοί υπολογιστές και σταθμοί εργασίας).

- Συγκέντρωση πόρων: Οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται για να εξυπηρετούν πολλούς καταναλωτές χρησιμοποιώντας μοντέλο πολλαπλών μισθωτών, με διαφορετικούς φυσικούς και εικονικούς πόρους δυναμικά εκχωρημένους και ανακατανομής ανάλογα με τη ζήτηση των καταναλωτών.
- Ταχεία ελαστικότητα: Οι δυνατότητες μπορούν να εφοδιαστούν ελαστικά και να απελευθερωθούν, σε ορισμένες περιπτώσεις αυτομάτως, να κλιμακώνονται ταχέως προς τα έξω και προς τα μέσα ανάλογα με τη ζήτηση. Στον καταναλωτή, οι διαθέσιμες δυνατότητες παροχής υπηρεσιών συχνά εμφανίζονται απεριόριστες και μπορούν να χρησιμοποιηθούν σε οποιαδήποτε ποσότητα ανά πάσα στιγμή.
- Μετρούμενη υπηρεσία: Τα συστήματα Cloud ελέγχουν αυτόματα και βελτιστοποιούν τη χρήση των πόρων, αξιοποιώντας τη δυνατότητα μέτρησης σε κάποιο επίπεδο αφαίρεσης κατάλληλου για τον τύπο υπηρεσίας (π.χ. αποθήκευση, επεξεργασία, εύρος ζώνης και ενεργούς λογαριασμούς χρηστών). Η χρήση των πόρων μπορεί να παρακολουθείται, να ελέγχεται και να αναφέρεται, παρέχοντας διαφάνεια τόσο για τον παροχέα όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας.



Εικόνα 1 Εξέλιξη του cloud

1.2 Βασικά είδη μοντέλων υπηρεσιών που μας προσφέρει το cloud computing

Αν και η αρχιτεκτονική προσανατολισμένη στις υπηρεσίες υποστηρίζει "όλα ως υπηρεσία" (με τα ακρωνύμια EaaS ή XaaS ή απλά aas), οι πάροχοι cloud computing προσφέρουν τις "υπηρεσίες" τους με βάση διαφορετικά μοντέλα, των οποίων τα τρία βασικά μοντέλα ανά NIST είναι υποδομή ως υπηρεσία (IaaS), την πλατφόρμα ως υπηρεσία (PaaS) και το λογισμικό ως υπηρεσία (SaaS). Αυτά τα μοντέλα προσφέρουν αυξανόμενη αφαίρεση. Έτσι, συχνά απεικονίζονται ως στρώματα σε μια στοίβα: υποδομή-, πλατφόρμα- και λογισμικό-ως-υπηρεσία,. Για παράδειγμα, μπορούμε να παρέχουμε SaaS που εφαρμόζονται σε φυσικές μηχανές (γυμνό μέταλλο), χωρίς τη χρήση υποκείμενων στρωμάτων PaaS ή IaaS, και αντίστροφα

μπορεί κανείς να τρέξει ένα πρόγραμμα στο IaaS και να το αποκτήσει απευθείας πρόσβαση χωρίς να το βάλει ως SaaS.

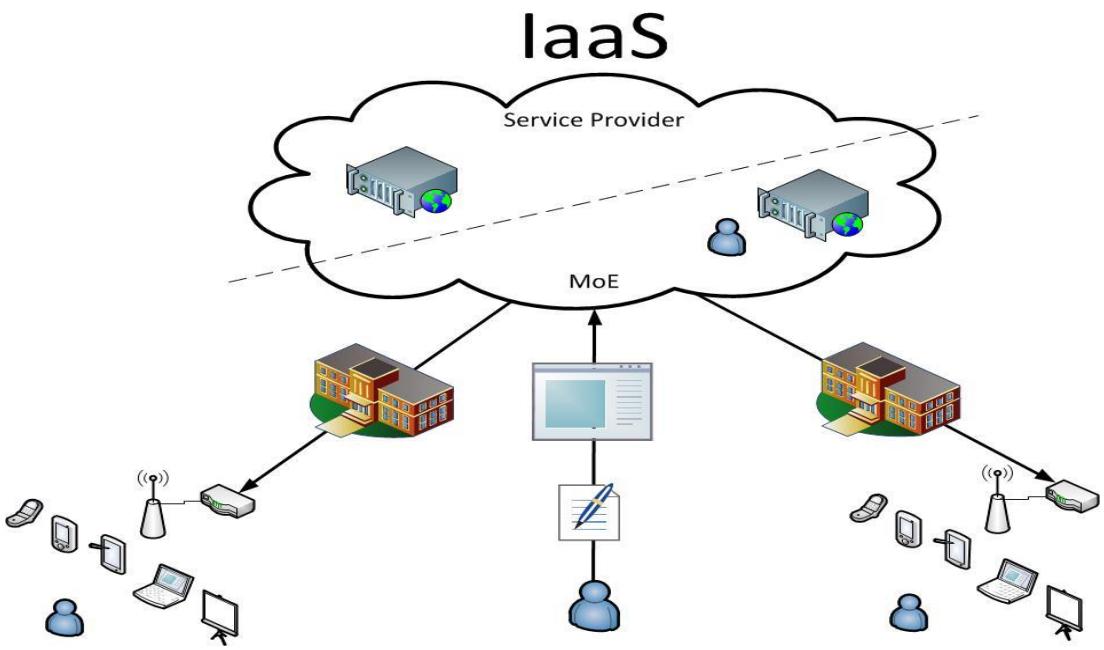
SaaS (λογισμικό ως υπηρεσία)

Αυτός ο τύπος δημόσιου cloud computing παρέχει εφαρμογές μέσω του διαδικτύου μέσω του προγράμματος περιήγησης(π.χ. ηλεκτρονικού ταχυδρομείου μέσω διαδικτύου) είτε μέσω διεπαφής προγράμματος. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή του cloud, συμπεριλαμβανομένων των δικτύων, των διακομιστών, των λειτουργικών συστημάτων, των αποθηκευτικών χώρων ή ακόμη και των μεμονωμένων δυνατοτήτων εφαρμογής, με την πιθανή εξαίρεση περιορισμένων ρυθμίσεων διαμόρφωσης εφαρμογών για συγκεκριμένους χρήστες.Οι πιο δημοφιλείς εφαρμογές SaaS για επιχειρήσεις μπορούν να βρεθούν στο G Suite της Google και στο Office 365 της Microsoft. μεταξύ των εταιρικών εφαρμογών, η Salesforce οδηγεί το πακέτο. Ωστόσο, σχεδόν όλες οι εφαρμογές των επιχειρήσεων, συμπεριλαμβανομένων των προγραμμάτων ERP από την Oracle και τη SAP, υιοθέτησαν το μοντέλο SaaS. Τυπικά, οι εφαρμογές SaaS προσφέρουν εκτεταμένες επιλογές διαμόρφωσης καθώς και περιβάλλοντα ανάπτυξης που επιτρέπουν στους πελάτες να κωδικοποιούν τις δικές τους τροποποιήσεις και προσθήκες.

Εικόνα 2 Software as Service (SasS)

IaaS (υποδομή ως υπηρεσία)

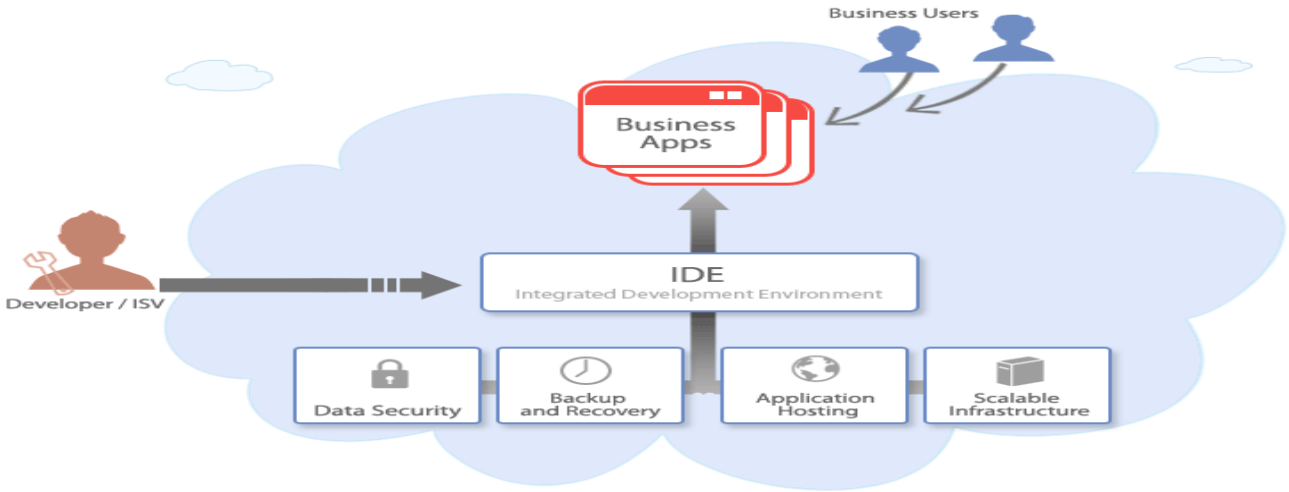
Σε βασικό επίπεδο, οι πάροχοι δημόσιων cloud της IaaS προσφέρουν υπηρεσίες αποθήκευσης και υπολογισμών με βάση την αμοιβή ανά χρήση. Όμως, το πλήρες φάσμα των υπηρεσιών που προσφέρονται από όλους τους σημαντικούς δημόσιους παρόχους cloud είναι εντυπωσιακό: εξαιρετικά κλιμακούμενες βάσεις δεδομένων, εικονικά ιδιωτικά δίκτυα, μεγάλα δεδομένα ανάλυσης, εργαλεία ανάπτυξης, μηχανική μάθηση, παρακολούθηση εφαρμογών κ.ο.κ. Ο ορισμός του cloud computing από τον NIST περιγράφει το IaaS ως "όπου ο καταναλωτής είναι σε θέση να αναπτύξει και να εκτελέσει αυθαίρετο λογισμικό, το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές.Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή cloud αλλά έχει τον έλεγχο των λειτουργικών συστημάτων, και αναπτύσσονται εφαρμογές και ενδεχομένως περιορισμένος έλεγχος επιλεγμένων στοιχείων δικτύου (π.χ. firewalls υποδοχής). Η Amazon Web Services ήταν ο πρώτος πάροχος της IaaS και παραμένει ο ηγέτης, ακολουθούμενη από το Microsoft Azure, το Google Cloud Platform και το IBM Cloud.



Εικόνα 3 IaaS (infrastructure as a service)

PaaS (πλατφόρμα ως υπηρεσία)

Το PaaS παρέχει σύνολα υπηρεσιών και ροές εργασίας που στοχεύουν συγκεκριμένα προγραμματιστές, οι οποίοι μπορούν να χρησιμοποιούν κοινά εργαλεία, διαδικασίες και API για να επιταχύνουν την ανάπτυξη, τη δοκιμή και την ανάπτυξη εφαρμογών. Η δυνατότητα που παρέχεται στον καταναλωτή είναι η ανάπτυξη στην υποδομή του cloud των εφαρμογών που δημιουργούνται από καταναλωτές ή αποκτώνται, οι οποίες δημιουργούνται χρησιμοποιώντας γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες και εργαλεία που υποστηρίζονται από τον πάροχο. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή του cloud, συμπεριλαμβανομένων των δικτύων, των διακομιστών, των λειτουργικών συστημάτων ή του χώρου αποθήκευσης, αλλά έχει τον έλεγχο των αναπτυγμένων εφαρμογών και ενδεχομένως των ρυθμίσεων διαμόρφωσης για το περιβάλλον φιλοξενίας εφαρμογών.. Για τις επιχειρήσεις, η PaaS μπορεί να εξασφαλίσει ότι οι προγραμματιστές έχουν εύκολη πρόσβαση σε πόρους, ακολουθούν ορισμένες διαδικασίες και χρησιμοποιούν μόνο μια συγκεκριμένη σειρά υπηρεσιών, ενώ οι φορείς εκμετάλλευσης διατηρούν την υποκείμενη υποδομή.Επίσης μια ποικιλία PaaS προσαρμοσμένη για προγραμματιστές εφαρμογών για κινητά πηγαίνει γενικά με το όνομα MBaaS (κινητό back end ως υπηρεσία), ή μερικές φορές μόνο BaaS (back end ως υπηρεσία).



Εικόνα 4 Platform as Service (PasS)

Άλλα μοντέλα:

- Storage as a service (SaaS)
- Hardware as Service (HaaS)
- Database as Service (DaaS)

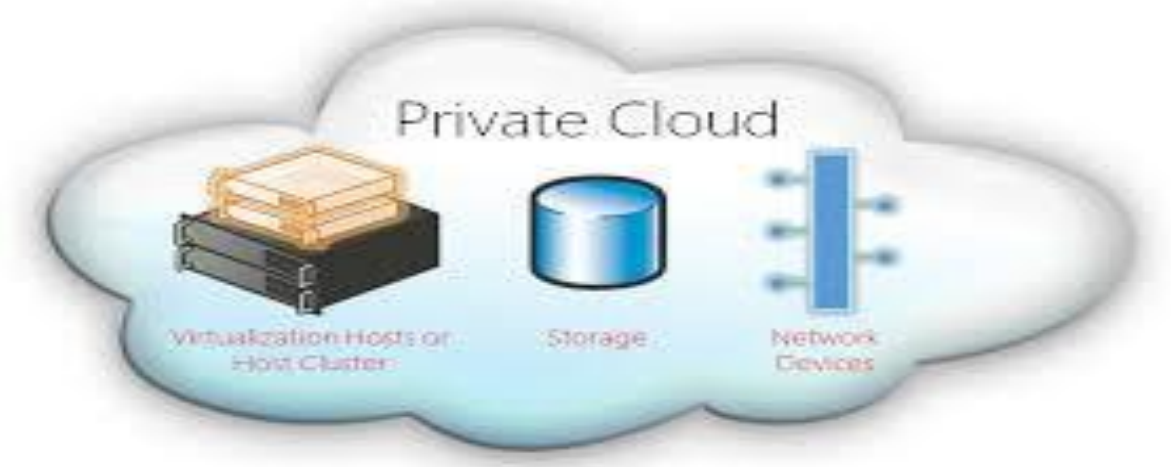
1.2.1 Βασικά είδη εφαρμογών που μας προσφέρει το cloud computing

1. Private cloud

Το ιδιωτικό σύννεφο περιορίζει τις τεχνολογίες που χρησιμοποιούνται για την εκτέλεση δημόσιων σύννεφων του IaaS σε λογισμικό που μπορεί να αναπτυχθεί και να λειτουργήσει στο κέντρο δεδομένων ενός πελάτη. Τα ιδιωτικά σύννεφα μπορούν να επωφεληθούν από την αποτελεσματικότητα του σύννεφου, ενώ παράλληλα παρέχουν τον μεγαλύτερο έλεγχο των πόρων και τη διευκόλυνση της πολλαπλής μίσθωσης.

Βασικές πτυχές του ιδιωτικού νέφους

- Μια διεπαφή αυτοεξυπηρέτησης ελέγχει τις υπηρεσίες, έτσι επιτρέποντας στο προσωπικό της πληροφορικής να παρέχει γρήγορα, να διαθέσει και να παραδίδει πόρους πληροφορικής κατά παραγγελία.
- Υψηλά αυτοματοποιημένη διαχείριση πόρων για τα πάντα, από την ικανότητα υπολογισμών έως την αποθήκευση, την ανάλυση και το μεσαίο λογισμικό.
- Εξειδικευμένη ασφάλεια και διακυβέρνηση σχεδιασμένη για τις συγκεκριμένες απαιτήσεις μιας εταιρείας.



Εικόνα 5 Private cloud

2. Public cloud

Τα δημόσια σύννεφα ανήκουν και λειτουργούν από εταιρείες που προσφέρουν ταχεία πρόσβαση σε ένα δημόσιο δίκτυο σε προσιτούς υπολογιστικούς πόρους. Με τις δημόσιες υπηρεσίες cloud, οι χρήστες δεν χρειάζεται να αγοράζουν υλικό, λογισμικό ή υποστηρικτική υποδομή, η οποία ανήκει και διαχειρίζεται οι πάροχοι.

Βασικές πτυχές του δημόσιου νέφους

- Καινοτόμες επιχειρηματικές εφαρμογές SaaS για εφαρμογές που κυμαίνονται από τη διαχείριση πόρων των πελατών (CRM) έως τη διαχείριση συναλλαγών και την ανάλυση δεδομένων
- Ευέλικτη, κλιμακούμενη υπηρεσία IaaS για αποθήκευση και υπολογιστικές υπηρεσίες με μια προειδοποίηση
- Ισχυρό PaaS για περιβάλλοντα ανάπτυξης και ανάπτυξης εφαρμογών που βασίζονται σε σύννεφο

Εικόνα 6 Public cloud

3. Hybrid cloud

Ένα υβριδικό σύννεφο είναι η ενσωμάτωση ενός ιδιωτικού cloud με ένα δημόσιο σύννεφο. Στα πλέον ανεπτυγμένα, το υβριδικό σύννεφο περιλαμβάνει τη δημιουργία παράλληλων περιβαλλόντων όπου οι εφαρμογές μπορούν εύκολα να κινούνται μεταξύ ιδιωτικών και δημόσιων σύννεφων. Σε άλλες περιπτώσεις, οι βάσεις δεδομένων μπορεί να παραμείνουν στο κέντρο δεδομένων των πελατών και να ενσωματωθούν με δημόσιες εφαρμογές σύννεφοι - ή τα εικονικά φορτία του κέντρου δεδομένων ενδέχεται να αναπαραχθούν στο σύννεφο κατά τη διάρκεια της αιχμής της ζήτησης. Οι τύποι ενσωμάτωσης μεταξύ ιδιωτικού και δημόσιου νέφους ποικίλλουν ευρέως, αλλά πρέπει να είναι εκτεταμένοι για να κερδίσουμε ένα υβριδικό σύννεφο.

Βασικές πτυχές του υβριδικού σύννεφου

- Επιτρέπει στις εταιρείες να διατηρούν τις κρίσιμες εφαρμογές και τα ευαίσθητα δεδομένα σε ένα περιβάλλον παραδοσιακού κέντρου δεδομένων ή σε ένα ιδιωτικό νέφος

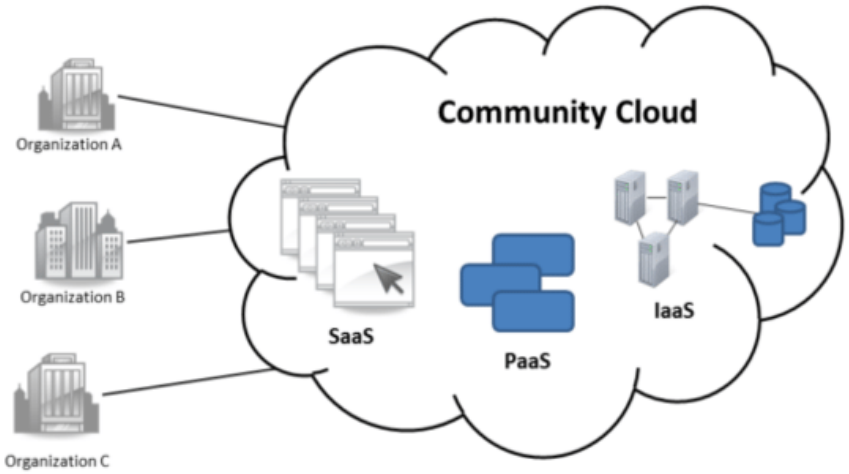
- Επιτρέπει την αξιοποίηση των δημόσιων πόρων cloud όπως το SaaS, για τις πιο πρόσφατες εφαρμογές και του IaaS, για ελαστικούς εικονικούς πόρους
- Διευκολύνει τη φορητότητα δεδομένων, εφαρμογών και υπηρεσιών και περισσότερες επιλογές για μοντέλα ανάπτυξης

Εικόνα 7 Hybrid cloud

1.2.2 Άλλα μοντέλα ανάπτυξης

1 Community cloud

Το κοινοτικό σύννεφο έχει κοινές υποδομές μεταξύ διαφόρων οργανισμών από μια συγκεκριμένη κοινότητα με κοινές ανησυχίες (ασφάλεια, συμμόρφωση, δικαιοδοσία κ.λπ.), είτε διαχειρίζεται εσωτερικά είτε από τρίτο μέρος και είτε φιλοξενείται εσωτερικά είτε εξωτερικά. Το κόστος κατανέμεται σε λιγότερους χρήστες από ένα δημόσιο σύννεφο (αλλά περισσότερο από ένα ιδιωτικό σύννεφο), έτσι μόνο μερικά από τα δυναμικά εξοικονόμησης κόστους του cloud computing πραγματοποιούνται.



Εικόνα 8 Community cloud

2 Distributed cloud

Μια πλατφόρμα υπολογιστικού νέφους μπορεί να συναρμολογηθεί από ένα διανεμημένο σύνολο μηχανών σε διαφορετικές τοποθεσίες, συνδεδεμένο σε ένα μόνο δίκτυο ή υπηρεσία διανομέα. Είναι δυνατόν να γίνει διάκριση μεταξύ δύο τύπων κατανεμημένων σύννεφων: υπολογισμός δημόσιων πόρων και σύννεφο εθελοντών.

- Υπολογισμός δημόσιων πόρων - Αυτός ο τύπος κατανεμημένου σύννεφου προκύπτει από έναν εκτεταμένο ορισμό του cloud computing, επειδή είναι περισσότερο παρόμοιο με το κατανεμημένο υπολογιστικό σύστημα από το cloud computing. Παρόλα αυτά, θεωρείται μια υποκατηγορία του cloud computing και ορισμένα παραδείγματα περιλαμβάνουν κατανεμημένες πλατφόρμες υπολογιστών όπως το BOINC και το Folding @ Home.
- Το cloud-Volunteer cloud computing χαρακτηρίζεται ως η διασταύρωση των υπολογιστών δημόσιων πόρων και του cloud computing, όπου μια υποδομή υπολογιστικού νέφους κατασκευάζεται χρησιμοποιώντας εθελοντικούς πόρους. Πολλές

προκλήσεις προκύπτουν από αυτό το είδος υποδομής, λόγω της μεταβλητότητας των πόρων που χρησιμοποιήθηκαν για την κατασκευή του και του δυναμικού περιβάλλοντος στο οποίο λειτουργεί. Μπορεί επίσης να ονομαστεί σύννεφα ομότιμων ή ad-hoc σύννεφα. Μια ενδιαφέρουσα προσπάθεια προς την κατεύθυνση αυτή είναι το Cloud @ Home, στοχεύει στην υλοποίηση μιας υποδομής υπολογιστικού νέφους χρησιμοποιώντας εθελοντικούς πόρους παρέχοντας ένα επιχειρηματικό μοντέλο για την παροχή κινήτρων για εισφορές μέσω οικονομικής αποκατάστασης.

3 Multicloud

Το Multicloud είναι η χρήση πολλαπλών υπηρεσιών cloud computing σε μια ενιαία ετερογενή αρχιτεκτονική για να μειωθεί η εξάρτηση από μεμονωμένους πωλητές,

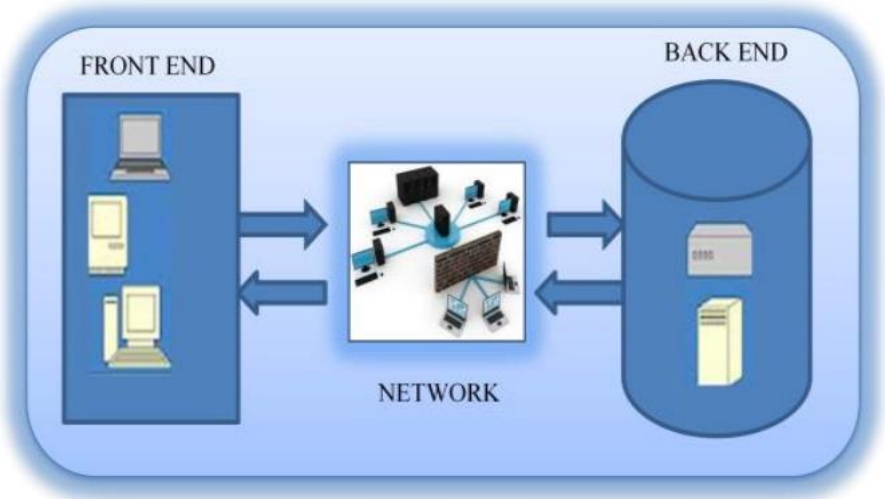
να αυξηθεί η ευελιξία μέσω επιλογών, να μετριαστεί η καταστροφή κ.λπ. Διαφέρει από το υβριδικό σύννεφο στο ότι αναφέρεται σε πολλαπλές υπηρεσίες cloud, τρόπους (δημόσια, ιδιωτική, κληρονομιά).

1.3 Αρχιτεκτονική του cloud computing

Αρχιτεκτονική σύννεφων: η αρχιτεκτονική συστημάτων των συστημάτων λογισμικού που εμπλέκονται στην παράδοση του cloud computing, συνήθως περιλαμβάνει πολλαπλές συνιστώσες σύννεφο που επικοινωνούν μεταξύ τους μέσω ενός χαλαρού μηχανισμού ζεύξης όπως μια ουρά μηνυμάτων. Η ελαστική πρόβλεψη συνεπάγεται ευφυΐα στη χρήση σφιχτής ή χαλαρής σύζευξης όπως εφαρμόζεται σε μηχανισμούς όπως αυτοί και άλλοι.

Τα δύο πιο σημαντικά συστατικά στην αρχιτεκτονική του cloud computing είναι το μπροστά και το πίσω μέρος.

Το μπροστά άκρο είναι το τμήμα που βλέπει ο πελάτης δηλαδή πελάτη-υπολογιστή. Αυτό περιλαμβάνει το πλέγμα του πελάτη και τις υποβολές που χρησιμοποιούνται για την πρόσβαση στο σύννεφο μέσω διεπαφής χρήστη, όπως ενός προγράμματος περιήγησης στο World Wide Web. Το πίσω μέρος της αρχιτεκτονικής του cloud computing είναι το «cloud» το οποίο περιλαμβάνει ποικίλους εξυπηρετητές και γεγονότα υπολογιστών και συσκευές αποθήκευσης ψηφίων.



Εικόνα 9 Αρχιτεκτονική του cloud computing

Τεχνολογία σύννεφων: είναι η εφαρμογή των κλάδων της μηχανικής στο cloud computing. Εισάγει μια συστηματική προσέγγιση στις ανησυχίες υψηλού επιπέδου σχετικά με την εμπορευματοποίηση, την τυποποίηση και τη διακυβέρνηση στη σύλληψη, ανάπτυξη, λειτουργία και συντήρηση των συστημάτων υπολογιστικού νέφους. Πρόκειται για μια διεπιστημονική μέθοδο που περιλαμβάνει συμβολές από διάφορους τομείς, όπως συστήματα, λογισμικό, ιστό, απόδοση, πληροφορίες, ασφάλεια, πλατφόρμα, κίνδυνος και ποιοτική μηχανική.

1.3.1 Μέθοδοι και συστήματα για την παροχή αρχιτεκτονικών ανάπτυξης σε περιβάλλοντα υπολογιστικού νέφους

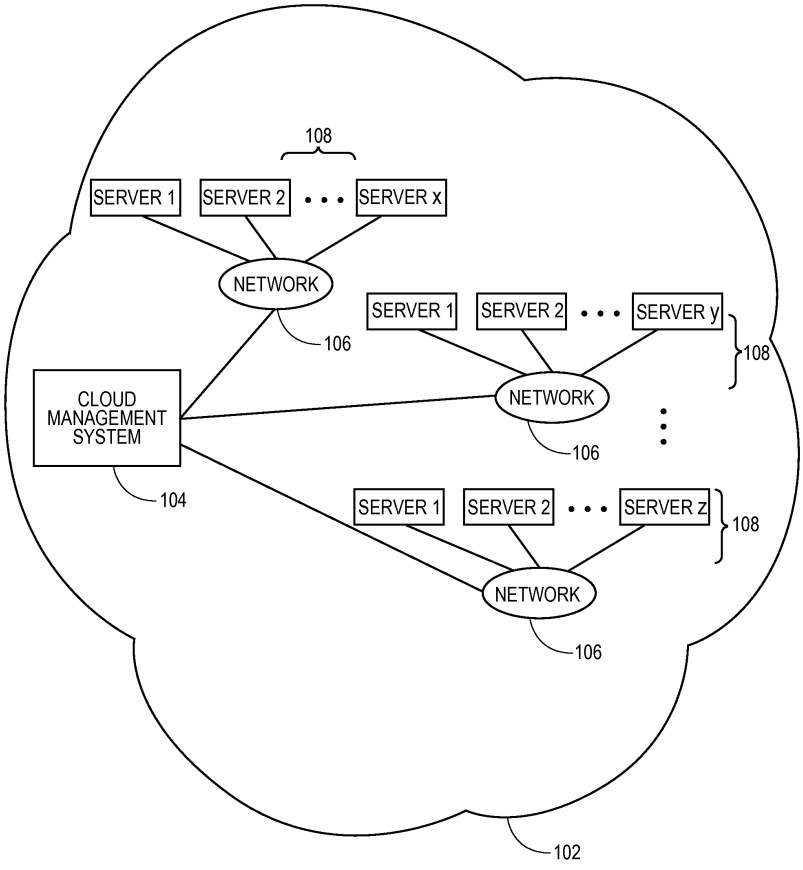
Το σύστημα απόφασης μπορεί να προσδιορίσει μία ή περισσότερες παραμέτρους για την ανάλυση εφαρμογών και διαδικασιών που εκτελούνται σε ένα σύννεφο, να παρακολουθεί τις εφαρμογές και τις διεργασίες που εκτελούνται στο σύννεφο και να συλλέγει πληροφορίες όπως η χρήση των πόρων του cloud, ο αριθμός και ο τύπος των υπολογιστικών διαδικασιών από τις υπολογιστικές διαδικασίες. Το σύστημα απόφασης μπορεί στη συνέχεια να παράγει προσαρμοσμένες αρχιτεκτονικές ανάπτυξης με βάση τις πληροφορίες που συλλέγονται.

Οι διαδικασίες cloud λειτουργούν σωστά ή και αποτελεσματικά με το ότι το cloud παρέχει επαρκείς πόρους στις διαδικασίες cloud κλπ. τις απαιτήσεις του χρήστη και τη χρήση του cloud, ο χρήστης μπορεί να έχει πολλές εφαρμογές ή / και διεργασίες, να εμφανίζονται σε ένα σύννεφο και μπορεί να χρησιμοποιεί πολλαπλά ανεξάρτητα σύννεφα για να υποστηρίζει τις διαδικασίες του cloud. Ως εκ τούτου, ο χρήστης ενδέχεται να δυσκολεύεται να προσδιορίσει μια βέλτιστη αρχιτεκτονική ανάπτυξης στο cloud, καθώς οι εφαρμογές και / ή οι διαδικασίες εκδηλώνονται ή τερματίζονται με την πάροδο του χρόνου. Επιπλέον, ο χρήστης ενδέχεται να έχει δυσκολία στην παρακολούθηση των εφαρμογών ή / και των διαδικασιών που χρησιμοποιούνται από τις διαδικασίες cloud. Για παράδειγμα, καθώς οι εφαρμογές και / ή οι διεργασίες εκτελούνται στα cloud, οι διαδικασίες cloud μπορούν να δημιουργήσουν νέες διαδικασίες cloud. Ως εκ τούτου, η αρχική αρχιτεκτονική ανάπτυξης που

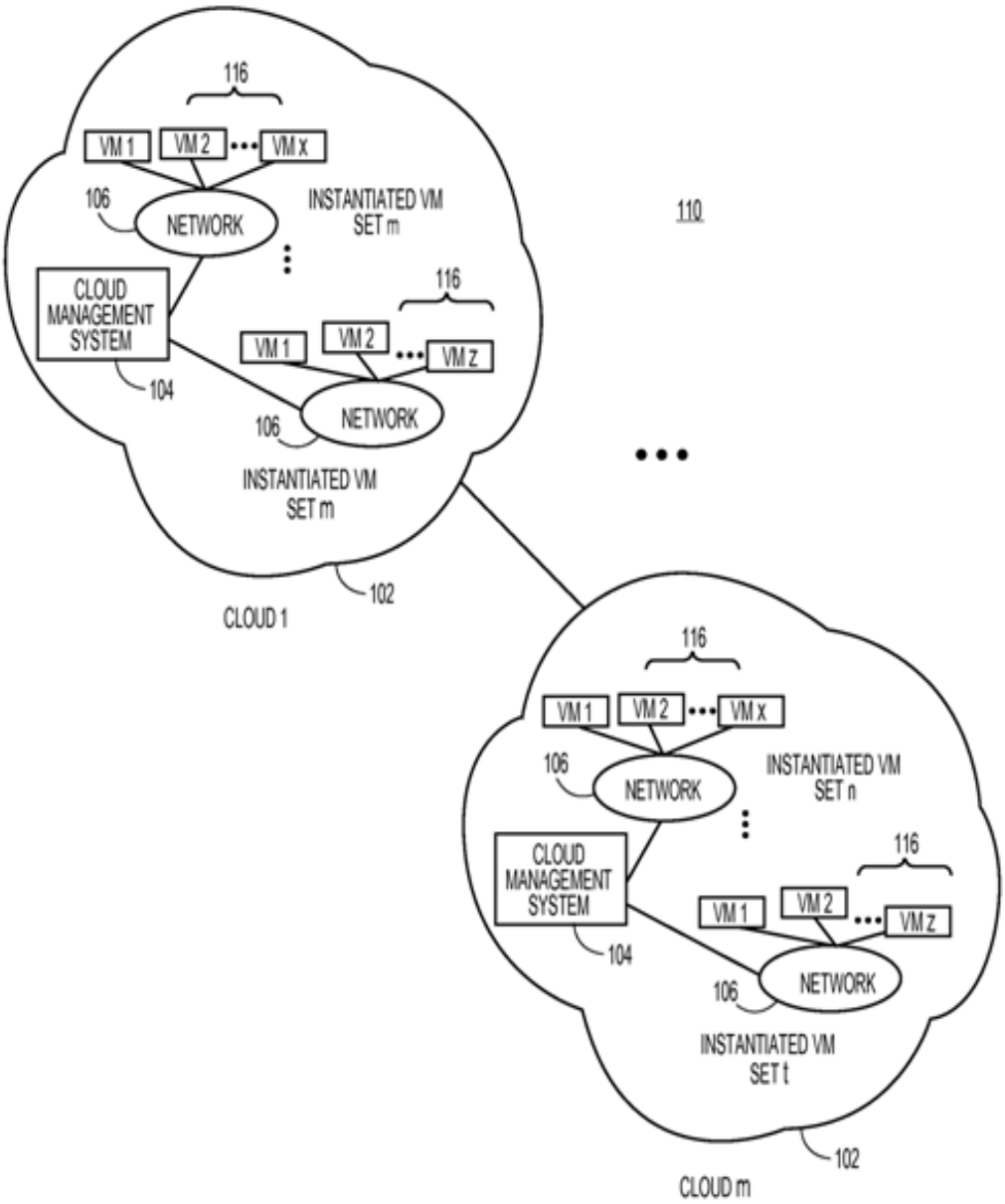
φιλοξενεί τις εφαρμογές ή / και τις διεργασίες του χρήστη ενδέχεται να μην είναι πλέον βέλτιστη ή ακόμη και ικανή να υποστηρίξει τις εφαρμογές ή / και τις διεργασίες του χρήστη.

Περιγραφή εικόνων με βάση τα παραπάνω

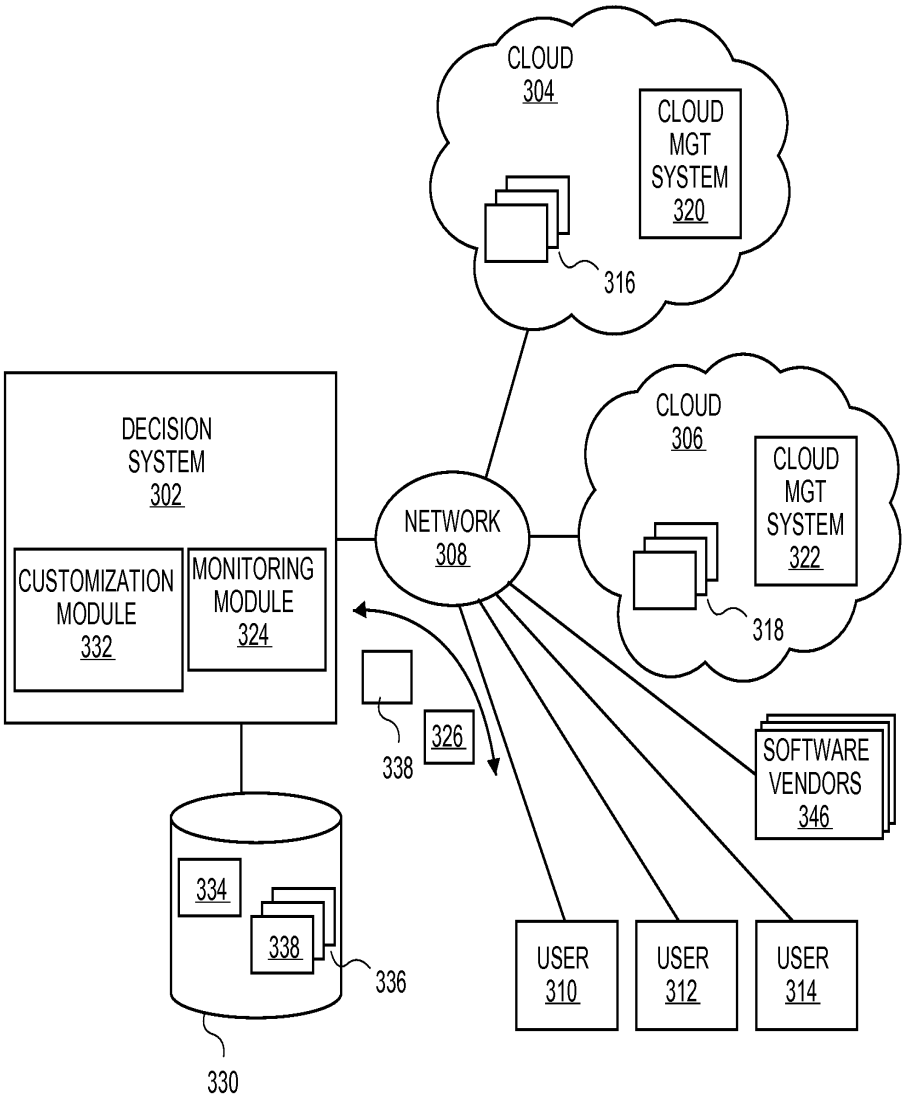
Διάφορα χαρακτηριστικά μπορούν να εκτιμηθούν, καθώς αυτά κατανοούνται καλύτερα με μια αναφορά στην ακόλουθη λεπτομερή περιγραφή των υλοποιήσεων όταν εξετάζονται σε σχέση με τις συνοδευόμενες εικόνες, στις οποίες:



Εικόνα 10 απεικονίζει μια γενική αρχιτεκτονική του συστήματος cloud, στην οποία μπορούν να ασκηθούν διάφορες ενσωματώσεις της παρούσας διδασκαλίας.



Εικόνα 11απεικονίζει μια γενική αρχιτεκτονική συστήματος cloud στην οποία μπορούν να εφαρμοστούν διάφορες ενσωματώσεις σε μια άλλη άποψη που περιλαμβάνει πολλές διατάξεις νέφους.



Εικόνα 12 απεικονίζει ένα γενικό σύστημα στο οποίο ένα σύστημα απόφασης μπορεί να αναλύει δεδομένα που σχετίζονται με εφαρμογές ή / και διεργασίες που εκτελούνται σε ένα περιβάλλον υπολογιστικού cloud και παρέχει προσαρμοσμένες αρχιτεκτονικές ανάπτυξης.

```
<!ELEMENT deployment_analysis (analysis_parameters+)>
<!ATTLIST deployment_analysis
application_ID NMTOKEN #REQUIRED
start_date CDATA #REQUIRED
start_time NMTOKEN #REQUIRED
requester_ID “foobar”>

<!ELEMENT analysis_parameters (deployment_architecture, analysis_duration,
number_of_durations, processor_utilization+, network_traffic_level*,
storage_utilization*, software_license_info*)>

<!ELEMENT deployment_architecture (number_of_machines+, type_of_architecture+)>
<!ELEMENT number_of_machines (#PCDATA)>
<!ELEMENT type_of_architecture (physical | virtual | private_cloud | public_cloud)>

<!ELEMENT analysis_total_duration (#PCDATA)>
<!ATTLIST analysis_total_duration unit (second | minute | hour | day) “hour”>

<!ELEMENT number_of_durations (#PCDATA)>

<!ELEMENT processor_utilization (duration_identifier+, utilization_level+)>
<!ELEMENT duration_identifier (#PCDATA)>
<!ELEMENT utilization_level (#PCDATA)>

<!ELEMENT network_traffic_level (duration_identifier+, traffic_level+)>
<!ATTLIST network_traffic_level unit (Mbit/s | Gbit/s | MB/s | GB/s) “Mbit/s”>
<!ELEMENT duration_identifier (#PCDATA)>
<!ELEMENT traffic_level (#PCDATA)>

<!ELEMENT storage_utilization (duration_identifier+, storage_level+)>
<!ATTLIST storage_utilization
unit (KB | MB | GB) “MB”
storage_type (volatile | cache | persistent) #REQUIRED>
<!ELEMENT duration_identifier (#PCDATA)>
<!ELEMENT storage_level (#PCDATA)>

<!ELEMENT software_license_info (number_of_licenses+, license_identifier?)>
<!ELEMENT number_of_licenses (#PCDATA)>
<!ELEMENT license_identifier (#PCDATA)>
```

Εικόνα 13 απεικονίζει έναν υποδειγματικό ορισμό δεδομένων.

```
<?xml version=”1.0” ?>
<!DOCTYPE deployment_analysis SYSTEM “deployment_analysis.dtd”>
<deployment_analysis application_ID=”APPLICATION A” start_date=”02/24/2010”
start_time=1200>
        <analysis_parameters>
                <deployment_architecture>
                        <number_of_machines>20</number_of_machines>
                        <type_of_architecture>private_cloud</type_of_architecture>
                </deployment_architecture>
                <analysis_total_duration>24</analysis_total_duration>
                <number_of_durations>24</number_of_durations>
                <processor_utilization>
                        <duration_identifier>1</duration_identifier>
                        <utilization_level>8%</utilization_level>
                </processor_utilization>
                <network_traffic_level unit=Mbit/s>
                        <duration_identifier>1</duration_identifier>
                        <traffic_level>753</traffic_level>
                </network_utilization>
                <processor_utilization>
                        <duration_identifier>2</duration_identifier>
                        <utilization_level>6%</utilization_level>
                </processor_utilization>
                <network_traffic_level unit=Mbit/s>
                        <duration_identifier>2</duration_identifier>
                        <traffic_level>878</traffic_level>
                </network_utilization>
                …
                <processor_utilization>
                        <duration_identifier>24</duration_identifier>
                        <utilization_level>9%</utilization_level>
                </processor_utilization>
                <network_traffic_level unit=Mbit/s>
                        <duration_identifier>24</duration_identifier>
                        <traffic_level>488</traffic_level>
                </network_utilization>
        </analysis_parameters>
</deployment_analysis>
```

Εικόνα 14 απεικονίζει ένα υποδειγματικό σύνολο δεδομένων που παράγεται από το σύστημα απόφασης σύμφωνα με τον ορισμό των δεδομένων.

DEPLOYMENT ARCHITECTURE ANALYSIS AND RECOMMENDATION			
APPLICATION ID: APPLICATION A	START DATE: 02/24/2010	START TIME: 12:00	REQUESTER: foobar

DEPLOYMENT PARAMETERS

NUMBER OF MACHINES:	20
TYPE:	PRIVATE CLOUD
TOTAL DURATION:	24 hr
PERIODS OF DURATION:	24 (EACH DURATION = 1 hr)

OBSERVED RESOURCE UTILIZATION

DURATION PERIOD #	PROCESSOR UTILIZATION	NETWORK TRAFFIC LEVEL
1	8%	753 Mbit/s
2	6%	878 Mbit/s
...	...	...
24	9%	488 Mbit/s

AVERAGE RESOURCE UTILIZATION:

PROCESSOR UTILIZATION:	7%
NETWORK TRAFFIC LEVEL:	790Mbit/s

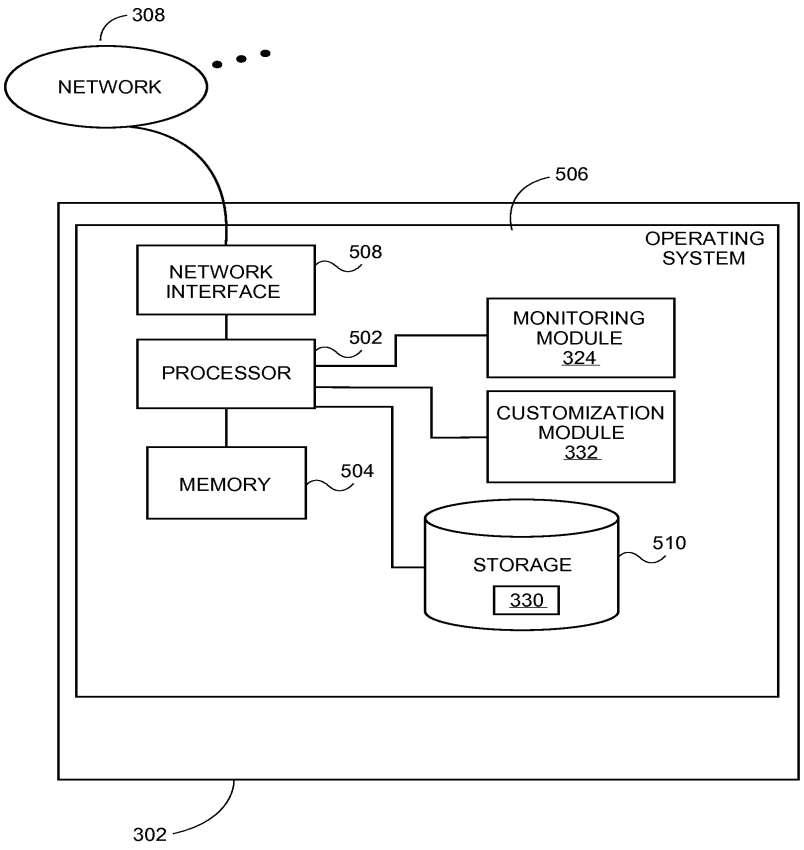
RECOMMENDED DEPLOYMENT ARCHITECTURE

IT IS RECOMMENDED THAT APPLICATION A BE RUN ON VIRTUAL MACHINES INSTANTIATED IN A PUBLIC COMPUTING CLOUD BECAUSE APPLICATION A, OVER A PERIOD OF 24 HOURS:

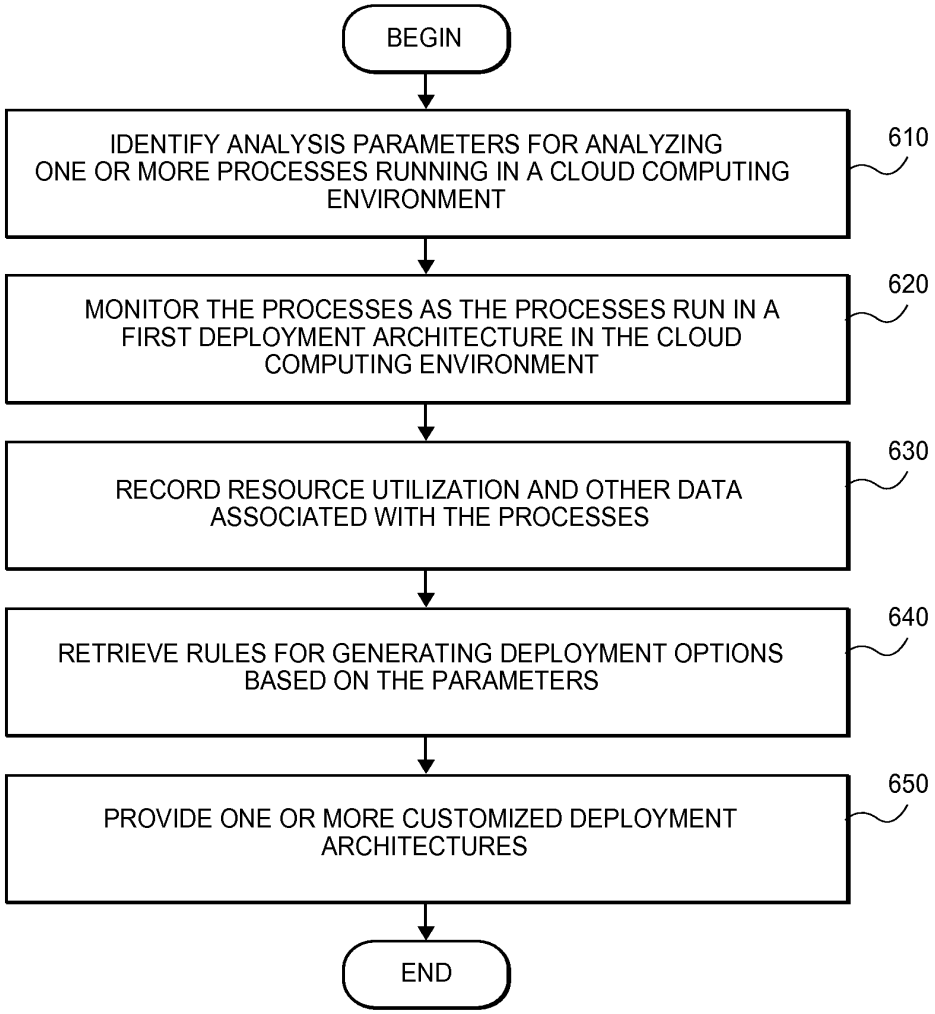
(1) CONSUMED ON THE AVERAGE LESS THAN 10% OF PROCESSOR POWER; AND

(2) UTILIZED ON THE AVERAGE GREATER THAN 512 Mbit/s OF NETWORK BANDWIDTH.

Εικόνα 15 απεικονίζει μια παραδειγματική αναφορά που παράγεται από το σύστημα απόφασης.



Εικόνα 16 απεικονίζει μια παραδειγματική διαμόρφωση υλικού για ένα σύστημα απόφασης.



Εικόνα 17 απεικονίζει ένα διάγραμμα ροής μιας παραδειγματικής διαδικασίας για την παρακολούθηση εφαρμογών ή / και διεργασιών που εκτελούνται σε ένα περιβάλλον υπολογιστικού νέφους και δημιουργεί μία ή περισσότερες προσαρμοσμένες αρχιτεκτονικές ανάπτυξης.

1.4 Πως δουλεύει το cloud computing

Το σύννεφο περιλαμβάνει επίπεδα κυρίως ως προς τα back-end επίπεδα και τα επίπεδα front-end ή client-end. Τα επίπεδα front-end είναι αυτά που βλέπουμε και αλληλεπιδρούν όταν έχουμε πρόσβαση σε μήνυμα μας στο Internet , για παράδειγμα στο Gmail. Χρησιμοποιούμε προγράμματα που εκτελούνται στο μπροστινό μέρος ενός σύννεφου.Το ίδιο ισχύει και όταν αποκτάμε πρόσβαση στο λογαριασμό μας στο facebook. Το back-end περιλαμβάνει την αρχιτεκτονική υλικού και λογισμικού που τροφοδοτεί τη διεπαφή που βλέπουμε στο μπροστινό μέρος. Επειδή οι υπολογιστές έχουν ρυθμιστεί να λειτουργούν ταυτόχρονα,οι εφαρμογές μπορούν να επωφεληθούν από όλη αυτή την υπολογιστική ισχύ σαν να τρέχουν σε μια συγκεκριμένη συσκευή.

Το Cloud computing επιτρέπει επίσης πολύ ευελιξία, υπολογίζοντας τη ζήτηση, μπορούμε να αυξήσουμε πόσα από τα στοιχεία του cloud χρησιμοποιούμε χωρίς να χρειάζεται να αντιστοιχίσουμε συγκεκριμένο υλικό για την εργασία ή απλά να μειώσουμε την αποζημίωση των παραχωριθέντων στοιχείων που μας έχουν δοθεί όταν δεν είναι απαραίτητα . Η χρήση του cloud computing Subashini και της Kavitha υποστηρίζουν τις υπηρεσίες για πολλούς λόγους που περιβάλλουν επειδή η υπηρεσία αυτή παρέχει γρήγορη πρόσβαση στις εφαρμογές και μειώνει τις χρεώσεις υπηρεσιών. Οι παροχείς υπολογιστών Cloud θα πρέπει να αντιμετωπίζουν την ιδιωτικότητα και την ασφάλεια ως ζήτημα για μεγαλύτερες και επείγουσες βασικές ανησυχίες. Η εξέταση με τους παρόχους "ενιαίου cloud" εξελίσσεται λιγότερο δημοφιλής υπηρεσία με τους πελάτες λόγω υποσχέσεις δυσκολίες, όπως η αποτυχία προσβασιμότητας υπηρεσιών για κάποιο χρονικό διάστημα και οι κακόβουλες επιθέσεις του εσωτερικού στο ενιαίο σύννεφο. Τώρα, το ενιαίο σύννεφο κινείται προς τα πολλαπλά σύννεφα, τα "σύννεφα" ή "σύννεφο σύννεφων".

1.5 Συστήματα και μέθοδοι για την ανάπτυξη δεδομένων cloud με βάση προτιμώμενες και / ή υπάρχουσες σχέσεις συνδρομής

Οι υλοποιήσεις αφορούν συστήματα και μεθόδους μεταφοράς δεδομένων σε δίκτυο cloud. Σε ορισμένες πτυχές, ένας διαχειριστής ενός ωφέλιμου φορτίου δεδομένων μπορεί να επιθυμεί να μεταφέρει το ωφέλιμο φορτίο δεδομένων από μια υπηρεσία διανομής δεδομένων σε ένα υποψήφιο προμηθευτή cloud για να αξιοποιήσει το κόστος, την ασφάλεια, την ενοποίηση ή άλλα πλεονεκτήματα. Η υπηρεσία διανομής δεδομένων μπορεί να εντοπίσει τους υποψήφιους παρόχους cloud που είναι σε θέση να φιλοξενήσουν το φορτίο δεδομένων. Επιπλέον, η υπηρεσία διανομής δεδομένων μπορεί να εξετάσει τυχόν σχέσεις μεταξύ του διαχειριστή και των υποψήφιων παρόχων cloud και με βάση τις σχέσεις, μπορεί να παρουσιάσει στον διαχειριστή αντίστοιχες προσφορές από τους υποψήφιους παρόχους cloud για να φιλοξενήσει το φορτίο δεδομένων. Ο διαχειριστής μπορεί να ελέγξει τις προσφορές, να κάνει μια επιλογή και το φορτίο δεδομένων μπορεί να μεταφερθεί στον επιλεγμένο πάροχο cloud για φιλοξενία.

Περιγραφή

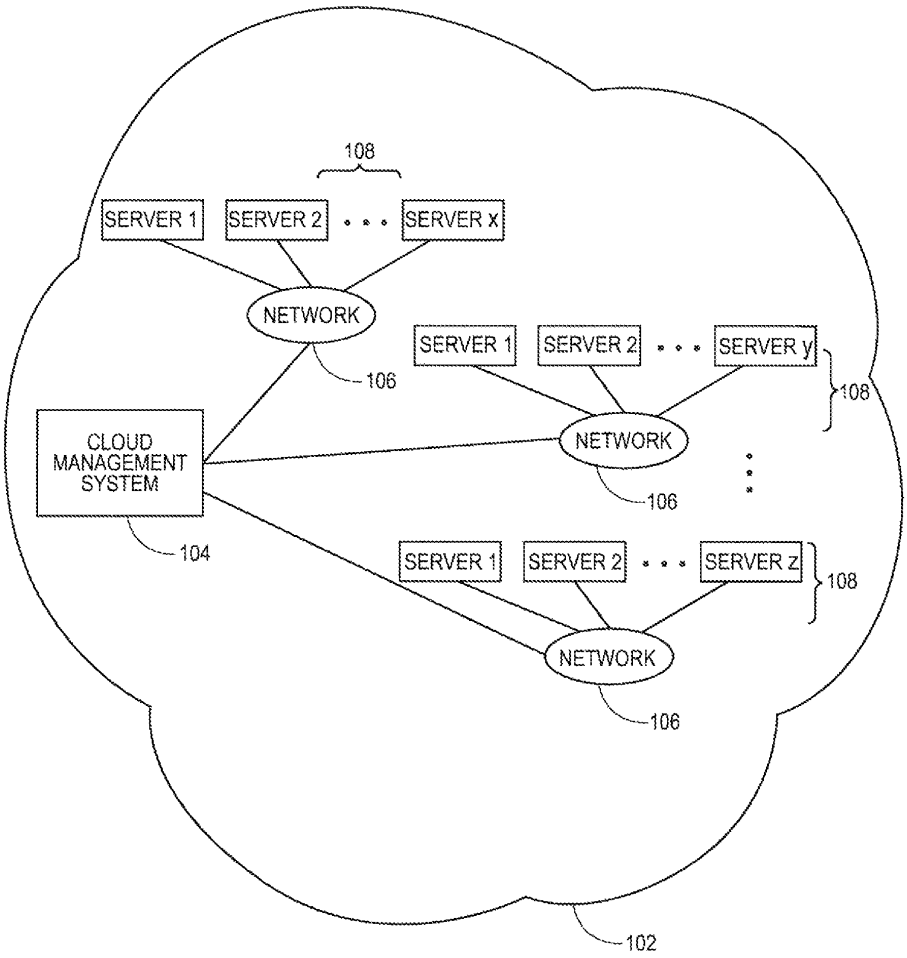
Η εμφάνιση των αρχιτεκτονικών υπολογιστών βασισμένων σε νέφος άνοιξε νέες δυνατότητες για την ταχεία και επεκτάσιμη ανάπτυξη των εικονικών καταστημάτων, των μέσων ενημέρωσης, των ιστότοπων κοινωνικής δικτύωσης και πολλών άλλων δικτυακών τόπων ή υπηρεσιών on-line. Σε γενικές γραμμές, μια αρχιτεκτονική που βασίζεται σε cloud αναπτύσσει ένα σύνολο φιλοξενημένων πόρων, όπως επεξεργαστές, λειτουργικά συστήματα, λογισμικό και άλλα στοιχεία που μπορούν να συνδυαστούν για να δημιουργήσουν εικονικές μηχανές. Ένας χρήστης ή πελάτης μπορεί να ζητήσει την παράσταση μιας εικονικής μηχανής ή ενός συνόλου μηχανών από αυτούς τους πόρους από ένα κεντρικό διακομιστή ή ένα σύστημα διαχείρισης cloud για να εκτελέσει επιδιωκόμενες εργασίες, υπηρεσίες ή εφαρμογές. Για παράδειγμα, ένας χρήστης μπορεί να επιθυμεί να δημιουργήσει ένα παράδειγμα ενός εικονικού διακομιστή από το cloud ώστε να δημιουργήσει ένα κατάστημα για

την εμπορία προϊόντων ή υπηρεσιών σε προσωρινή βάση, για παράδειγμα, να πουλήσει εισιτήρια ή εμπόρευμα για μια αθλητική ή μουσική παράσταση. Ο χρήστης μπορεί να εγγραφεί στο σύνολο των πόρων που απαιτούνται για τη δημιουργία και τη λειτουργία του συνόλου των εικονικών μηχανών σε κατάσταση επίτευξης μιας διάρκειας, όπως ώρες ή ημέρες, για την προβλεπόμενη εφαρμογή τους.

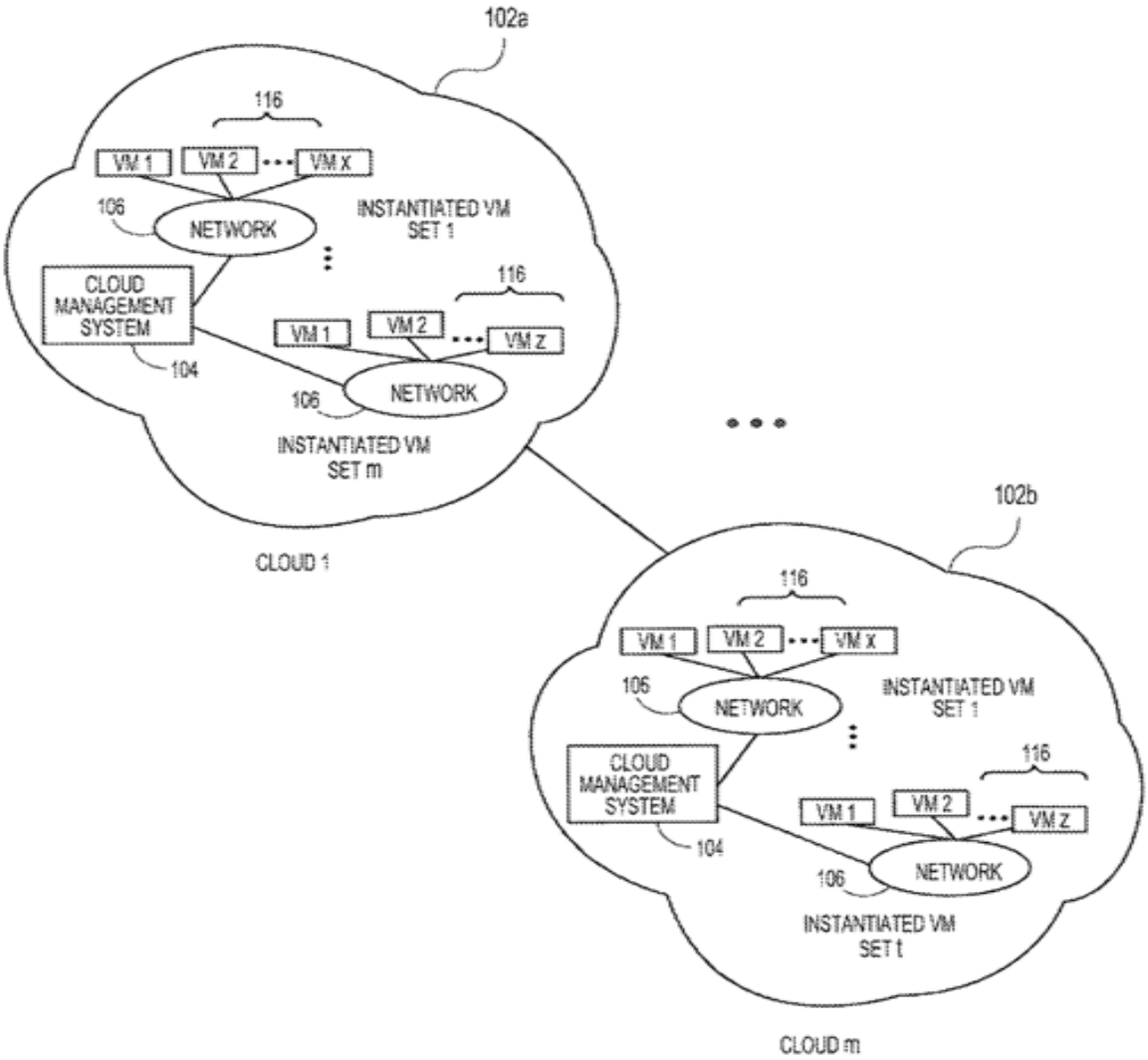
Τα υπάρχοντα συστήματα μπορούν να περιλαμβάνουν μια υπηρεσία διανομής δεδομένων ρυθμισμένη να φιλοξενεί ένα σύνολο δεδομένων πριν από τη μεταφορά του συνόλου δεδομένων στο χώρο αποθήκευσης που βασίζεται σε σύννεφο. Για διάφορους λόγους, ένας διαχειριστής ή άλλος χρήστης μπορεί να θελήσει να εξετάσει τη μεταφορά ή τη μετεγκατάσταση του συνόλου δεδομένων που διαμένουν στην υπηρεσία διανομής δεδομένων στον αποθηκευτικό χώρο του cloud. Για παράδειγμα, ο διαχειριστής ενδέχεται να έχει μεταναστεύσει το σύνολο δεδομένων από ένα δίκτυο επί τόπου στην υπηρεσία διανομής και να μεταφερθεί στον αποθηκευτικό χώρο του cloud. Επιπλέον, ο διαχειριστής μπορεί να έχει μια υπάρχουσα σχέση με διάφορους παρόχους αποθήκευσης cloud που θα μπορούσαν να καταστήσουν δυνατή τη μεταφορά του συνόλου δεδομένων. Αντί να ρυθμίσει με μη αυτόματο τρόπο τη μεταφορά του συνόλου δεδομένων, ο διαχειριστής μπορεί να επιθυμεί να παρουσιάσει ένα σύνολο επιλογών για τη μεταφορά του συνόλου δεδομένων σε έναν ή περισσότερους παρόχους cloud. Επιπλέον, ο διαχειριστής μπορεί να θέλει να χρησιμοποιήσει υπάρχουσες εγγραφές με τους παρόχους cloud για να αξιοποιήσει τους όρους και τις προσφορές φιλοξενίας δεδομένων.

Ως εκ τούτου, μπορεί να είναι επιθυμητό να παρέχονται συστήματα και μέθοδοι για την ανάπτυξη ενός συνόλου δεδομένων σε ένα δίκτυο που βασίζεται σε cloud με βάση υπάρχουσες σχέσεις. Συγκεκριμένα, μπορεί να είναι επιθυμητό να παρέχονται συστήματα και μέθοδοι για την παρουσίαση ενός διαχειριστή με επιλογές cloud hosting που βασίζονται σε σχέσεις μεταξύ του διαχειριστή και των δικτύων.

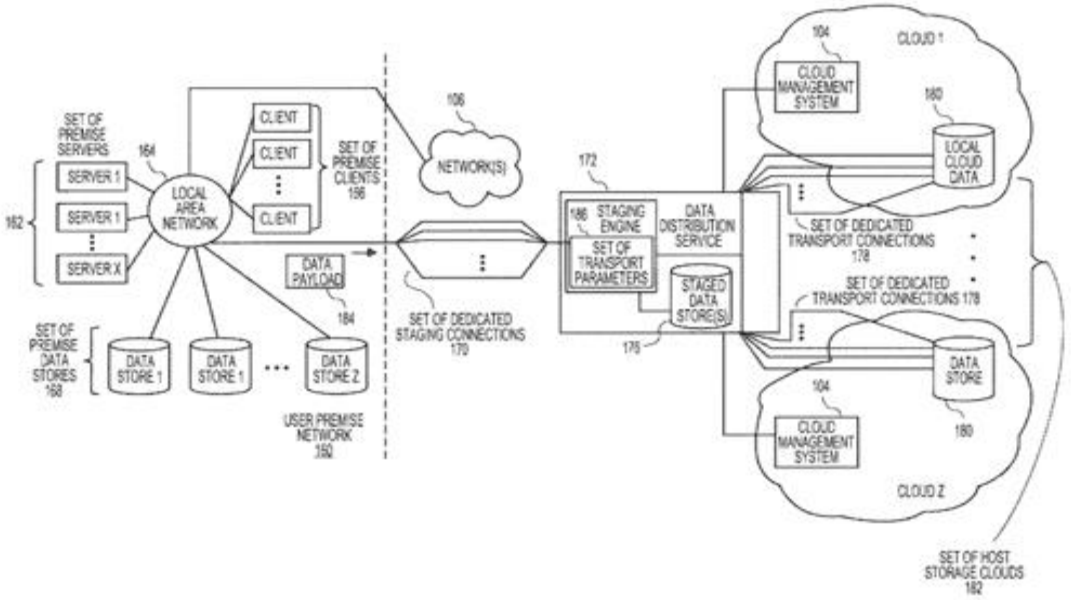
Περιγραφή εικόνων με βάση τα παραπάνω



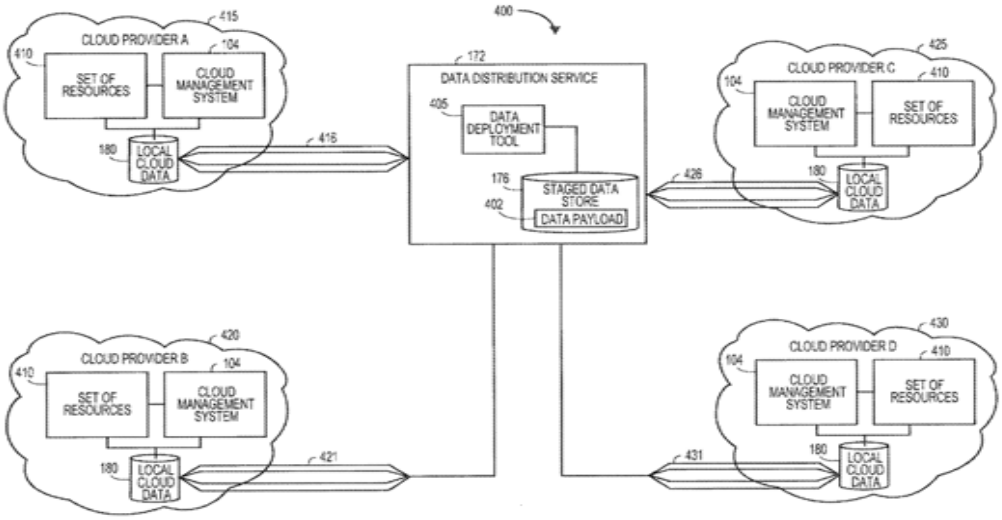
Εικόνα 18 απεικονίζει μια γενική αρχιτεκτονική συστήματος cloud, στην οποία μπορούν να ασκηθούν διάφορες πτυχές συστημάτων και μεθόδων για τη μεταφορά δεδομένων με βάση τις υπάρχουσες σχέσεις.



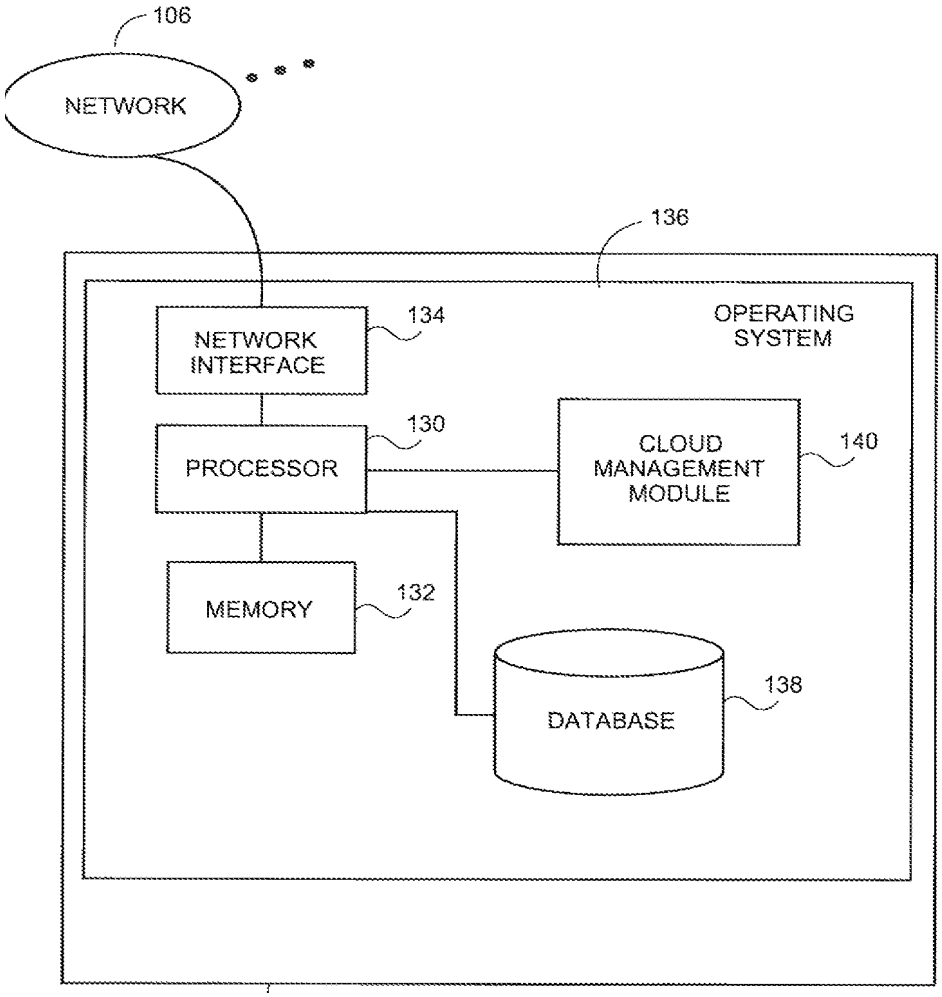
Εικόνα 19 απεικονίζει μια γενική αρχιτεκτονική του συστήματος cloud, στην οποία μπορούν να εφαρμοστούν διάφορες πτυχές των συστημάτων και των μεθόδων μεταφοράς δεδομένων με βάση τις υφιστάμενες σχέσεις.



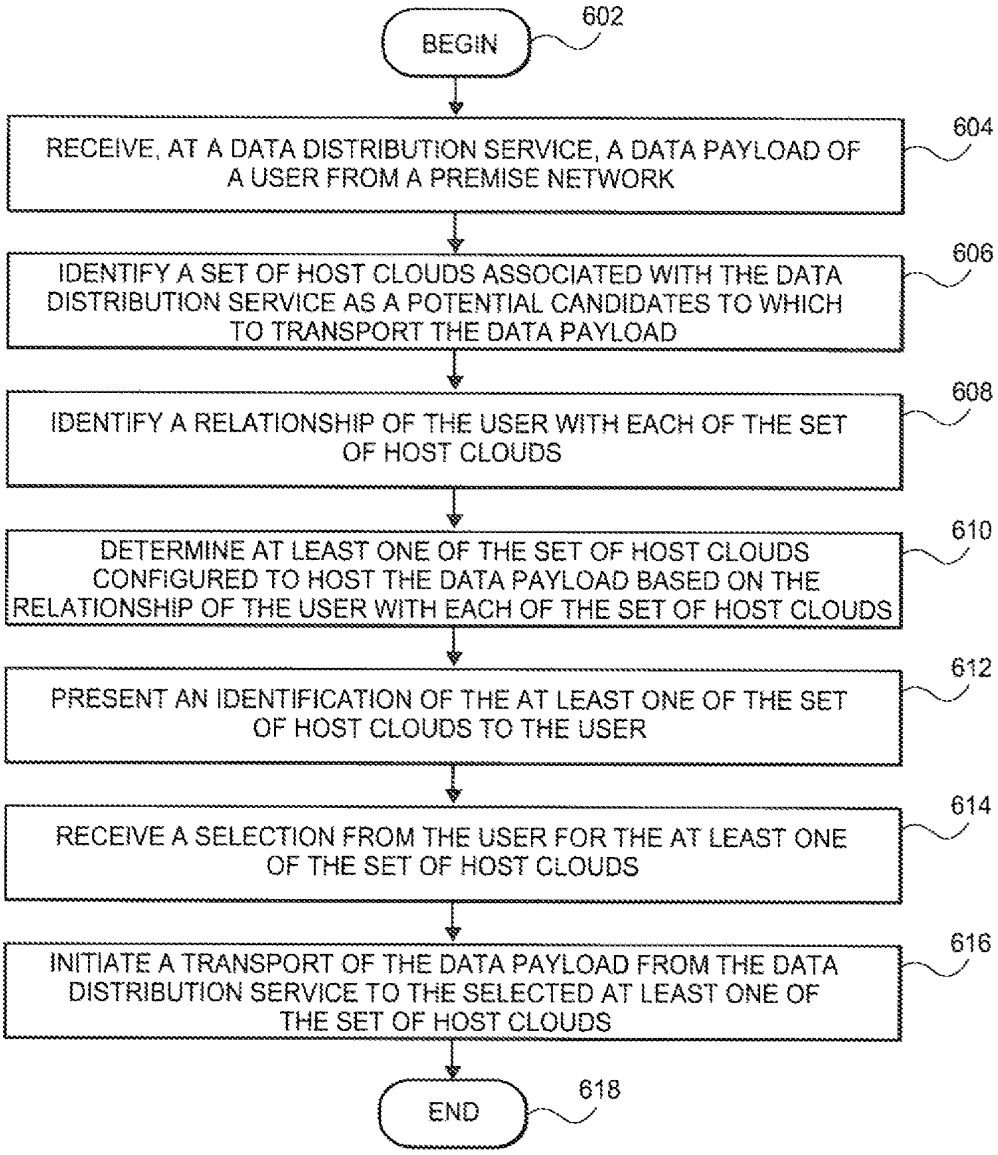
Εικόνα 20 απεικονίζει μια διαμόρφωση δικτύου στην οποία μπορεί να δημιουργηθεί μια υπηρεσία διανομής δεδομένων μεταξύ ενός δικτύου προκατασκευών και ενός νέφους αποθήκευσης υποδοχής.



Εικόνα 21 απεικονίζει μια διαμόρφωση δικτύου στην οποία μπορούν να ασκηθούν διάφορες πτυχές συστημάτων και μεθόδων για τη μεταφορά.



Εικόνα 22 απεικονίζει μια παραδειγματική διαμόρφωση υλικού για ένα σύστημα διαχείρισης cloud το οποίο μπορεί να υποστηρίζει και να διατηρεί ένα ή περισσότερα δίκτυα που βασίζονται σε cloud.



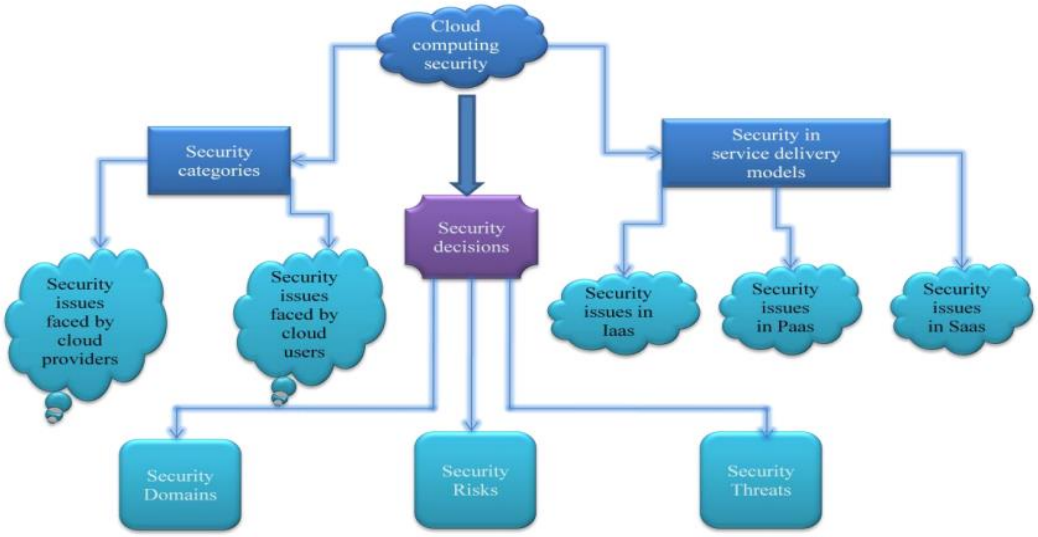
Εικόνα 23 απεικονίζει ένα διάγραμμα ροής για τη διαμόρφωση μιας μεταφοράς δεδομένων σε ένα δίκτυο που βασίζεται σε cloud.

2ο Κεφάλαιο: Ασφάλεια στο cloud computing

Με την υιοθέτηση των δημόσιων cloud υπηρεσιών, μεγάλο μέρος του δικτύου μας, τα συστήματα, εφαρμογές και δεδομένα θα βρίσκονται υπό τον έλεγχο του παρόχου. Η παράδοση των cloud μοντέλων υπηρεσιών θα δημιουργήσει clouds εικονικών περιμέτρων καθώς και ένα πρότυπο ασφαλείας με τις αρμοδιότητες να μοιράζονται μεταξύ πελάτη-παρόχου των cloud υπηρεσιών (CSP). Πολλοί πάροχοι νέφους μπορούν να μοιράζονται πληροφορίες με τρίτους εάν είναι απαραίτητο για λόγους νόμου και τάξης, ακόμη και χωρίς ένταλμα. Αυτό επιτρέπεται στις πολιτικές απορρήτου τους, τις οποίες πρέπει να συμφωνούν οι χρήστες πριν αρχίσουν να χρησιμοποιούν υπηρεσίες cloud. Οι λύσεις για την προστασία της ιδιωτικής ζωής περιλαμβάνουν την πολιτική και τη νομοθεσία, καθώς και τις επιλογές των τελικών χρηστών για τον τρόπο αποθήκευσης των δεδομένων. Οι χρήστες μπορούν να κρυπτογραφήσουν δεδομένα που επεξεργάζονται ή αποθηκεύονται στο σύννεφο, για να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Σύμφωνα με τη Cloud Security Alliance, οι τρεις πρώτες απειλές στο σύννεφο είναι Ασφαλείς διεπαφές και API, απώλεια δεδομένων και διαρροή και αποτυχία υλικού, που αντιστοιχούσαν σε 29%, 25% και 10% όλων των διακοπών ασφαλείας cloud αντίστοιχα. Μαζί, αυτά αποτελούν κοινές ευπάθειες τεχνολογίας. Σε μια πλατφόρμα παροχής cloud που μοιράζονται διάφοροι χρήστες, ενδέχεται να υπάρχει πιθανότητα οι πληροφορίες που ανήκουν σε διαφορετικούς πελάτες να βρίσκονται στον ίδιο διακομιστή δεδομένων. Επιπλέον οι χάκερ ξοδεύουν σημαντικό χρόνο και προσπάθεια αναζητώντας τρόπους να διεισδύσουν στο σύννεφο κάνοντας μεγάλες τρύπες στην υποδομή σύννεφων για να εισέλθουν στα δεδομένα. Επειδή τα δεδομένα από εκατοντάδες ή χιλιάδες επιχειρήσεις μπορούν να αποθηκευτούν σε μεγάλους διακομιστές σύννεφων, οι χάκερ μπορούν θεωρητικά να αποκτήσουν τον έλεγχο

των τεράστιων καταστημάτων πληροφοριών μέσω μιας ενιαίας επίθεσης - μιας διαδικασίας που ονομάζεται "hyperjacking". Μερικά παραδείγματα περιλαμβάνουν την παραβίαση ασφαλείας Dropbox και διαρροή iCloud 2014. Το Dropbox είχε παραβιαστεί τον Οκτώβριο του 2014, έχοντας πάνω από 7 εκατομμύρια κωδικούς πρόσβασης χρηστών κλεμμένους από χάκερ, σε μια προσπάθεια να αποκτήσει χρηματική αξία από την Bitcoins (BTC). Έχοντας αυτούς τους κωδικούς πρόσβασης, είναι σε θέση να διαβάσουν τα ιδιωτικά δεδομένα καθώς και να έχουν τα δεδομένα αυτά να αναπροσαρμόζονται από τις μηχανές αναζήτησης (καθιστώντας τις πληροφορίες δημόσιες). Υπάρχει το πρόβλημα της νόμιμης ιδιοκτησίας των δεδομένων. Πολλές συμφωνίες περί Όρων Παροχής Υπηρεσιών σιωπούν σχετικά με το ζήτημα της ιδιοκτησίας. Ο φυσικός έλεγχος του εξοπλισμού ηλεκτρονικών υπολογιστών (ιδιωτικό σύννεφο) είναι πιο ασφαλής από την απενεργοποίηση του εξοπλισμού και υπό τον έλεγχο κάποιου άλλου (δημόσιο σύννεφο). Αυτό παρέχει μεγάλο κίνητρο στους δημόσιους παρόχους υπηρεσιών cloud computing να δώσουν προτεραιότητα στην οικοδόμηση και διατήρηση ισχυρής διαχείρισης ασφαλών υπηρεσιών. Ορισμένες μικρές επιχειρήσεις που δεν διαθέτουν τεχνογνωσία στην ασφάλεια ΤΠ θα μπορούσαν να διαπιστώσουν ότι είναι πιο ασφαλές για αυτούς να χρησιμοποιούν ένα δημόσιο σύννεφο. Υπάρχει ο κίνδυνος οι τελικοί χρήστες να μην κατανοούν τα θέματα που εμπλέκονται κατά την πρόσβασή σας σε μια υπηρεσία σύννεφο όπου τα άτομα μερικές φορές δεν διαβάζουν τις πολλές σελίδες των όρων παροχής υπηρεσιών και απλά κάντε κλικ στο "Αποδοχή" χωρίς να το διαβάσετε. Αυτό είναι σημαντικό τώρα που το cloud computing γίνεται δημοφιλές και απαιτείται για να λειτουργούν ορισμένες υπηρεσίες, για παράδειγμα για έναν ευφυή προσωπικό βοηθό (το Siri της Apple ή το Google Now). Επίσης το ιδιωτικό νέφος θεωρείται πιο ασφαλές με υψηλότερα επίπεδα ελέγχου για τον ιδιοκτήτη, ωστόσο το δημόσιο σύννεφο φαίνεται να είναι πιο ευέλικτο και απαιτεί λιγότερες επενδύσεις χρόνου και χρήματος από τον χρήστη.

Ένα βασικό δόγμα που ισχύει στο cloud computing είναι ότι οι οργανισμοί και τα συστήματα πληροφοριών αλλάζουν συνεχώς και επίσης η διαχείριση της ασφάλειας είναι μια συνεχής διαδικασία και είναι κάτι πολύ σημαντικό για την ασφάλεια της διαχείρισης του cloud.



Εικόνα 24 Ασφάλεια στο cloud computing

2.1 Περιορισμοί και μειονεκτήματα

Το Cloud computing είναι φθηνότερο λόγω οικονομικών μεγεθών και - όπως και κάθε εξωτερική ανάθεση - τείνετε να πάρετε αυτό που παίρνετε. Λιγότερες επιλογές σε πολύ φθηνότερη τιμή: είναι ένα χαρακτηριστικό, όχι ένα σφάλμα. Επίσης ο πάροχος σύννεφων μπορεί να μην καλύψει τις νομικές ανάγκες και ότι οι επιχειρήσεις πρέπει να σταθμίσουν τα οφέλη του cloud computing έναντι των κινδύνων. Στο cloud computing, ο έλεγχος της υποδομής back-end περιορίζεται μόνο στον προμηθευτή σύννεφο. Οι πάροχοι σύννεφων συχνά αποφασίζουν για τις πολιτικές διαχείρισης, γεγονός που μετριάζει τι μπορούν να κάνουν οι χρήστες του cloud με την ανάπτυξή τους. Οι χρήστες σύννεφων περιορίζονται επίσης στον έλεγχο και τη διαχείριση των εφαρμογών, των δεδομένων και των υπηρεσιών τους. Περιλαμβάνει ανώτατα όρια δεδομένων, τα οποία τοποθετούνται σε χρήστες σύννεφο από τον προμηθευτή σύννεφο που κατανέμει συγκεκριμένο εύρος ζώνης για κάθε πελάτη και συχνά μοιράζονται μεταξύ άλλων χρηστών του cloud. Επίσης η ιδιωτικότητα και η εμπιστευτικότητα αποτελούν μεγάλες ανησυχίες σε ορισμένες

δραστηριότητες. Για παράδειγμα, οι ορκωτοί μεταφραστές που εργάζονται υπό τις προϋποθέσεις μιας NDA ενδέχεται να αντιμετωπίσουν προβλήματα σχετικά με ευαίσθητα δεδομένα που δεν είναι κρυπτογραφημένα. Το Cloud computing είναι επωφελές για πολλές επιχειρήσεις. μειώνει το κόστος και τους επιτρέπει να επικεντρωθούν στην αρμοδιότητα αντί για τα θέματα πληροφορικής και υποδομών. Παρ 'όλα αυτά, το cloud computing έχει αποδειχθεί ότι έχει κάποιους περιορισμούς και μειονεκτήματα, ειδικά για τις μικρότερες επιχειρηματικές δραστηριότητες, ιδιαίτερα όσον αφορά την ασφάλεια και τα downtime. Οι τεχνικές διακοπές είναι αναπόφευκτες και συμβαίνουν μερικές φορές όταν οι πάροχοι υπηρεσιών σύνεσης κατακλύζονται κατά τη διαδικασία εξυπηρέτησης των πελατών τους. Αυτό μπορεί να οδηγήσει σε προσωρινή αναστολή λειτουργίας. Δεδομένου ότι τα συστήματα αυτής της τεχνολογίας βασίζονται στο Διαδίκτυο, ένα άτομο δεν μπορεί να έχει πρόσβαση στις εφαρμογές, το διακομιστή ή τα δεδομένα του από το σύννεφο κατά τη διάρκεια μιας διακοπής.

Πρότυπα Διαχείρισης Ασφάλειας:

Τα πρότυπα που έχουν σχέση με τις πρακτικές διαχείρισης της ασφάλειας στο cloud είναι το ITIL και το ISO/IEC 27001 και 27002.

2.2 Προκλήσεις ασφάλειας υπολογιστών cloud

Η τρέχουσα υιοθέτηση του cloud computing συνδέεται με πολλές προκλήσεις, επειδή οι χρήστες εξακολουθούν να είναι σκεπτικοί σχετικά με την αυθεντικότητά του. Με βάση έρευνα που πραγματοποίησε η IDC το 2008, οι κύριες προκλήσεις που εμποδίζουν την υιοθέτηση του Cloud Computing αναγνωρίζονται από οργανισμούς είναι οι εξής:

1. **Ασφάλεια:** Είναι σαφές ότι το ζήτημα της ασφάλειας έχει παίξει τον σημαντικότερο ρόλο στην παρεμπόδιση της αποδοχής του Cloud computing. Χωρίς αμφιβολία, βάζοντας τα δεδομένα σας, τρέχοντας το λογισμικό σας στο σκληρό δίσκο κάποιου άλλου χρησιμοποιώντας την CPU κάποιου άλλου, φαίνεται να είναι τρομακτικό σε πολλούς. Τα γνωστά ζητήματα ασφάλειας, όπως η απώλεια δεδομένων, το ηλεκτρονικό ψάρεμα (phishing), το botnet (που εκτελούνται εξ αποστάσεως σε μια συλλογή μηχανών), θέτουν σοβαρά απειλή για τα δεδομένα και το λογισμικό του οργανισμού. Επιπλέον, το μοντέλο πολλαπλών μισθώσεων και οι συγκεντρωτικοί υπολογιστικοί πόροι στο cloud computing έχουν εισαγάγει νέες προκλήσεις ασφάλειας που απαιτούν νέες τεχνικές αντιμετώπισης. Για παράδειγμα, οι χάκερ μπορούν να χρησιμοποιήσουν το Cloud για να οργανώσουν το botnet, καθώς το Cloud συχνά παρέχει πιο αξιόπιστες υπηρεσίες υποδομής σε σχετικά φθηνότερη τιμή για να ξεκινήσουν μια επίθεση.

2. **Μοντέλο κοστολόγησης:** Οι καταναλωτές του νέφους πρέπει να εξετάσουν τις συναλλαγές μεταξύ των υπολογισμών, της επικοινωνίας και της ολοκλήρωσης. Ενώ η μετάβαση στο Cloud μπορεί να μειώσει σημαντικά το κόστος της υποδομής, αυξάνει το κόστος της επικοινωνίας δεδομένων, δηλαδή το κόστος μεταφοράς των δεδομένων ενός οργανισμού προς και από το κοινό και το κοινό Cloud και το κόστος ανά μονάδα υπολογιστικού πόρου που χρησιμοποιείται είναι πιθανό να είναι πιο ψηλά. Το πρόβλημα αυτό είναι ιδιαίτερα εμφανές εάν ο καταναλωτής χρησιμοποιεί το μοντέλο ανάπτυξης υβριδικού cloud όπου τα δεδομένα του οργανισμού διανέμονται μεταξύ πολλών δημόσιων / ιδιωτικών (εσωτερικών υποδομών πληροφορικής) / κοινοτικών σύννεφων. Ο διαισθητικός τρόπος και ο υπολογισμός έχει νόημα μόνο για εντατικές εργασίες CPU [9].

3. **Μοντέλο φόρτισης:** Η ελαστική ομάδα πόρων έχει κάνει την ανάλυση κόστους πολύ πιο περίπλοκη από τα κανονικά κέντρα δεδομένων, τα οποία συχνά υπολογίζουν το κόστος τους με βάση τις καταναλώσεις στατικού

υπολογισμού. Επιπλέον, μια εικονική μηχανή σε μορφή instantiated έχει γίνει η μονάδα ανάλυσης κόστους αντί του υποκείμενου φυσικού διακομιστή. Για τους παρόχους cloud της SaaS, το κόστος ανάπτυξης πολυεθνικής στο πλαίσιο της προσφοράς τους μπορεί να είναι πολύ σημαντικό. Αυτά περιλαμβάνουν: εκ νέου σχεδιασμός και ανάπλαση του λογισμικού που χρησιμοποιήθηκε αρχικά για την απλή μίσθωση, το κόστος της παροχής νέα χαρακτηριστικά που επιτρέπουν την εντατική προσαρμογή, την απόδοση και τη βελτίωση της ασφάλειας για την ταυτόχρονη πρόσβαση των χρηστών, και ασχολείται με την πολυπλοκότητα που προκαλείται από τις παραπάνω αλλαγές. Ως εκ τούτου, οι πάροχοι SaaS πρέπει να σταθμίσουν το αντιστάθμισμα μεταξύ της παροχής πολυεθνικής και της εξοικονόμησης κόστους που αποφέρει η πολυεπίπεδη, όπως η μείωση των γενικών εξόδων μέσω της απόσβεσης, ο μειωμένος αριθμός αδειών χρήσης λογισμικού επί τόπου κ.λπ. το βιώσιμο μοντέλο χρέωσης του παρόχου SaaS είναι κρίσιμο για την κερδοφορία και τη βιωσιμότητα των παρόχων υπηρεσιών cloud της SaaS [9].

4. **Συμφωνία επιπέδου εξυπηρέτησης (SLA):** Παρόλο που οι καταναλωτές του cloud δεν έχουν έλεγχο στους υποκείμενους υπολογιστικούς πόρους, πρέπει να διασφαλίσουν την ποιότητα, τη διαθεσιμότητα, την αξιοπιστία και την απόδοση αυτών των πόρων όταν οι καταναλωτές μεταναστεύσουν τις βασικές λειτουργίες τους στις εμπιστευμένες σύννεφο. Με άλλα λόγια, είναι ζωτικής σημασίας για τους καταναλωτές να λαμβάνουν εγγυήσεις από τους παρόχους σχετικά με την παράδοση υπηρεσιών. Συνήθως, αυτές παρέχονται μέσω συμφωνιών επιπέδου υπηρεσιών (SLA) που αποτελούν αντικείμενο διαπραγμάτευσης μεταξύ παρόχων και καταναλωτών. Το πρώτο ζήτημα είναι ο ορισμός των προδιαγραφών SLA με τέτοιο τρόπο ώστε να έχει το κατάλληλο επίπεδο λεπτομερούς επεξεργασίας, δηλαδή τις αντιπαραθέσεις μεταξύ εκφραστικότητας και περίπλοκου χαρακτήρα, ώστε να μπορούν να καλύψουν τις περισσότερες προσδοκίες των καταναλωτών και είναι σχετικά απλό να σταθμιστούν, αξιολογείται και επιβάλλεται από τον μηχανισμό

κατανομής πόρων στο σύννεφο. Επιπλέον, διαφορετικές προσφορές σύννεφων (IaaS, PaaS και SaaS) θα πρέπει να καθορίσουν διαφορετικές προδιαγραφές SLA. Αυτό δημιουργεί επίσης ορισμένα προβλήματα εφαρμογής στους παρόχους cloud. Επιπλέον, οι προηγμένοι μηχανισμοί SLA πρέπει να ενσωματώνουν συνεχώς στοιχεία ανατροφοδότησης και προσαρμογής των χρηστών στο πλαίσιο αξιολόγησης SLA [16].

5. **Τι να μεταναστεύσει:** Με βάση μια έρευνα (μέγεθος δείγματος = 244) που διεξήγαγε η IDC το 2008, τα επτά συστήματα πληροφορικής / εφαρμογές που μεταναστεύουν στο cloud είναι: Εφαρμογές Διαχείρισης Πληροφορικής (26.2%), Συνεργασίες (25.4% Προσωπικές Εφαρμογές (25%), Επιχειρηματικές Εφαρμογές (23,4%), Ανάπτυξη και Ανάπτυξη Εφαρμογών (16,8%), Χωρητικότητα διακομιστή (15,6%) και Χωρητικότητα Αποθήκευσης (15,5%). Αυτό το αποτέλεσμα αποκαλύπτει ότι οι οργανώσεις εξακολουθούν να έχουν ανησυχίες σχετικά με την ασφάλεια / προστασία της ιδιωτικής ζωής κατά τη μεταφορά των δεδομένων τους στο Cloud. Επί του παρόντος, οι περιφερειακές λειτουργίες όπως η διαχείριση της πληροφορικής και οι προσωπικές εφαρμογές είναι τα πιο εύκολα συστήματα πληροφορικής για να μετακινηθούν. Οι οργανισμοί είναι συντηρητικοί κατά τη χρήση του IaaS σε σύγκριση με το SaaS. Αυτό οφείλεται εν μέρει στο γεγονός ότι οι οριακές λειτουργίες συχνά ανατίθενται σε εξωτερικούς συνεργάτες στο Cloud και οι βασικές δραστηριότητες διατηρούνται εσωτερικά. Η έρευνα δείχνει επίσης ότι σε τρία χρόνια, το 31,5% της οργάνωσης θα μετακινήσει τη χωρητικότητα αποθήκευσης στο νέφος. Ωστόσο, ο αριθμός αυτός εξακολουθεί να είναι σχετικά χαμηλός σε σύγκριση με τις συνεργαζόμενες εφαρμογές (46,3%) την εποχή εκείνη [1]

Στόμα διαλειτουργικότητας Cloud: Επί του παρόντος, κάθε προσφορά cloud έχει τον δικό της τρόπο για το πώς αλληλεπιδρούν οι πελάτες cloud / εφαρμογές / χρήστες με το σύννεφο, οδηγώντας στο φαινόμενο "Hazy Cloud". Αυτό παρεμποδίζει σοβαρά την ανάπτυξη οικοσυστημάτων νέφους, αναγκάζοντας το

κλείδωμα του πωλητή, το οποίο απαγορεύει τη δυνατότητα των χρηστών να επιλέγουν από εναλλακτικούς πωλητές / προσφέροντας ταυτόχρονα, προκειμένου να βελτιστοποιήσουν τους πόρους σε διαφορετικά επίπεδα εντός ενός οργανισμού. Το πιο σημαντικό είναι ότι τα ιδιόκτητα API cloud καθιστούν πολύ δύσκολη την ενσωμάτωση των υπηρεσιών cloud με τα υπάρχοντα υπάρχοντα συστήματα ενός οργανισμού (π.χ. ένα κέντρο δεδομένων για εφαρμογές υψηλής διαδραστικής μοντελοποίησης σε μια φαρμακευτική εταιρεία). Ο πρωταρχικός στόχος της διαλειτουργικότητας είναι να συνειδητοποιήσει την ομαλή ρευστά δεδομένα σε σύννεφα και μεταξύ σύννεφων και τοπικών εφαρμογών. Υπάρχουν ορισμένα επίπεδα που η διαλειτουργικότητα είναι απαραίτητη για τον υπολογισμό του cloud. Πρώτον, για τη βελτιστοποίηση του ενεργητικού και των πόρων πληροφορικής, ένας οργανισμός πρέπει συχνά να διατηρεί εσωτερικά πληροφοριακά στοιχεία και ικανότητες που σχετίζονται με τις βασικές ικανότητές του, ενώ παράλληλα αναθέτουν σε cloud τις οριακές λειτουργίες και δραστηριότητες (π.χ. το σύστημα ανθρώπινων πόρων). Δεύτερον, συχνά, για λόγους βελτιστοποίησης, ένας οργανισμός μπορεί να χρειαστεί να αναθέσει σε εξωτερικούς συνεργάτες ορισμένες οριακές λειτουργίες στις υπηρεσίες cloud που προσφέρονται από διαφορετικούς πωλητές. Η τυποποίηση φαίνεται να είναι μια καλή λύση για την αντιμετώπιση του ζητήματος της διαλειτουργικότητας. Ωστόσο, καθώς το cloud computing μόλις αρχίζει να απογειώνεται, το πρόβλημα της διαλειτουργικότητας δεν εμφανίστηκε στην επείγουσα ατζέντα των μεγάλων προμηθευτών cloud. [9]

2.3 Μυστική κοινή χρήση

Εφευρέθηκε από τους Adi Shamir και George Blakley το 1979.

Είναι μια μέθοδος διανομής μυστικού μεταξύ μιας ομάδας συμμετεχόντων, όπου ο κάθε συμμετέχοντας έχει ένα μέρος του μυστικού. Για να ανακατασκευαστεί το μυστικό θα πρέπει να υπάρχουν όλα ή ένας επαρκής αριθμός ενδεχομένως διαφορετικών τύπων κομματιών-μερών του μυστικού που θα συνδυαστούν, αλλιώς μεμονωμένα κομμάτια δεν έχουν καμία χρησιμότητα. Σε ένα τύπο μυστικού συστήματος ανταλλαγής, υπάρχει ένας αντιπρόσωπος και n παίχτες. Ο αντιπρόσωπος δίνει στους παίχτες ένα κομμάτι από το μυστικό, αλλά μόνο όταν πληρούνται συγκεκριμένες προϋποθέσεις θα μπορούν οι παίχτες να ανασυγκροτήσουν το μυστικό από τα κομμάτια τους. Ο αντιπρόσωπος το επιτυγχάνει αυτό, δίνοντας σε κάθε παίχτη ένα μερίδιο με τέτοιο τρόπο ώστε οποιαδήποτε ομάδα t ή περισσότεροι παίχτες να μπορούν να ανακατασκευάσουν το μυστικό, αλλά καμία ομάδα λιγότερων από t παίχτες μπορεί. Ένα τέτοιο σύστημα ονομάζεται κατώτατο όριο(t,n).

Σημασία:

Τα συστήματα μυστικής κοινής χρήσης, είναι κατάλληλα για την αποθήκευση πληροφοριών που είναι ιδιαίτερα ευαίσθητες και εξαιρετικά σημαντικές. Παράδειγμα: κλειδιά κρυπτογράφησης, κωδικούς εκτόξευσης πυραύλων και τραπεζικούς λογαριασμούς. Κάθε μια από αυτές τις πληροφορίες θα πρέπει να διατηρείται σε μέγιστο βαθμό εμπιστευτική, διότι η έκθεσή τους μπορεί να είναι καταστροφική και επίσης είναι σημαντικό να μη χαθούν. Οι παραδοσιακές μέθοδοι κρυπτογράφησης είναι ακατάλληλες για ταυτόχρονη επίτευξη υψηλού επιπέδου εμπιστευτικότητας και αξιοπιστίας. Αυτό οφείλεται στο γεγονός ότι κατά την αποθήκευση ενός κλειδιού κρυπτογράφησης θα πρέπει να επιλέξουμε να διατηρήσουμε ένα μόνο αντίγραφο του κλειδιού, σε μια θέση για μέγιστη μυστικότητα ή να διατηρήσουμε πολλαπλά αντίγραφα σε διαφορετικές θέσεις για μεγαλύτερη αξιοπιστία. Η αύξηση της αξιοπιστίας του κλειδιού με την αποθήκευση πολλαπλών αντιγράφων, μειώνει την εμπιστευτικότητα, δημιουργώντας

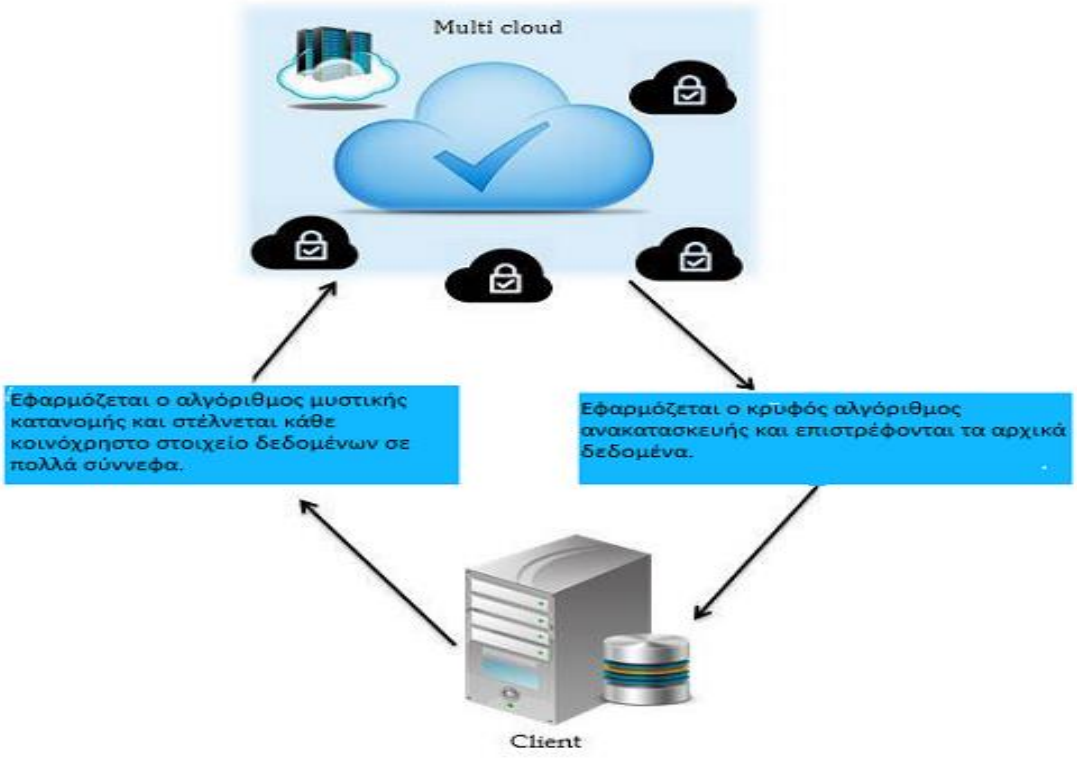
πρόσθετους φορείς επίθεσης. Υπάρχουν πολλές ευκαιρίες για ένα αντίγραφο να πέσει σε λάθος χέρια. Έτσι τα συστήματα μυστικής κατανομής αντιμετωπίζουν αυτό το πρόβλημα και επιτρέπουν την επίτευξη αυθαίρετα υψηλών επιπέδων εμπιστευτικότητας και αξιοπιστίας.

Τα συστήματα μυστικής κοινής χρήσης είναι σημαντικά σε περιβάλλοντα υπολογιστικού νέφους(cloud computing). Έτσι ένα κλειδί μπορεί να διανεμηθεί σε πολλούς servers μέσω ενός μηχανισμού μυστικής κοινής χρήσης και στη συνέχεια ν' ανασυγκροτείται όταν χρειάζεται. Η μυστική κοινή χρήση, επίσης έχει προταθεί για τα δίκτυα αισθητήρων όπου οι σύνδεσμοι είναι πιθανόν να αξιοποιηθούν με την αποστολή των δεδομένων σε μετοχές που καθιστούν το έργο του ακουστικού σκληρότερο. Η ασφάλεια σε αυτά τα περιβάλλοντα μπορεί να αυξηθεί με τη συνεχή αλλαγή τρόπου κατασκευής των μετοχών.

2.4 Το σχέδιο του Adi Shamir

Σε αυτό το σχήμα, οποιαδήποτε t από n μετοχές μπορεί να χρησιμοποιηθεί για να ανακτήσει το μυστικό. Το σύστημα βασίζεται στην ιδέα ότι μπορείτε να τοποθετήσετε ένα μοναδικό πολυώνυμο βαθμού (t - 1) σε οποιοδήποτε σύνολο σημείων t που βρίσκονται στο πολυώνυμο. Χρειάζονται δύο σημεία για να ορίσετε μια ευθεία γραμμή, τρία σημεία για να καθορίσετε πλήρως ένα τετράγωνο, τέσσερα σημεία για να ορίσετε μια κυβική καμπύλη κ.ο.κ. Δηλαδή, παίρνει t σημεία για να καθορίσει ένα πολυώνυμο βαθμού t - 1. Η μέθοδος είναι να δημιουργηθεί ένα πολυώνυμο βαθμού t - 1 με το μυστικό ως τον πρώτο συντελεστή και τους υπόλοιπους συντελεστές που συλλέγονται τυχαία. Στη συνέχεια βρείτε n σημεία στην καμπύλη και δώστε ένα σε κάθε παίκτη. Όταν τουλάχιστον t από τους παίκτες n αποκαλύπτουν τα σημεία τους, υπάρχουν επαρκείς πληροφορίες για να ταιριάζουν σε ένα πολυώνυμο βαθμού (t - 1), ενώ ο πρώτος συντελεστής είναι το μυστικό.

➢ Αλγόριθμος του Adi Shamir



Εικόνα 25 Δομικό διάγραμμα του αλγορίθμου κατανομής

Ο στόχος του αλγορίθμου είναι να διαιρέσει τα DATA δεδομένων σε n κομμάτια (DATA1, DATA2, DATA3, DATA4 ..DATAn) έτσι ώστε,

1. Η ανάκτηση κάθε k ή περισσότερων τεμαχίων DATAi καθιστά τα DATA εύκολα υπολογιστικά.
2. Η ανάκτηση οποιωνδήποτε k-1 ή λιγότερων τεμαχίων DATAi αφήνει DATA εντελώς απροσδιόριστη.

Το παραπάνω σχήμα είναι γνωστό ως κατώφλι (k, n). εάν k = n, τότε όλα τα κομμάτια είναι διαθέσιμα για την ανακατασκευή των DATA.Ο στόχος του αλγορίθμου κρυπτογράφησης του Adi Shamir είναι ότι τα σημεία k είναι αρκετά για να καθορίσουν ένα πολυώνυμο βαθμού k-1. Για παράδειγμα, 2 σημεία επαρκούν για τον ορισμό μιας γραμμής.

Επιλέξτε έναν συντελεστή c^0, c^1, c^2, c^3 ... .c^{k-1} στο H και αφήστε c^0 = S, όπου S είναι τα μυστικά δεδομένα που πρόκειται να αποθηκευτούν στο σύννεφο. Κατασκευάστε

το πολυώνυμο H (z) = c^0 + c1z^1 + c2 z^2 + ... + ck-1z^{k-1}. Στη συνέχεια, ορίζονται n σημεία, για παράδειγμα ορίστε i = 1,2 ... .n για να ανακτήσετε (i, H (i)). Δημιουργείται ζεύγος με είσοδο στο πολυώνυμο και έξοδο.

Λαμβάνοντας υπόψη κάθε υποσύνολο του k αυτών των ζευγών, χρησιμοποιώντας παρεμβολή μπορούν να βρεθούν οι συντελεστές του πολυωνύμου και το ο σταθερός όρος a0 είναι το μυστικό.

- **ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΣΑΜΙΡ:**

Το μυστικό χωρίζεται σε κομμάτια εξετάζοντας ένα κατά προσέγγιση πολυώνυμο βαθμού

H (z) = c^0 + c1z^1 + c2z^2 + ... + ck-1z^{k-1}

Στο οποίο c^0 = S, S^1 = H (1), S^2 = H (2), ..., S^n = H (n) και αντιπροσωπεύουν μία μετοχή z^i, G(z^i) = y^i).

ΠΑΡΑΔΕΙΓΜΑ : Για την κατανόηση της αριθμητικής ακεραίας θα χρησιμοποιήσουμε αντί άλλου διανύσματος ή επιστημονική αριθμητική βάση. Επομένως, το παρεχόμενο παράδειγμα δεν εξασφαλίζει απόλυτη μυστικότητα και δεν αποτελεί τέλειο παράδειγμα του σχεδίου του Adi Shamir.

Εξετάζουμε τον αριθμό 1999 ως τα μυστικά δεδομένα. Χωρίζοντας το σε 6 μέρη δηλαδή n = 6. Τα μέρη που απαιτούνται για την ανασυγκρότηση του μυστικού είναι 3 δηλαδή k = 3.

Επιλέγονται τυχαία δύο αριθμοί.Π.χ οι 154 και 19 όπου c1 = 154 και c2 = 19.Το πολυώνυμό μας για την παραγωγή μετοχών είναι: H (z) = 1999 + 154z + 19z^2.

Από το πολυώνυμο κατασκευάζονται έξι μέρη , όπου είναι τα (1, 2172). (2, 2383). (3, 2632). (4, 2919). (5, 3244). (6, 3607).

Διαφορετικό ενιαίο σημείο δίνεται σε κάθε συμμετέχοντα, τόσο z όσο και H (z).

Οποιαδήποτε 3 σημεία είναι αρκετά για να ανασυγκροτηθεί το μυστικό.

Υποθέτουμε: (a0, b0): (2, 2383); (a1, b1): (4, 2919). (a2, b2): (5,3244)

Εφαρμόστε πολυώνυμα βάσης Lagrange:

l0 = a-a1 / a0-a1. a-a2 / a0-a2 = 1 / $6a^2$-3 / 2a + 10/3

l1 = a-a0 / a1-a0. a-a2 / a1-α2 = 1 / $2a^2$ + 7 / 2a-5

l2 = a-a0 / a2-a0. a-a1 / a2-a1 = 1 / $3a^2$-2a + 8/3

Επομένως,

$\mathbf{H(z)} = \sum_{j=0}^{2} \mathbf{bj} \,.\, \mathbf{lj(z)}$ = 2383 (1/$6z^2$ - 3/2z +10/3) + 2919 (1/$2z^2$ + 7/2z – 5) + 3244 (1/$3z^2$ – 2z +8/3) Άρα H (z) = 1999 + 154z + $19z^2$.

Πώς να διαρρεύσει ένα μυστικό

Επισημοποιούμε την έννοια της υπογραφής δακτυλίου, η οποία καθιστά δυνατή τη διευκρίνιση ενός συνόλου πιθανών υπογραφόντων χωρίς να αποκαλύπτεται ποιο μέλος πράγματι παρήγαγε την υπογραφή. Αντίθετα με τις υπογραφές των ομάδων, οι υπογραφές των δακτυλίων δεν έχουν διαχειριστές ομάδων, καμία διαδικασία εγκατάστασης, καμία διαδικασία ανάκλησης και κανένα συντονισμό: οποιοσδήποτε χρήστης μπορεί να επιλέξει οποιοδήποτε σύνολο πιθανών υπογραφόντων που συμπεριλαμβάνει τον εαυτό του και να υπογράψει οποιοδήποτε μήνυμα χρησιμοποιώντας το μυστικό κλειδί του και το κοινό κλειδιά, χωρίς να λάβουν την έγκριση ή τη συνδρομή τους. Οι υπογραφές δακτυλίων παρέχουν έναν κομψό τρόπο διαρροής έγκυρων μυστικών με ανώνυμο τρόπο, να υπογράφουν τυχαία μηνύματα ηλεκτρονικού ταχυδρομείου με τρόπο που μπορεί να επαληθευτεί μόνο από τον αποδέκτη τους και να επιλυθούν άλλα προβλήματα σε υπολογισμό πολλών μερών. Η κύρια συμβολή του παρόντος εγγράφου είναι μια νέα κατασκευή τέτοιων υπογραφών, η οποία είναι άνευ όρων υπογεγραμμένη-διφορούμενη.

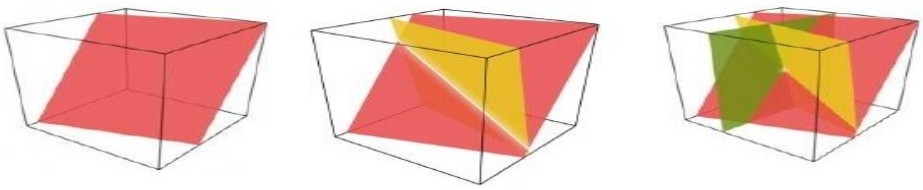
2.5 Το σχέδιο του George Blakley

Δύο μη παράλληλες γραμμές στο ίδιο επίπεδο τέμνονται ακριβώς σε ένα σημείο. Τρία μη παράλληλα επίπεδα στο διάστημα τέμνονται σε ένα ακριβώς σημείο. Γενικότερα, οποιαδήποτε *n* μη παράλληλα *(n-1*)διαστατικά υπερπλαίσια τέμνονται σε ένα συγκεκριμένο σημείο. Το μυστικό μπορεί να κωδικοποιηθεί ως κάθε μεμονωμένη συντεταγμένη του σημείου τομής. Εάν το μυστικό κωδικοποιείται χρησιμοποιώντας όλες τις συντεταγμένες, ακόμη και αν είναι τυχαίες, τότε ένας εσωτερικός (κάποιος που κατέχει ένα ή περισσότερα από τα *(n-1*)διαστατικά υπερπλαίσια) αποκτά πληροφορίες για το μυστικό. Αν κάποιος εμπιστευόμενος μπορεί να αποκτήσει περισσότερες γνώσεις σχετικά με το μυστικό από ό, τι ένας ξένος μπορεί, τότε το σύστημα δεν έχει πλέον πληροφορίες θεωρητική ασφάλεια . Εάν χρησιμοποιείται μόνο μία από τις συντεταγμένες *n* , τότε το εσωτερικό δεν γνωρίζει παρά έναν ξένο (δηλαδή, ότι το μυστικό πρέπει να βρίσκεται στην *x*- άξονα για ένα 2-διαστάσεων σύστημα). Κάθε παίκτης λαμβάνει αρκετές πληροφορίες για να καθορίσει ένα υπερπληρωτή. Το μυστικό ανακτάται υπολογίζοντας το σημείο τομής των επιπέδων των αεροπλάνων και στη συνέχεια παίρνοντας μια συγκεκριμένη συντεταγμένη της εν λόγω διασταύρωσης. Τέλος το σχέδιο του George Blakley είναι λιγότερο αποδοτικό από το Adi Shamir. ενώ οι μετοχές της Adi Shamir είναι το καθένα τόσο μεγάλες όσο το αρχικό μυστικό, οι μετοχές του George Blakley είναι t φορές μεγαλύτερες, όπου t είναι ο αριθμός κατωφλίων των παικτών. Το σχέδιο του George Blakley μπορεί να ενισχυθεί προσθέτοντας περιορισμούς σε ποια αεροπλάνα μπορούν να χρησιμοποιηθούν ως μετοχές. Το προκύπτον σχήμα είναι ισοδύναμο με το πολυωνυμικό σύστημα του Adi Shamir.

Στην παρακάτω εικόνα:

- Το μυστικό κωδικοποιείται ως ένα σημείο σε ένα διάστημα

- Κλειδιά δίνονται σαν υπερβολικά επίπεδα που περιστρέφονται γύρω από το σημείο στο διάστημα. Επομένως, η τομή ενός υπερδιπλασιασμού θα είναι το κλειδί.



Εικόνα 26 Blakley's schema

2.6 Μυστική κοινή χρήση χρησιμοποιώντας το θεώρημα του κινέζικου υπολοίπου

Η μυστική κοινή χρήση συνίσταται στην ανάκτηση μυστικού *S* από ένα σύνολο μετοχών, το καθένα από τα οποία περιέχει μερικές πληροφορίες σχετικά με το μυστικό. Το Κινεζικό υπόλοιπο θεώρημα δηλώνει ότι για ένα δεδομένο σύστημα ταυτόχρονων εξισώσεων συσχέτισης, η λύση είναι μοναδική σε μερικά **Z** / *n* **Z** , με *n* > 0 κάτω από κάποιες κατάλληλες συνθήκες στις συσχετίσεις. Η μυστική κοινή χρήση μπορεί έτσι να χρησιμοποιήσει το κινέζικο υπόλοιπο θεώρημα για να παράγει τα μερίδια που παρουσιάζονται στις εξισώσεις σύμφωνου και το μυστικό θα μπορούσε να ανακτηθεί με την επίλυση του συστήματος συσχέτισης για να πάρει τη μοναδική λύση, η οποία θα είναι το μυστικό για την ανάκτηση.

- **Σχέδια μυστικής κοινής χρήσης: διάφοροι τύποι**

Υπάρχουν διάφοροι τύποι προγραμμάτων μυστικής κοινής χρήσης. Οι πιο βασικοί τύποι είναι τα λεγόμενα συστήματα κατωφλίων, όπου μόνο η σοβαρότητα του συνόλου μετοχών έχει σημασία. Με άλλα λόγια, δεδομένου μίας μυστικής *S* και *n* μετοχών, κάθε σύνολο μετοχών *t* είναι ένα σύνολο με τη μικρότερη καρδιανότητα από την οποία μπορεί να ανακτηθεί το μυστικό, με την έννοια ότι οποιοδήποτε σύνολο μετοχών *t-1* δεν αρκεί για να δώσει *S* . Αυτό είναι

γνωστό ως δομή πρόσβασης κατωφλίου. Καλούμε τα συστήματα αυτά (*t* , *n*) όριο μυστική ανταλλαγή προγραμμάτων, ή *t* -out-of- *n* .

Τα προγράμματα μοιράσματος μυστικού ορίου διαφέρουν μεταξύ τους με τη μέθοδο δημιουργίας των μετοχών, ξεκινώντας από ένα συγκεκριμένο μυστικό. Το πρώτο από αυτά είναι το όριο μυστικό πρόγραμμα κοινής χρήσης Adi Shamir του , η οποία βασίζεται στο πολυώνυμο παρεμβολής για να βρει *S* από ένα δεδομένο σύνολο των μετοχών, και ο George Blakley γεωμετρικά μυστικό σύστημα καταμερισμού «s, η οποία χρησιμοποιεί γεωμετρικές μεθόδους για να ανακτήσει το μυστικό *S* . Τα συστήματα μυστικής κατανομής ορίων που βασίζονται στο κινέζικο υπόλοιπο θεώρημα οφείλονται στους Mignotte και Asmuth-Bloom, χρησιμοποιούν ειδικές ακολουθίες ακεραίων μαζί με το κινέζικο υπόλοιπο θεώρημα.

- **Κοινή μυστική χρήση του κινέζικου υπολοίπου θεωρήματος**

Δεδομένου ότι το κινέζικο υπόλοιπο θεώρημα μας παρέχει μια μέθοδο για να προσδιορίσουμε με μοναδικό τρόπο ένα *S* αριθμό modulo *k* - πολλά σχετικά ακεραίους , m1,m2…..mk, δεδομένου ότι $S < \prod_{i=1}^{k} m_i$, Τότε, η ιδέα είναι να κατασκευάσει ένα σύστημα που θα καθορίσει τις μυστικές *S* ,δίνονται οποιεσδήποτε *k* μετοχές (σε αυτήν την περίπτωση, το υπόλοιπο του *S* modulo καθένα από τα αριθμών m_i), αλλά δεν θα αποκαλύψει το μυστικό δεδομένο λιγότερο από *k* τέτοιων μερίδια. Τελικά επιλέγουμε *n* σχετικούς ακέραιους αριθμούς m1<m2<..<mn έτσι ώστε το *S να* είναι μικρότερο από το προϊόν οποιασδήποτε επιλογής *k* αυτών των ακεραίων, αλλά ταυτόχρονα είναι μεγαλύτερο από οποιαδήποτε επιλογή του *k-1* αυτών. Τότε οι μετοχές s1,s2..,sn ορίζεται από το si=S mod mi για i=1,2,…n. Με αυτό τον τρόπο, χάρη στο κινέζικο θεώρημα υπολοίπου, μπορούμε να καθορίσουμε με μοναδικό τρόπο το *S* από οποιοδήποτε σύνολο *k* ή περισσότερες μετοχές, αλλά όχι από μικρότερη από *k* . Αυτό παρέχει τη λεγόμενη δομή πρόσβασης κατωφλίου .

- **Το μυστικό σύστημα κοινής χρήσης του κατώτατου ορίου του Mignotte**

Όπως αναφέρθηκε προηγουμένως, Mignotte του κατωφλίου μυστικό επιμερισμού σύστημα χρησιμοποιεί, μαζί με το θεώρημα κινέζικου υπολοίπου, ειδική ακολουθία ακεραίων που ονομάζεται (*k* , *n*) -Mignotte αλληλουχίες οι οποίες αποτελούνται από *n* ακεραίων, κατά ζεύγη coprime, έτσι ώστε το προϊόν του μικρότερου *k* από αυτούς είναι μεγαλύτερη από το προϊόν των μεγαλύτερων *k* - 1 . Αυτός ο όρος είναι κρίσιμος επειδή το σύστημα βασίζεται στην επιλογή του μυστικού ως ακέραιου αριθμού μεταξύ των δύο προϊόντων και ότι τουλάχιστον τα μερίδια *k* είναι απαραίτητα για την πλήρη ανάκτηση του μυστικού, ανεξάρτητα από τον τρόπο που επιλέγονται. Άρα αφήνουμε $2 \leq k \leq n$ να είναι ακέραιοι. Η ακολουθία A (*k* , *n*) -Mignotte είναι μια αυστηρά αυξανόμενη ακολουθία θετικών ακέραιων αριθμών m1<..<mn ,με (mi,mj)=1 για όλα τα $1 \leq i < j \leq n$, έτσι ώστε $m_{n-k+2} \cdots m_n < m_1 \cdots m_k$.Ονομάζουμε αυτό το εύρος της εγκεκριμένης εμβέλειας. Κατασκευάζουμε ένα σχέδιο μοιραζόμενης μυστικής (*k* , *n*) - κατωφλίου ως εξής: επιλέγουμε το μυστικό *S* ως τυχαίο ακέραιο αριθμό στην εγκεκριμένη περιοχή,υπολογίζουμε για κάθε $1 \leq i \leq n$, η αναγωγή modulo mi του *S* που ονομάζουμε s*i,* αυτές είναι οι μετοχές.Για κάθε διαφορετική μετοχή *ksi1,….sik,* θεωρούμε το σύστημα συσχέτισης: x= *si1 mod mi1 ……x= s ik mod mik.* Από το κινέζικο υπόλοιπο θεώρημα, από τότε *mi1,… mik* είναι ζευγάρια coprime, το σύστημα έχει μια μοναδική λύση modulo *mi1,… mik* . Με την κατασκευή των μετοχών μας, αυτή η λύση δεν είναι παρά το μυστικό *S* να ανακάμψει.

- **Το μυστικό σύστημα κοινής χρήσης του Asmuth-Bloom**

Αυτό το σχήμα χρησιμοποιεί επίσης ειδικές ακολουθίες ακεραίων. Έστω $2 \leq k \leq n$ ακέραιοι. Θεωρούμε μια ακολουθία θετικών ακεραίων ζεύγους coprime m0<..<mn,έτσι ώστε m0*mn-k+2….mn<m1….mk.Γιαυτό επιλέγουμε το μυστικό S ως ένα τυχαίο ακέραιο στο $\mathbf{Z} / m_0\mathbf{Z}$. Στη συνέχεια, επιλέγουμε έναν τυχαίο ακέραιο αριθμό α έτσι S+α*m0<m1….mk.Υπολογίζουμε τη μείωση modulo m_i της S+α*m0,για όλα τα για όλα τα $1 \leq i \leq n$, αυτά είναι τα μερίδια Ii=(si,mi). Τώρα, για κάθε διαφορετική μετοχή *k Ii,…,Iik,θεωρούμε το σύστημα συσχέτισης: x=si1 mod mi1….. ,x=sik mod mik.* Από το κινέζικο υπόλοιπο θεώρημα, από τότε mi,…,mik είναι ζευγαρώς coprime , το σύστημα έχει μια μοναδική

λύση S_0 modulo mi1,…mik. Με την κατασκευή των μετοχών μας, το μυστικό S είναι η μείωση modulo m_0 του S_0 .

Είναι σημαντικό να σημειωθεί ότι η Mignotte (k , n) - το όριο μυστικό κοινής χρήσης σύστημα δεν είναι τέλειο, υπό την έννοια ότι μια σειρά από λιγότερο από k μετοχές περιέχει κάποιες πληροφορίες σχετικά με το μυστικό.Ενώ το σχήμα Asmuth-Bloom είναι τέλειο: α είναι ανεξάρτητο από το μυστικό S *και* το α μπορεί να είναι οποιοδήποτε ακέραιο modulo. Αυτό το προϊόν των k - 1 moduli είναι το μεγαλύτερο από οποιοδήποτε από τα n επιλέξει k - 1 πιθανά προϊόντα, επομένως κάθε υποσύνολο k - 1 ισοδυναμιών μπορεί να είναι οποιοδήποτε ακέραιο modulo το προϊόν του και καμία πληροφορία από το S διαρρέει.

Παράδειγμα

Τα παρακάτω είναι ένα παράδειγμα στο Σχέδιο του Asmuth-Bloom.

Επιλέγουμε $k = 3$ και $n = 4$. Οι αριθμοί μας coprime είναι m0=3,m1=11,m2=17 και m4=19.

Επειδή 3*17*19<11*13*17.Παίρνουμε ότι το μυστικό S=2 και επιλέγουμε α=51,ικανοποιώντας την απιτούμενη προυπόθεση για το σχέδιο του Asmuth-Bloom.

2+51*3=155 και υπολογίζουμε τις μετοχές για κάθε από τους ακεραίους 11,13,17,19 αντίστοιχα 1,12,2,3.

Θεωρούμε μία πιθανή ομάδα τριών μετοχών ,μεταξύ τεσσάρων πιθανών συνόλων των τριών μετοχών: {1,12,2} και δείχνουν ότι ανακτά το μυστικό S=2.

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 12 \mod 13 \\ x \equiv 2 \mod 17 \end{cases}$$

Για να λυθεί το σύστημα M=11*13*17.Από έναν εποικοδομητικό αλγόριθμο για την επίλυση ενός τέτοιου συστήματος, γνωρίζουμε ότι μια λύση στο σύστημα είναι x0=1*e1+12*e2+2*e3 , όπου κάθε e_i βρίσκεται ως εξής:

Από την ταυτότητα του Bézout, (mi,M/mi)=1,όπου θετικοί ακέραιοι ri και si που μπορούν να βρεθούν χρησιμοποιώντας τον εκτεταμένο Euclidean αλγόριθμο , έτσι ώστε

ri*mi+si*M/mi=1 και σειρά ei=si*M/mi.

Από τη ταυτότητα 1=1*221-20*11=(-5)*187+72*13=5*143+(-42)*17 ,

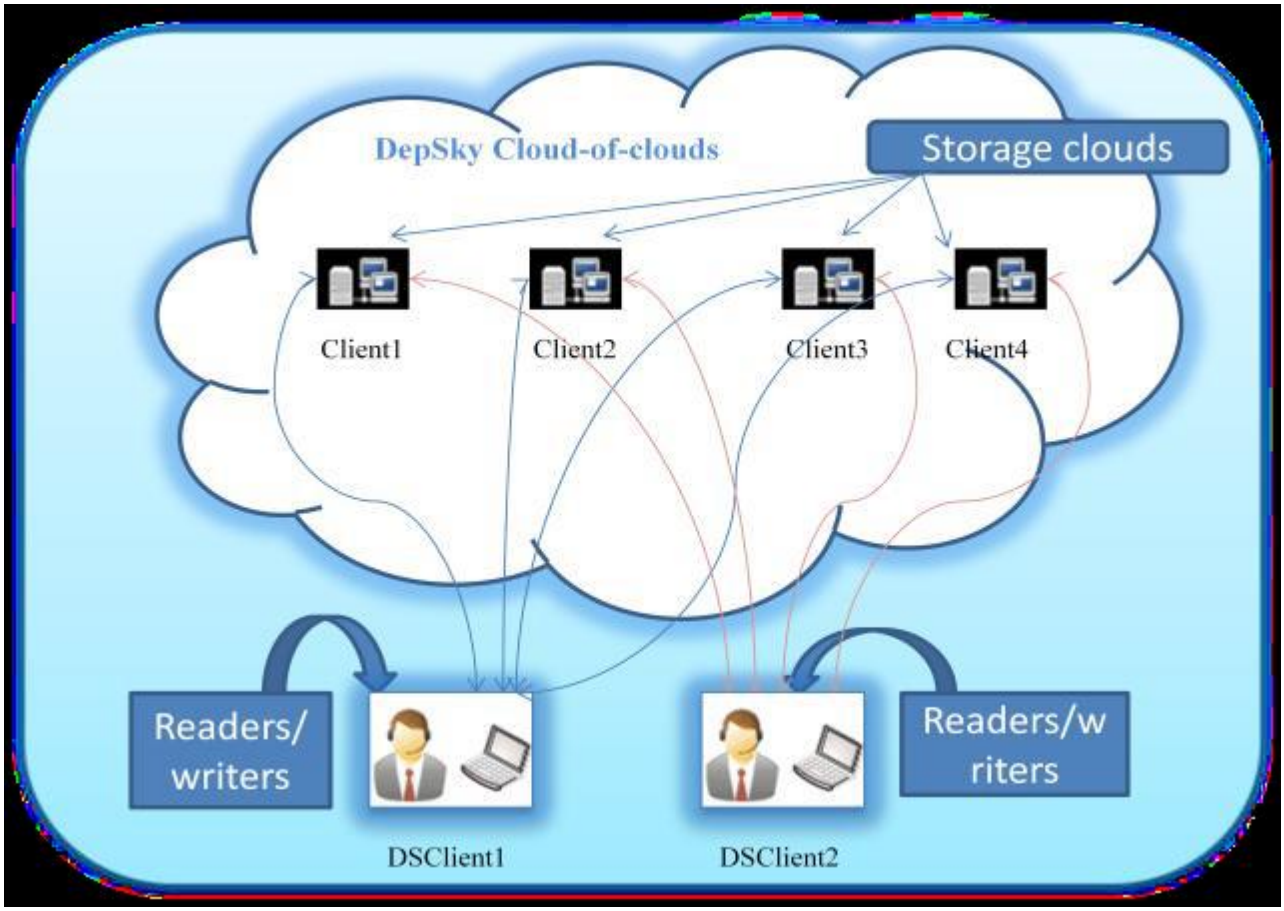
Παίρνουμε το e1=221,e2=-935,e3=715 και η μοναδική λύση modulo 11*13*17 είναι 155 και τέλος S=155=2 mod 3.

2.7 Μοντέλο Πολλαπλών Σύννεφων

Ο όρος "πολλαπλά σύννεφα" είναι παρόμοιος με τους όρους "δια-σύννεφα" ή "σύννεφο σύννεφων" που εισήγαγε ο Βουκόλιτς. Αυτοί οι όροι υποδηλώνουν ότι το cloud computing δεν πρέπει να τελειώνει με ένα μόνο σύννεφο.

Αρχιτεκτονική DepSky(Μοντέλο Πολλαπλών Σύννεφων)

Η αρχιτεκτονική DepSky αποτελείται από τέσσερα σύννεφα και κάθε σύννεφο χρησιμοποιεί τη δική του ειδική διεπαφή. Ο αλγόριθμος DepSky ζει στις μηχανές των αγοραστών ως βιβλιοθήκη προγραμμάτων για να μεταδίδει με κάθε σύννεφο. Αυτά τα τέσσερα σύννεφα είναι σύννεφα αποθήκευσης, επομένως δεν υπάρχουν κρυφοί χαρακτήρες που πρέπει να εκτελεστούν. Η βιβλιοθήκη DepSky επιτρέπει διαδικασίες ανάγνωσης και γραφής με τα σύννεφα αποθήκευσης και τους πολλαπλούς πελάτες τους.



Εικόνα 27 Σχέδιο συστήματος DepSKy

Το μοντέλο του συστήματος DepSky περιλαμβάνει τρία μέρη: αναγνώστες, συγγραφείς και τέσσερις παρόχους αποθήκευσης σύννεφων, όπου οι αναγνώστες και συγγραφείς είναι οι εργασίες του πελάτη. Η διαφορά μεταξύ αναγνωστών και συγγραφέων για αποθήκευση σε σύννεφα είναι ότι οι αναγνώστες μπορούν να αποτύχουν αυθαίρετα (για παράδειγμα, μπορούν να αποτύχουν με τη συντριβή, μπορούν να αποτύχουν από καιρό σε καιρό και στη συνέχεια να εμφανίσουν οποιαδήποτε συμπεριφορά) ενώ οι συγγραφείς αποτυγχάνουν μόνο με το crashing. Cloud αποθηκευτές στο μοντέλο του DepSky: Τα βυζαντινά πρωτόκολλα περιλαμβάνουν ένα σετ (n) όπου n = 3 f +1, και f είναι ο μέγιστος αριθμός σύννεφων που θα μπορούσαν να είναι ελαττωματικοί. Επιπλέον, κάθε υποσύνολο (n - f) σύννεφο αποθήκευσης δημιουργεί βυζαντινά πρωτόκολλα απαρτίας.

Το μοντέλο δεδομένων DepSky: Δεδομένου ότι το σύστημα DepSky ασχολείται με διαφορετικούς παρόχους cloud, η βιβλιοθήκη DepSky ασχολείται με διαφορετικούς παρόχους διασύνδεσης cloud και συνεπώς η μορφή δεδομένων γίνεται αποδεκτή

από κάθε σύννεφο. Το μοντέλο δεδομένων DepSky αποτελείται από τρία επίπεδα αφαίρεσης: τη μονάδα εννοιολογικών δεδομένων, μια γενική μονάδα δεδομένων και την υλοποίηση της μονάδας δεδομένων.

Αλγόριθμοι DepSky

- **DEPSKY-A- Διαθέσιμο DepSky**

Το πρώτο πρωτόκολλο DEPSKY ονομάζεται DEPSKY-A και βελτιώνει την προσβασιμότητα και την ακεραιότητα των αποθηκευμένων σε σύννεφο γεγονότων και αριθμών, αναπαράγοντάς τον σε ορισμένους παρόχους που χρησιμοποιούν μεθόδους απαρτίας.

- **DEPSKY-CA- εμπιστευτικό & διαθέσιμο DepSky**

Το πρωτόκολλο DEPSKY-A έχει δύο σημαντικούς περιορισμούς. Πρώτον, μια μονάδα δεδομένων των διαστάσεων S καταναλώνει το n_S αποθήκευσης της απεικόνισής τους, ένας συννεφιασμένος ουρανός ενσωματώνει διαφορετικά χρώματα και μορφές σύννεφων που οδηγεί σε διαφορετικές εφαρμογές και διοικητικούς τομείς. Αυτή η ενότητα παρουσιάζει το σύστημα DEPSKY. Αρχίζει με την παρουσίαση της αρχιτεκτονικής του σχήματος και στη συνέχεια καθορίζει τα μοντέλα δεδομένων και σχήματος, τους δύο κύριους αλγορίθμους (DEPSKY-A και DEPSKY-CA.) Αυτό το τμήμα θα εξηγήσει την τελευταία εργασία που έχει ολοκληρωθεί στην τοποθεσία των πολλαπλών σύννεφων. παρουσιάζουν ένα σύστημα εικονικής αποθήκευσης που ονομάζεται DepSky, το οποίο αποτελείται από ένα μείγμα διαφορετικών σύννεφων για την κατασκευή ενός νέφους σύννεφων . Το σύστημα DepSky τοποθετεί την προσβασιμότητα και την εμπιστευτικότητα των δεδομένων στο δικό του σύστημα αποθήκευσης χρησιμοποιώντας παροχείς πολλαπλών σύννεφων, συνδυάζοντας πρωτόκολλα βυζαντινού συστήματος απαρτίας, κρυπτογράφηση κρυπτογράφησης και κρυπτογράφηση χωρητικότητας του προγράμματος και κόστος σε μέσο n φορές περισσότερο από ό, τι αν ήταν αποθηκευμένο σε ένα μοναχικό σύννεφο. Δεύτερον, αποθηκεύει τα γεγονότα και τα αριθμητικά στοιχεία στο σαφές κείμενο, οπότε δεν δίδει διαβεβαιώσεις εμπιστευτικότητας. Για να αντιμετωπίσουμε αυτούς τους περιορισμούς,

χρησιμοποιούμε ένα σχέδιο διανομής μυστηρίων που συνδυάζει συμμετρική κρυπτογράφηση με ένα ακαδημαϊκό μυστικό σχεδιασμό διανομής και έναν βέλτιστο κώδικα διαγραφής για να χωρίσουν τα δεδομένα σε ένα σύνολο μπλοκ έτσι ώστε τα f +1 μπλοκ να είναι απαραίτητα για ανακτήσουμε τα αρχικά δεδομένα και για λιγότερα μπλοκ δεν δίνουν δεδομένα σχετικά με τα αποθηκευμένα δεδομένα.

2.8 Προληπτική μυστική κοινή χρήση

Εάν οι παίκτες αποθηκεύσουν τις μετοχές τους σε μη ασφαλείς εξυπηρετητές υπολογιστών, ένας εισβολέας θα μπορούσε να σπάσει και να κλέψει τις μετοχές. Αν δεν είναι πρακτικό να αλλάξουμε το μυστικό, μπορούν να ανανεωθούν οι μετοχές χωρίς συμβιβασμό (στυλ Adi Shamir). Ο αντιπρόσωπος παράγει ένα νέο τυχαίο πολυώνυμο με σταθερό μηδέν και υπολογίζει για κάθε εναπομείναντα παίκτη ένα νέο παραγγελθέν ζεύγος, όπου οι συντεταγμένες x των παλιών και των νέων ζευγών είναι οι ίδιες. Κάθε παίκτης προσθέτει στη συνέχεια τις παλιές και τις νέες συντεταγμένες y και διατηρεί το αποτέλεσμα ως τη νέα συντεταγμένη y του μυστικού. Όλες οι μη ενημερωμένες κοινές μετοχές που συσσωρεύονται οι εισβολείς γίνονται άχρηστες. Ένας εισβολέας μπορεί να ανακτήσει το μυστικό μόνο αν μπορεί να βρει αρκετές άλλες μη ενημερωμένες μετοχές για να φτάσει στο όριο. Αυτή η κατάσταση δεν πρέπει να συμβεί επειδή οι παίκτες διέγραψαν τις παλιές μετοχές τους. Επίσης, ένας εισβολέας δεν μπορεί να ανακτήσει πληροφορίες σχετικά με το αρχικό μυστικό από τα αρχεία ενημέρωσης επειδή περιέχει μόνο τυχαίες πληροφορίες.Ο αντιπρόσωπος μπορεί να αλλάξει τον αριθμό κατωφλίου κατά τη διανομή ενημερώσεων, αλλά πρέπει πάντα να παραμένει σε εγρήγορση των παικτών που διατηρούν μετοχές που έχουν λήξει.

2.9 Επαληθεύσιμη μυστική κοινή χρήση

Ένας παίκτης μπορεί να είναι με δικά του μερίδια για να αποκτήσει πρόσβαση σε άλλες μετοχές. Ένα VSS επιτρέπει στους παίκτες να είναι σίγουροι ότι κανένας άλλος παίκτης δεν ψεύδεται για το περιεχόμενο του αποθέματός τους μέχρι να υπάρξει μια λογική πιθανότητα λάθους. Τέτοια συστήματα δεν μπορούν να υπολογιστούν συμβατικά. οι παίκτες πρέπει να προσθέσουν και να πολλαπλασιάσουν συλλογικά τους αριθμούς χωρίς να ξέρουν ακριβώς τι προστίθεται και πολλαπλασιάζεται. Ο Tal Rabin και ο Michael Ben-Or δημιούργησαν ένα multi-contract system (MPC) που επιτρέπει στους παίκτες να ανιχνεύσουν ανυπαρξία από τον έμπορο ή μέρος του μέχρι το ένα τρίτο του αριθμού των κατωφλίων παικτών, ακόμη και αν αυτοί οι παίκτες συντονίζονται από ένα " προσαρμοστικό "επιτιθέμενο που μπορεί να αλλάξει στρατηγικές σε πραγματικό χρόνο σύμφωνα με τις πληροφορίες που έχουν αποκαλυφθεί.

2.10 Υπολογιστικά ασφαλής μυστική κοινή χρήση

Το μειονέκτημα των καθεστώτων μυστικής μοιράσματος που είναι ανεπιφύλακτα ασφαλή είναι ότι η αποθήκευση και η μετάδοση των μετοχών απαιτεί πόρους αποθήκευσης και εύρους ζώνης ισοδύναμους με το μέγεθος των μυστικών χρόνων από τον αριθμό των μετοχών. Αν το μέγεθος του μυστικού ήταν σημαντικό, π.χ. 2 GB, και ο αριθμός των μετοχών ήταν 20, τότε 20 GB των δεδομένων πρέπει να αποθηκεύονται από τους μετόχους. Εναλλακτικές τεχνικές έχουν προταθεί για να αυξηθεί σημαντικά η αποτελεσματικότητα των συστημάτων μυστικής κατανομής, παραμένοντας από την απαίτηση της άνευ όρων ασφάλειας.

Μία από αυτές τις τεχνικές, που είναι γνωστή ως μυστική κοινή χρήση, συνδύασε τον αλγόριθμο διασποράς πληροφοριών του Rabin (IDA) με τη μυστική από κοινού χρήση του Adi Shamir. Τα δεδομένα κρυπτογραφούνται για πρώτη φορά με τυχαία παραγόμενο κλειδί, χρησιμοποιώντας έναν συμμετρικό αλγόριθμο κρυπτογράφησης. Στη συνέχεια αυτά τα δεδομένα χωρίζονται σε N κομμάτια

χρησιμοποιώντας IDA του Rabin. Αυτό το IDA έχει ρυθμιστεί με ένα όριο, με τρόπο παρόμοιο με τα προγράμματα μυστικής κοινής χρήσης, αλλά σε αντίθεση με τα προγράμματα μυστικής κοινής χρήσης, το μέγεθος των δεδομένων που προκύπτουν αυξάνεται κατά έναν παράγοντα (αριθμός θραυσμάτων / κατώτατο όριο). Για παράδειγμα, εάν το όριο ήταν 10 και ο αριθμός των παραγόμενων από IDA θραυσμάτων ήταν 25, το συνολικό μέγεθος όλων των θραυσμάτων θα ήταν (25/10) ή 2,5 φορές το μέγεθος της αρχικής εισόδου. Στην περίπτωση αυτή, το σύστημα αυτό είναι 10 φορές πιο αποτελεσματικό από το αν το σχέδιο του Adi Shamir είχε εφαρμοστεί απευθείας στα δεδομένα. Το τελευταίο βήμα στη μυστική κοινή χρήση είναι η χρήση της μυστικής κατανομής Adi Shamir για την παραγωγή μετοχών του τυχαία παραγόμενου συμμετρικού κλειδιού (που συνήθως είναι της τάξεως των 16-32 bytes) και στη συνέχεια να δοθεί μία μετοχή και ένα κομμάτι σε κάθε μέτοχο.

2.11 Πολλαπλή μυστική και αποτελεσματική διανομή (διαδοχικά) μυστική κοινή χρήση

Οι πληροφορίες θεωρητικά ασφαλών προγραμμάτων μυστικής μοιράσματος είναι ανεπαρκείς ως προς το διάστημα, διότι μια τεχνική κοινής μυστικότητας k-out-of-n δημιουργεί n μερίδια καθένα τουλάχιστον μεγέθους αυτού του ίδιου του μυστικού, οδηγώντας σε μία αύξηση του απαιτούμενου αποθηκευτικού χώρου. Σε πολυ-μυστική κοινή χρήση που σχεδιάστηκε από τον Matthew K. Franklin και τον Moti Yung, πολλαπλά σημεία των πολυώνυμων οικοδεσποτών μυστικών. Η μέθοδος βρέθηκε χρήσιμη σε πολυάριθμες εφαρμογές από την κωδικοποίηση έως τους πολυπολιτισμικούς υπολογισμούς. Στο διαστημικό αποτελεσματικό μυστικό διαμοιρασμό, που επινοήθηκε από τους Abhishek Parakh και Subhash Kak, κάθε μετοχή είναι περίπου το κλάσμα (k-1) του μεγέθους του μυστικού. Αυτό το σχήμα κάνει χρήση επαναλαμβανόμενης πολυωνυμικής παρεμβολής και έχει πιθανές εφαρμογές στην ασφαλή διασπορά πληροφοριών στον Ιστό και στα δίκτυα αισθητήρων. Αυτή η μέθοδος βασίζεται στην κατανομή δεδομένων που περιλαμβάνει τις ρίζες ενός πολυωνύμου σε πεπερασμένο πεδίο. Έχουν επισημανθεί αργότερα ορισμένα τρωτά σημεία σχετικών με το διαστημικό σύστημα

μυστικότητας. Δείχνουν ότι ένα σχήμα που βασίζεται στη μέθοδο παρεμβολής δεν μπορεί να χρησιμοποιηθεί για να εφαρμόσει ένα σχήμα (k, n) όταν τα μυστικά k που πρόκειται να διανεμηθούν παράγονται εγγενώς από ένα πολυώνυμο βαθμού μικρότερο από k - 1 και το σχήμα δεν λειτουργεί εάν όλα των μυστικών που μοιράζονται είναι τα ίδια, κλπ.

2.12 Ασφαλής έναντι ανασφαλής μυστική κοινή χρήση

Ένα ασφαλές σύστημα μοιραζόμενης μυστικότητας διανέμει μετοχές, έτσι ώστε όποιος έχει λιγότερες από t μετοχές να μην έχει επιπλέον πληροφορίες για το μυστικό από κάποιον με 0 μετοχές. Για παράδειγμα, το σύστημα μυστικής κατανομής, στο οποίο η μυστική φράση "κωδικός πρόσβασης" χωρίζεται στα μερίδια "pa ------," "--ss ----", "---- wo--" και "------ rd,". Ένα άτομο με 0 μετοχές γνωρίζει μόνο ότι ο κωδικός πρόσβασης αποτελείται από οκτώ γράμματα. Θα έπρεπε να μαντέψει τον κωδικό πρόσβασης από 26 ^ 8 = 208 δισεκατομμύρια πιθανούς συνδυασμούς. Ωστόσο, ένα άτομο με μία μετοχή θα έπρεπε να μαντέψει μόνο τα έξι γράμματα, από 26 ^ 6 = 308 εκατομμύρια συνδυασμούς και ούτω καθεξής, καθώς περισσότερα άτομα συνωμοτούν. Συνεπώς, αυτό το σύστημα δεν είναι ένα "ασφαλές" σύστημα μοιραζόμενης μυστικής, επειδή ένας παίκτης με λιγότερα από τα μυστικά μερίδια είναι σε θέση να μειώσει το πρόβλημα της απόκτησης του εσωτερικού μυστικού χωρίς να χρειάζεται πρώτα να αποκτήσει όλα τα απαραίτητα μερίδια.

Αντίθετα, εξετάζοντας το σχέδιο μυστικής κατανομής, όπου το X είναι το μυστικό που πρέπει να μοιραστεί, το Pi είναι δημόσια ασύμμετρα κλειδιά κρυπτογράφησης και το Qi τα αντίστοιχα ιδιωτικά κλειδιά τους. Κάθε παίχτης J παρέχεται με {P1 (P2 (... (PN (X)))), Qj}. Σε αυτή την περίπτωση, οποιοσδήποτε παίχτης με ιδιωτικό κλειδί 1 μπορεί να αφαιρέσει το εξωτερικό στρώμα κρυπτογράφησης, ένας παίχτης με πλήκτρα 1 και 2 μπορεί να αφαιρέσει το πρώτο και το δεύτερο στρώμα κ.ο.κ. Ένας παίχτης με λιγότερα από τα πλήκτρα N δεν μπορεί ποτέ να φτάσει πλήρως στο μυστικό X χωρίς να χρειάζεται να αποκρυπτογραφήσει κρυπτογραφημένο άμορφης

μάζας με δημόσιο κλειδί για το οποίο δεν έχει το αντίστοιχο ιδιωτικό κλειδί - ένα πρόβλημα που θεωρείται σήμερα ότι δεν είναι υπολογιστικά εφικτό. Επίσης μπορούμε να δούμε ότι οποιοσδήποτε χρήστης με όλα τα ιδιωτικά κλειδιά Ν είναι σε θέση να αποκρυπτογραφήσει όλα τα εξωτερικά στρώματα για να αποκτήσει το Χ, το μυστικό και κατά συνέπεια αυτό το σύστημα είναι ένα ασφαλές σύστημα μυστικής διανομής.

Περιορισμοί:

Ορισμένα συστήματα μυστικής κοινή χρήσης λέγεται ότι είναι θεωρητικά ασφαλή και μπορούν να αποδειχτούν, ενώ άλλοι παραιτούνται από αυτή την άνευ όρων ασφάλεια για βελτιωμένη αποτελεσματικότητα διατηρώντας παράλληλα αρκετή ασφάλεια για να θεωρηθούν ασφαλή ως άλλα κοινά κρυπτογραφικά πρωτόγονα. Για παράδειγμα, θα μπορούσαν να επιτρέψουν την προστασία των μυστικών με μετοχές με 128 μονάδες εντροπίας η καθεμία, δεδομένου ότι κάθε μετοχή θα θεωρείται αρκετό για να υπονομεύσει οποιοδήποτε πιθανό αντίπαλο σήμερα, απαιτώντας μια επίθεση βίαιης δύναμης μέσου μεγέθους 2 ^ 127. Κοινή σε όλα τα καθεστώτα μυστικής ανταλλαγής χωρίς όρους, υπάρχουν περιορισμοί:

Κάθε μέρος του μυστικού πρέπει να είναι τουλάχιστον τόσο μεγάλο όσο το ίδιο το μυστικό. Αυτό το αποτέλεσμα βασίζεται στη θεωρία των πληροφοριών, αλλά μπορεί να κατανοηθεί διαισθητικά. Δεδομένης της μετοχής t-1, δεν μπορούν να προσδιοριστούν καθόλου πληροφορίες σχετικά με το μυστικό. Έτσι, το τελικό μέρος πρέπει να περιέχει τόσο πολλές πληροφορίες όσο το ίδιο το μυστικό. Υπάρχει μερικές φορές μια λύση για αυτόν τον περιορισμό συμπιέζοντας πρώτα το μυστικό πριν το μοιραστεί, αλλά αυτό συχνά δεν είναι δυνατό επειδή πολλά μυστικά (για παράδειγμα τα πλήκτρα) μοιάζουν με τυχαία δεδομένα υψηλής ποιότητας και είναι δύσκολο να συμπιεστούν.

Όλα τα συστήματα μυστικής κοινής χρήσης χρησιμοποιούν τυχαία κομμάτια. Για να διανείμετε ένα μυστικό ενός μπιτ μεταξύ των κατωφλίων t, είναι απαραίτητα t-1

τυχαία bits. Είναι απαραίτητο να διανείμετε ένα μυστικό της εντροπίας μήκους (t-1) * αυθαίρετου μήκους.

Ασήμαντο secret sharing:

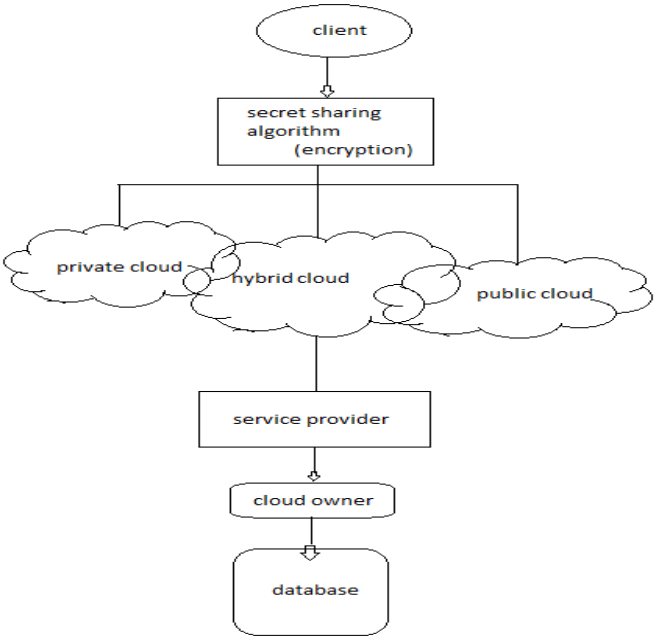
t = 1 μυστική ανταλλαγή είναι πολύ ασήμαντο. Το μυστικό μπορεί απλά να διανεμηθεί σε όλους τους n συμμετέχοντες.

t=n

Ιδιότητες secret sharing του Adi Shamir(k,n):

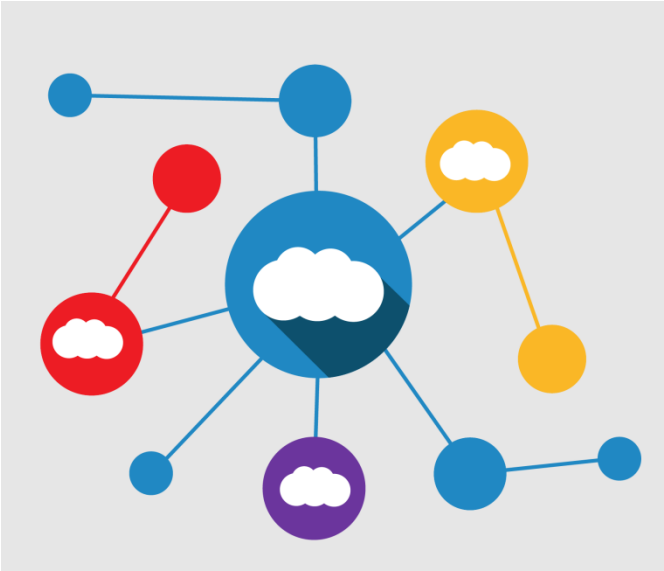
1. Ασφαλής
2. Ελάχιστο: Το μέγεθος κάθε τεμαχίου δεν υπερβαίνει το μέγεθος των αρχικών δεδομένων.
3. Επεκτάσιμη: Πότε k Διατηρείται σταθερή, Di Τα κομμάτια μπορούν να προστεθούν δυναμικά ή να διαγραφούν χωρίς να επηρεαστούν τα άλλα κομμάτια.
4. Δυναμική: Η ασφάλεια μπορεί εύκολα να βελτιωθεί χωρίς να αλλάξει το μυστικό, αλλά αλλάζοντας περιστασιακά το πολυώνυμο (διατηρώντας τον ίδιο ελεύθερο όρο) και κατασκευάζοντας νέες μετοχές στους συμμετέχοντες.
5. Ευέλικτη: Σε οργανισμούς όπου η ιεραρχία είναι σημαντική, μπορούμε να παρέχουμε σε κάθε συμμετέχοντα διαφορετικό αριθμό κομματιών ανάλογα με τη σημασία τους μέσα στον οργανισμό. Για παράδειγμα, ο πρόεδρος μπορεί να ξεκλειδώσει το χρηματοκιβώτιο μόνο, ενώ 3 γραμματείς απαιτείται μαζί για να το ξεκλειδώσουν.

Το σύστημα μυστικής κατανομής του Adi Shamir έχει ένα καλό αφηρημένο υπόβαθρο που παρέχει ένα εξαιρετικό πλαίσιο για αποδείξεις και εφαρμογές.



Εικόνα 28 Γενικό διάγραμμα, multi cloud -secret sharing

3ο Κεφάλαιο: MULTI CLOUD



Είναι η χρήση πολλαπλών υπηρεσιών cloud computing σε μία ενιαία ετερογενή αρχιτεκτονική. Π.χ μία επιχείρηση μπορεί να χρησιμοποιεί ξεχωριστούς παρόχους cloud για υπηρεσίες υποδομής (iaas) και λογιμσικού(saas) ή να χρησιμοποιεί πολλαπλούς παρόχους υποδομής (iaas).Στη περίπτωση που χρησιμοποιεί πολλαπλούς παρόχους υποδομής(iaas),μπορούν να χρησιμοποιήσουν διαφορετικούς παρόχους υποδομής για διαφορετικούς φόρτους εργασίας, να αναπτύξουν ένα φορτίο ισορροπημένο σε πολλούς παρόχους(ενεργό) ή να αναπτύξουν ένα αντίγραφο ασφαλείας σε άλλο(ενεργό-παθητικό).Υπάρχουν διάφοροι λόγοι για την ανάπτυξη μίας πολυεπίπεδης αρχιτεκτονικής, συμπεριλαμβανόμενης της μείωσης της εξάρτησης από κάθε πωλητή ,της αύξησης της ευελιξίας μέσω της επιλογής και του περιορισμού των καταστροφών. Είναι παρόμοιο με τη χρήση των καλύτερων εφαρμογών από πολλούς προγραμματιστές σε έναν προσωπικό υπολογιστή ,αντί των προεπιλογών που προσφέρει ο πωλητής του λειτουργικού συστήματος. Είναι μία αναγνώριση του γεγονότος ότι κανένας πάροχος δε μπορεί να είναι πάντα για όλους. Διαφέρει από το υβριδικό σύννεφο στο ότι αναφέρεται σε πολλές υπηρεσίες ανάπτυξης. Διάφορα θέματα παρουσιάζονται επίσης σε ένα πολύπλευρο περιβάλλον. Η ασφάλεια και η διακυβέρνηση είναι πιο περίπλοκη και περισσότερα κινούμενα μέρη μπορούν να δημιουργήσουν προβλήματα ευελιξίας. Η επιλογή των σωστών προϊόντων και υπηρεσιών cloud μπορεί επίσης να αποτελέσει πρόκληση και οι χρήστες ενδέχεται να υποφέρουν από το παράδοξο επιλογής.MULTI- cloud αποτελείται από πολλαπλά σύννεφα όπως openstack,Microsoft azure κ.λπ. Για παράδειγμα ενδέχεται να εκτελείται φόρτο εργασίας που απαιτεί μεγάλες ομάδες

πόρων αποθήκευσης και δικτύωσης σε ένα ιδιωτικό νέφος όπως το openstack.Ταυτόχρονα ενδέχεται να υπάρχει φόρτο εργασίας που χρειάζεται να κλιμακωθεί γρήγορα σε ένα δημόσιο σύννεφο, όπως το Microsoft azure ή το AWS.Κάθε φόρτος εργασίας τρέχει το ιδανικό σύννεφο, αλλά τώρα υπάρχουν πολλαπλά σύννεφα για διαχείριση.

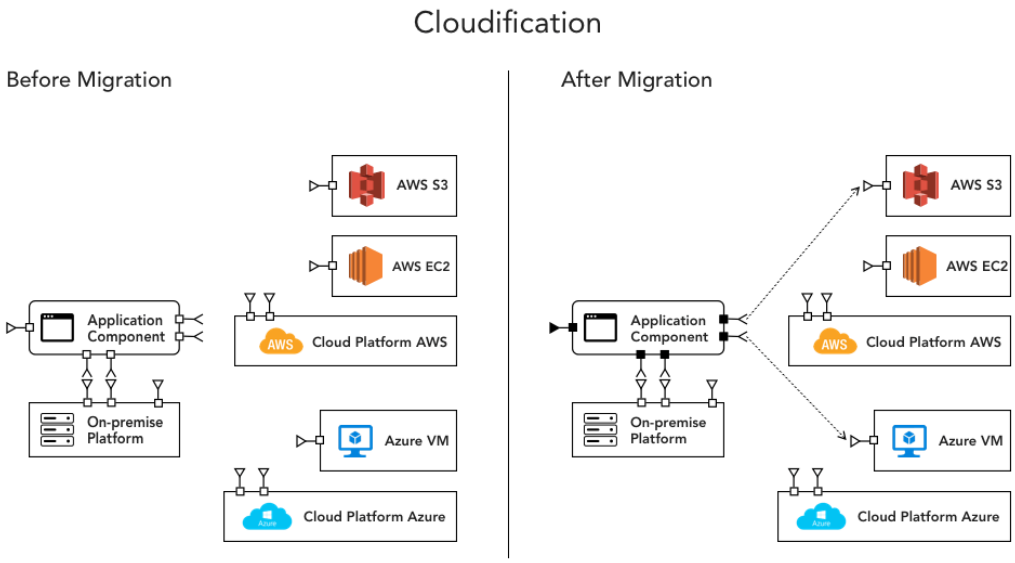
3.1 Αρχιτεκτονική multi- cloud για την παροχή απορρήτου δεδομένων και ακεραιότητας.

Τα τελευταία χρόνια η χρήση του cloud computing σε διαφορετικούς τρόπους όπως η αποθήκευση cloud, cloud hosting, cloud servers αυξάνονται στις βιομηχανίες και άλλες οργανώσεις σύμφωνα με τις απαιτήσεις. Ενώ εξετάζοντας τη δύναμη, τη σταθερότητα και την ασφάλεια του cloud, δεν μπορεί να αγνοήσει διαφορετικές απειλές για το χρήστη δεδομένα σχετικά με την αποθήκευση cloud.Ο έλεγχος πρόσβασης δεδομένων είναι ένας αποτελεσματικός τρόπος για να εξασφαλιστεί η ασφάλεια των δεδομένων στο σύννεφο. Ωστόσο, εξαιτίας της εξωτερικής ανάθεσης δεδομένων και των μη αξιόπιστων διακομιστών cloud, ο έλεγχος πρόσβασης δεδομένων γίνεται ένα προκλητικό ζήτημα στα συστήματα αποθήκευσης του cloud. Υπάρχουν συστήματα ελέγχου πρόσβασης που δεν εφαρμόζονται πλέον στα συστήματα αποθήκευσης cloud, επειδή είτε παράγουν πολλαπλά κρυπτογραφημένα αντίγραφα των ίδιων δεδομένων είτε απαιτούν ένα πλήρως αξιόπιστο διακομιστή σύννεφο. Ο κακόβουλος χρήστης στο χώρο αποθήκευσης σύννεφων γίνεται πιο δύσκολο να σταματήσει. Στο προτεινόμενο σύστημα εφαρμόζουμε την έννοια της πολλαπλής αποθήκευσης στο σύννεφο μαζί με την ενισχυμένη ασφάλεια χρησιμοποιώντας τεχνικές κρυπτογράφησης όπου μάλλον η αποθήκευση πλήρους αρχείου σε ένα σύστημα σύννεφο θα χωρίσει το αρχείο σε διαφορετικά κομμάτια και θα κρυπτογραφήσει και θα το αποθηκεύσει.

Ακολουθούν μερικές από τις αρχιτεκτονικές πολλών cloud:

Cloudification

Σε αυτή την αρχιτεκτονική εφαρμογή φιλοξενείται ένα στοιχείο που μπορεί να χρησιμοποιεί διαφορετικές υπηρεσίες cloud σε άλλες cloud πλατφόρμες για καλύτερη παρουσίαση.



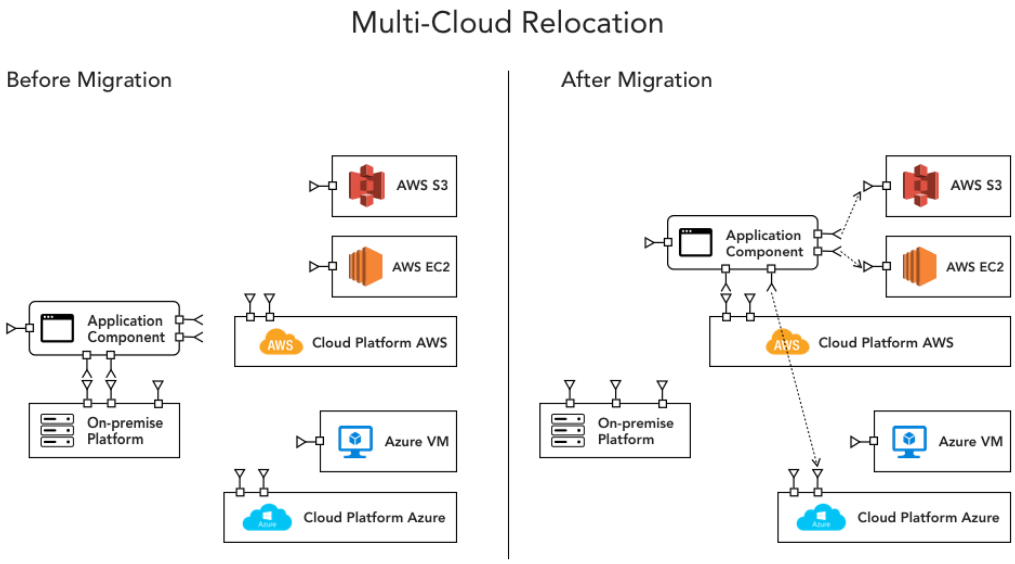
Εικόνα 29 Cloudification

Εδώ το στοιχείο εφαρμογής C1 έχει φιλοξενηθεί επί τόπου, αλλά μετά την υιοθέτηση του πολλαπλού cloud, χρησιμοποιεί την AWS υπηρεσία αποθήκευσης AWS S3 και για τον υπολογισμό χρησιμοποιεί εικονικές μηχανές Azure.

Πλεονεκτήματα: Βελτιώνει την διαθεσιμότητα σαν εφαρμογή που φιλοξενείται σε cloud πλατφόρμες και αποφεύγει το vendor lock-in.

Πολλαπλή μετακίνηση cloud

Σε αυτή την αρχιτεκτονική εφαρμογή φιλοξενείται ένα στοιχείο στην cloud πλατφόρμα και άλλες υπηρεσίες cloud από πολλαπλές πλατφόρμες cloud για την ενίσχυση των δυνατοτήτων.



Εικόνα 30 Multi-Cloud Relocation

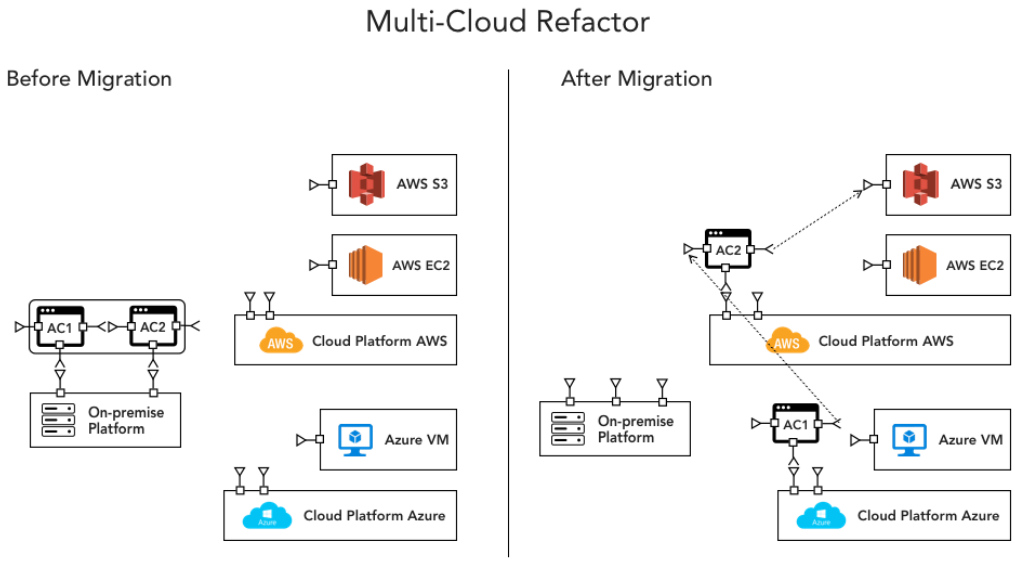
Εδώ η συνιστώσα εφαρμογής C1 επαναφέρεται στην πλατφόρμα AWS και είναι ανοικτή για να χρησιμοποιήσει τις περιβαλλοντικές υπηρεσίες του Azure. Χρησιμοποιεί το AWS S3 για αποθήκευση και διαθέτει μια επιλογή είτε για AWS είτε για Azure.

Πλεονεκτήματα: Βελτιώνει την διαθεσιμότητα σαν εφαρμογή που φιλοξενείται σε cloud πλατφόρμες και αποφεύγει το vendor lock-in.

Multi-Cloud Refactor

Για την παροχή καλύτερης QoS, μια εφαρμογή on-premise έχει ανασχεδιαστεί για ανάπτυξη σε πολλές πλατφόρμες cloud. Εδώ η εφαρμογή πρέπει να επανασχεδιαστεί , έτσι ώστε η ανάπτυξη εξαρτημάτων υψηλής χρήσης να μπορεί να

βελτιστοποιηθεί ανεξάρτητα. Η ανάπτυξη εξαρτημάτων υψηλής χρήσης βελτιστοποιείται ανεξάρτητα από αυτά που χρησιμοποιούνται με χαμηλή κατανάλωση. Ο παράλληλος σχεδιασμός επιτρέπει την καλύτερη απόδοση σε πλατφόρμες πολλαπλών cloud.



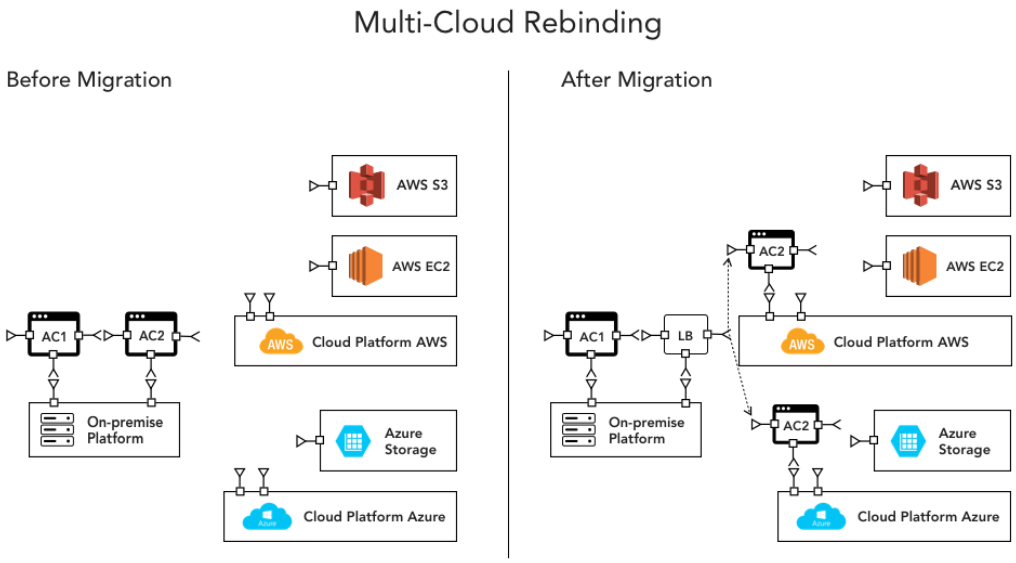
Εικόνα 31 Multi-Cloud Refactor

Εδώ AC1 και AC2 είναι δύο συστατικά στοιχεία εφαρμογών που φιλοξενούνται επί τόπου πριν από τη μετάβαση. Καθώς και τα δύο εξαρτήματα είναι ανεξάρτητες μονάδες ακεραιότητας, το AC1 αναπτύσσεται σε AWS χρησιμοποιώντας το AWS S3. Η AC2 αναπτύχθηκε σε Azure, και μπορεί να χρησιμοποιήσει οποιαδήποτε Azure's cloud υπηρεσία.

Οφέλη: Βέλτιστη δυνατότητα κλιμάκωσης / απόδοσης, ποικιλία επιλογών ανάπτυξης πολλαπλών cloud, ευελιξία ώστε να ανταποκρίνεται στις αλλαγές των επιχειρήσεων / τεχνολογιών πληροφορικής.

Multi-Cloud Rebinding

Η ανασχεδιασμένη εφαρμογή αναπτύσσεται εν μέρει σε περιβάλλοντα πολλαπλών cloud και επιτρέπει στην εφαρμογή να συνεχίσει να λειτουργεί χρησιμοποιώντας δευτερεύουσα ανάπτυξη όταν υπάρχει αποτυχία στην κύρια πλατφόρμα.



Εικόνα 32 Multi-Cloud Rebinding

Εδώ AC1 και AC2 είναι δύο συστατικά στοιχεία εφαρμογών που φιλοξενούνται πριν από τη μετάβαση. Καθώς και τα δύο εξαρτήματα είναι ανεξάρτητες μονάδες ακεραιότητας, το AC1 αφήνεται στην αρχή ενώ δύο AC2 αναπτύσσονται σε AWS και Azure για ανάκτηση καταστροφών. Το AC1 και δύο εξαρτήματα AC2 συνδέονται μέσω του διαύλου EBS ή του διαύλου υπηρεσίας.

Πλεονεκτήματα: Οι μη υγιής υπηρεσίες γίνονται και πάλι υγιείς, η κυκλοφορία μπορεί να παραδοθεί, επιστρέφοντας την απόκριση του συστήματος στο μέγιστο.

3.2 Προσέγγιση ασφάλειας για την αποθήκευση δεδομένων σε multi-cloud

Σε πολλές οργανώσεις, η μετατροπή των πληροφοριών και η αποθήκευση ευαίσθητων δεδομένων έχει ύψιστη προτεραιότητα. Τα δεδομένα του πελάτη θα πρέπει να φυλάσσονται μυστικά και να μην είναι προσβάσιμα από όλες τις άλλες μη

εξουσιοδοτημένες. Για να διατηρηθεί η ασφάλεια των δεδομένων χρηστών, το περιβάλλον του cloud computing έχει ασκηθεί. Το cloud computing είναι μια αποδοτική από πλευράς κόστους υπηρεσία, διαθεσιμότητα υπηρεσιών, ευέλικτη και πλατφόρμα παροχής υπηρεσιών κατόπιν ζήτησης για την παροχή υπηρεσιών μέσω του Διαδικτύου. Ωστόσο, ως ασφάλεια ενός ενιαίου cloud, δεν παρέχει ένα ισχυρό επίπεδο προστασίας από τις κακόβουλες επιθέσεις. Συνεπώς, υπάρχει πάντοτε ο κίνδυνος μη διαθεσιμότητας δεδομένων σε περίπτωση βλάβης του συστήματος. Μια κίνηση προς τα "πολλά σύννεφα" ή "πολλαπλά σύννεφα" ή "νέφος σύννεφων" έχει προκύψει χρησιμοποιώντας τον Adi Shamir's Secret Sharing Algorithm. Εδώ, υλοποιείται ο αλγόριθμος μυστικής κοινής χρήσης του Adi Shamir για τον έλεγχο ταυτότητας ενός μοναδικού χρήστη και για την πρόσβαση σε ένα συγκεκριμένο αρχείο από το cloud storage.

3.3 Συγκριτική μελέτη των μηχανισμών ασφαλείας σε multi-cloud περιβάλλον

Το πλεονέκτημα του cloud computing είναι αιώνιο αλλά φέρνει περισσότερα ζητήματα, συμπεριλαμβανομένης της ασφάλειας. Ο διπλός έλεγχος της ασφάλειας του cloud computing αποτελεί πρωταρχικό παράγοντα για το φυσικό περιβάλλον του cloud computing, καθώς οι χρήστες συχνά αποθηκεύουν ευαίσθητα δεδομένα με παρόχους αποθήκευσης cloud αλλά αυτοί οι πάροχοι ενδέχεται να μην έχουν εμπιστοσύνη. Οι παροχείς αποθήκευσης Cloud μπορεί να είναι single-cloud ή multi-cloud. Ωστόσο, διαπιστώνεται ότι η έρευνα σχετικά με τη χρήση των παρόχων πολλαπλών συνόρων για τη διατήρηση της ασφάλειας έχει λάβει λιγότερη προσοχή

από την ερευνητική κοινότητα από τη χρήση μεμονωμένων σύννεφων. Αυτό το άρθρο ερευνά πολλές τρέχουσες έρευνες που σχετίζονται με την ασφάλεια των σύννεφων και των πολλών ουρανών και αντιμετωπίζουν πιθανές λύσεις και μεθοδολογία. Κύριο μέλημα αυτής της εργασίας είναι η χρήση πολλών σύννεφων και η ασφάλεια των δεδομένων και η μείωση των κινδύνων ασφαλείας. Το παρόν έγγραφο παρέχει μια συγκριτική ανάλυση διαφόρων μηχανισμών ασφαλείας όπως το HAIL, το ICStore, το RACS, το μοντέλο DepSky χρησιμοποιώντας κρυπτογραφημένους αλγόριθμους. Έτσι θα μπορούσε να βοηθήσει στην ανάλυση του βέλτιστου σεναρίου για ένα κομψό ασφαλές περιβάλλον cloud computing.

3.4 Συνδυασμός μυστικής κοινής χρήσης και υπολογιστικού νέφους

Ένας αλγόριθμος μυστικού καταμερισμού προσέγγισης στην ασφάλεια υπολογιστικού νέφους σε απλά έως πολλαπλά σύννεφα.:

Η χρήση του cloud computing αυξάνεται ταχέως σε πολλούς κλάδους οργάνωσης και πληροφορικής και παρέχει νέο λογισμικό με χαμηλό κόστος. Έτσι, το cloud computing μας δίνει πολλά οφέλη με χαμηλό κόστος και πρόσβαση σε δεδομένα μέσω του Διαδικτύου. Η κατοχύρωση των κινδύνων ασφάλειας του cloud computing είναι ο βασικός παράγοντας στο περιβάλλον του cloud computing,όπως για παράδειγμα μπορεί να ανατεθεί ευαίσθητες πληροφορίες με παρόχους υπηρεσιών αποθήκευσης cloud. Ωστόσο, οι πάροχοι υπηρεσιών "single cloud" είναι λιγότερο δημοφιλείς στους πελάτες λόγω της αποτυχίας της παροχής υπηρεσιών σε κινδύνους και ενδεχομένως των κακόβουλων εμπιστευτικών στοιχείων στο "ενιαίο σύννεφο". Προς την κατεύθυνση της κίνησης "πολλών σύννεφων" ή "πολλαπλών σύννεφων" ή "σύννεφων σύννεφων" έχει αναδυθεί σήμερα χρησιμοποιώντας τον Adi Shamir's Secret Sharing Algorithm.Πολλά από τα τρέχοντα ερευνητικά έγγραφα που σχετίζονται με την ασφάλεια του σύννεφου και των πολλαπλών σύννεφων χρησιμοποιώντας τον αλγόριθμο Adi Shamir Secret Sharing και εξετάζει πιθανές λύσεις και μεθοδολογία. Κύριος στόχος αυτού είναι η χρήση πολλών σύννεφων και

ασφάλειας δεδομένων και η μείωση των κινδύνων ασφάλειας και επηρεάζουν τον χρήστη του cloud computing χρησιμοποιώντας τον αλγόριθμο Adi Shamir Secret sharing. Πρόκειται για μια μορφή μυστικής ανταλλαγής, όπου ένα μυστικό χωρίζεται σε μέρη, τα οποία δίνουν σε κάθε συμμετέχοντα το δικό του μοναδικό κομμάτι, όπου κάποια από τα μέρη ή όλα αυτά απαιτούνται για την ανακατασκευή του μυστικού. Εάν κάνουμε την καταμέτρηση όλων των συμμετεχόντων για να συνδυάσουμε μαζί το μυστικό μπορεί να είναι ανέφικτο και επομένως μερικές φορές χρησιμοποιείται το κατώτατο όριο όπου οποιοδήποτε "k" των τμημάτων είναι αρκετό για να ανασυγκροτήσει το αρχικό μυστικό. Όροι ευρετηρίου - Αλγόριθμος μυστικής κατανομής Adi Shamir, ακεραιότητα δεδομένων, αποθήκευση σύννεφων, εισβολή δεδομένων, διαθεσιμότητα υπηρεσιών.

3.5 Λειτουργία μυστικής κοινής χρήσης για εξασφάλιση multi-clouds στο cloud computing και τις εφαρμογές στην κρυπτογραφία κατωφλίου

Το βασικό σύστημα μοιραζόμενης μυστικότητας αποτελείται από τους δύο αλγόριθμους, δηλαδή την κοινή χρήση και την ανάκτηση (rec). Ο αλγόριθμος κοινής χρήσης διαιρεί ολόκληρο το μήνυμα M σε μικρά κομμάτια. Για να διατηρηθεί το μυστικό του μηνύματος M, το μερίδιο είναι πιθανοτικό, για να δείξει αυτό θα χρησιμοποιήσουμε το βέλος (→).Το αρχικό μήνυμα θα επιστρέψουμε μέσω του ντετερμινιστικού αλγόριθμου rec από κάποια ή όλα τα μερίδια.

Κοινή χρήση: Κοινή χρήση (M) → (S1, S2, ..., Sn, pub). Τα διαιρούμενα S μυστικά κατανέμονται με ασφάλεια μεταξύ όλων των εξυπηρετητών 1 έως n, και η pub είναι κοινό μερίδιο.

Ανάκτηση: Rec (S'1, S'2, ..., S'n, pub) = M ". Η ιδιότητα ορθότητας του αλγόριθμου λέει ότι για κάθε μήνυμα M, Rec (μερίδιο (M)) = M.

Για να ποσοτικοποιήσουμε την ασφάλεια του συστήματος εισήγαμε τέσσερις παραμέτρους κατωφλίου.

Όριο απορρήτου: δείχνει ότι ο μέγιστος αριθμός εξυπηρετητών δεν μπορεί να βρει το μυστικό, ακόμη και αν είναι συμβιβασμένο.

Όριο ανοχής σφάλματος: ο ελάχιστος αριθμός εξυπηρετητών από τους οποίους θέλουμε να ανακτήσουμε το μυστικό, ακόμη και ορισμένοι αποτυχημένοι διακομιστές.

Κατώτατο όριο ευρωστίας: εάν διακυβεύονται ορισμένοι διακομιστές, εμφανίζεται η ανάκτηση από τον ελάχιστο αριθμό σωστών κοινόχρηστων στοιχείων.

Ορθότητα κατωφλίου: Αυτό καθορίζει τον ελάχιστο αριθμό σωστών μεριδίων, ώστε να μην επαναφέρετε ποτέ το λανθασμένο μυστικό.

tp + 1 ≤tf≤tr≤n και ts ≤ tr.Σε κάθε σχήμα κρυπτογράφησης κατωφλίου, ένα μήνυμα είναι κρυπτογραφημένο έτσι ώστε περισσότεροι διακομιστές να κρυπτογραφήσουν το μήνυμα, αλλά λιγότεροι ,όχι. Λέμε ότι ένα σχήμα απαιτεί από τους t-out-of-n χρήστες να αποκρυπτογραφήσουν όταν t = tfandtp = t - 1.

n-out-of-n σχήματα

Παράδειγμα:

Θα δούμε πώς μοιράζεται 2 –out-of-2, δηλαδή μοιράζεται ένα μυστικό μεταξύ δύο διακομιστών και πρέπει να υπάρχουν και τα δύο σωστά κοινόχρηστα για να ανακτηθεί το μυστικό. Υποθέτουμε ότι M ∈ G όπου G είναι μια πεπερασμένη αβελιανή ομάδα υπό προσθήκη όπου ορίζουμε τον αλγόριθμο κοινής χρήσης ως εξής και στη συνέχεια, ο αλγόριθμος ανάκτησης είναι Rec (μερίδιο S (M): S1, S2) = S.

Μια άμεση γενίκευση των παραπάνω είναι το σχήμα n-out-of-n. Επιλέγουμε n-1 μετοχές τυχαία: Κοινή χρήση (M): S1, S2,. . . , Sn-1 ← GSn = M- (S1 + SR2 + · · + S). Όπως και προηγουμένως, ο αλγόριθμος ανάκτησης είναι έπειτα Rec (S1, S'n) = S'1 + Βάσει αυτού παρατηρήσαμε είναι ο τρόπος με τον οποίο θα λειτουργήσει η μυστική τεχνική κοινής χρήσης.

Ανάλυση στο παραπάνω :

Το μυστικό σύστημα κοινής χρήσης κλειδιών μπορεί να χρησιμοποιηθεί στο cloud computing για την εξασφάλιση μυστικών τιμών και δεδομένων. Αρκετά ανεξάρτητα συστήματα είναι συνδεδεμένα για να κάνουν συγκεκριμένες εργασίες και μορφές σύννεφο, το κύριο θέμα αυτής της εργασίας μπορεί να υποδιαιρεθεί σε κατώτατα όρια για μεμονωμένα συστήματα υπολογιστών. Αυτό το υπολογιστικό σύστημα έρχεται από αυτά τα όρια. Εάν κάποιος τρίτος έχει αποκτήσει πρόσβαση στις πληροφορίες από μερικούς διακομιστές, θα έχει μόνο μερικά κομμάτια κωδικοποιημένα ή κρυπτογραφημένα δεδομένα Αυτό το υπολογιστικό σύστημα έρχεται από αυτά τα όρια. Εάν κάποιος τρίτος έχει αποκτήσει πρόσβαση στις πληροφορίες από μερικούς διακομιστές, θα έχει μόνο μερικά κομμάτια κωδικοποιημένα ή κρυπτογραφημένα δεδομένα. Δεν είναι τόσο εύκολο να εισέλθει στο διακομιστή σύννεφο ένα μη εξουσιοδοτημένο άτομο, επειδή αποτελείται από πολλά συστήματα έτσι, κάθε σύστημα μπορεί να έχει διαφορετικές λειτουργίες όπως το λειτουργικό σύστημα, το σύστημα τείχους προστασίας, το λογισμικό κλπ.

(M) το παράδειγμα: t-out-of-n σχέδια που κάθε μερίδιο του μυστικού πρέπει να είναι τουλάχιστον τόσο μεγάλο όσο το ίδιο το μυστικό. Από την άλλη πλευρά, ένα σύστημα είναι υπολογιστικά ασφαλές αν είναι ασφαλές έναντι ενός υπολογιστικά περιορισμένου αντιπάλου. Τέτοια συστήματα μπορεί να βασίζονται στη σκληρότητα των μαθηματικών προβλημάτων. Η τέλεια μυστικότητα είναι ένας ειδικός τύπος κρυπτογραφημένου αλγορίθμου κλειδιού. Εάν κάθε S δεν παρέχει καμία πληροφορία χωρίς να γνωρίζει το μυστικό κλειδί του μηνύματος M, τότε το μερίδιο S είναι το απόλυτα μυστικό. Η δημιουργία τέλειου ιδιωτικού απορρήτου είναι πιο επιθυμητή και εάν είναι τέλεια, θα υπάρξει πολύπλοκη αντίδραση μεταξύ στατικών και προσαρμόσιμων αντιπάλων.

Συμπέρασμα:

Συμπεραίνουμε ότι η ασφάλεια του cloud computing αποτελεί τη βασική μέριμνα πλέον, όπου η χρήση του cloud computing αυξάνεται ραγδαία. Το πρώτο σκέλος του cloud πελάτη θέλει να χάσει τα ευαίσθητα δεδομένα από κακόβουλα μέσα στο σύννεφο. Πρόσφατα εντοπίστηκε ένα άλλο σημαντικό πρόβλημα είναι η απώλεια της διαθεσιμότητας υπηρεσιών λόγω αυτού του μεγάλου αριθμού των πελατών που υφίστανται. Για τους χρήστες cloud η εισβολή στα δεδομένα προκαλεί πολλά προβλήματα. Η αποθήκευση σε multi-cloud έχει λιγότερα προβλήματα ασφάλειας σε σχέση με το ενιαίο σύννεφο με πλούσια έρευνα. Γι' αυτό για τη μείωση των κινδύνων ασφαλείας του cloud computing, υποστηρίχτηκε η μετάβαση από ένα σε πολλά σύννεφα στους χρήστες του cloud.

4ο Κεφάλαιο: Ασφάλεια ηλεκτρονικών αρχείων υγείας που βασίζονται σε cloud

4.1 Ανάλυση των απαιτήσεων ασφάλειας και ιδιωτικού απορρήτου των συστημάτων ηλεκτρονικών αρχείων υγείας που βασίζονται σε cloud

Η μετακίνηση των ιατρικών πληροφοριών των ασθενών στο σύννεφο συνεπάγεται διάφορους κινδύνους όσον αφορά την ασφάλεια και την προστασία της ιδιωτικής ζωής των ευαίσθητων αρχείων υγείας. Προκειμένου να αποδειχθεί ότι, πριν μεταφερθούν τα αρχεία υγείας των ασθενών στο Cloud, οι ανησυχίες σχετικά με την ασφάλεια και την προστασία της ιδιωτικής ζωής πρέπει να λαμβάνονται υπόψη τόσο από τους παρόχους υπηρεσιών υγείας όσο και από τους παρόχους υπηρεσιών Cloud. Υποβάλλονται σε ανάλυση οι απαιτήσεις ασφάλειας ενός γενικού παροχέα υπηρεσιών Cloud. Ορισμένα από τα θέματα ασφάλειας που πρέπει να λαμβάνονται υπόψη τόσο από τους παρόχους υπηρεσιών Cloud όσο και από τους πελάτες τους στον τομέα της υγειονομικής περίθαλψης είναι η πρόσβαση βάσει ρόλων, οι μηχανισμοί ασφάλειας δικτύων, η κρυπτογράφηση δεδομένων, οι ψηφιακές υπογραφές και η παρακολούθηση της πρόσβασης. Επιπλέον, για να εγγυηθεί την ασφάλεια των πληροφοριών και να συμμορφωθεί με τις πολιτικές απορρήτου, ο πάροχος υπηρεσιών Cloud πρέπει να συμμορφώνεται με διάφορες πιστοποιήσεις και απαιτήσεις τρίτων, όπως το SAS70 Τύπος II, PCI DSS Επίπεδο 1, ISO 27001 και οι Ομοσπονδιακές Πληροφορίες των ΗΠΑ Νόμος περί Διαχείρισης Ασφάλειας (FISMA).

Συνδυάζοντας πρότυπα ασφάλειας και ιδιωτικής ζωής των παρόχων υγειονομικής περίθαλψης που πρέπει να ληφθούν υπόψη κατά την ανάπτυξη συστημάτων διαχείρισης EHR με τις πολιτικές Cloud και τους μηχανισμούς ασφαλείας που εφαρμόζουν οι πάροχοι, θα επιτευχθεί ένα ασφαλές σενάριο "Cloud Health".

4.2 Ηλεκτρονικό αρχείο καταγραφής της υγείας και θέματα ιδιωτικότητας

Η ανάπτυξη των συστημάτων διαχείρισης EHR είναι ένα από τα σημαντικότερα επιτεύγματα στην ηλεκτρονική υγεία τα τελευταία χρόνια. Η εφαρμογή αυτών των συστημάτων αναπτύσσεται με ταχύ ρυθμό. Στην πραγματικότητα, οι περισσότερες ανεπτυγμένες χώρες έχουν υψηλό επίπεδο διείσδυσης σε αυτό το είδος συστήματος.

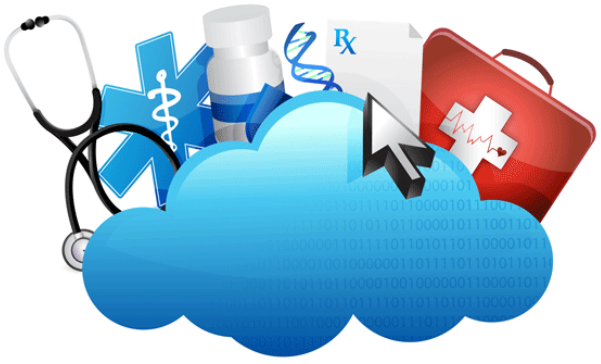
Σύμφωνα με τον ισπανικό νόμο 41/2002, ένα NAP ορίζεται ως η τεκμηρίωση, η οποία περιέχει πληροφορίες σχετικά με την κλινική εξέλιξη του ασθενούς κατά τη διάρκεια της διαδικασίας παροχής βοήθειας για την υγεία του. Στον νόμο αυτό, καθορίζονται οι χρήσεις των Ηλεκτρονικών αρχείων υγείας (HER), απαιτώντας από το ιατρικό προσωπικό τη διατήρηση της ιδιωτικής ζωής των ασθενών. Το ισπανικό δίκαιο αντιμετωπίζει τέτοιου είδους πληροφορίες ως αρχεία "ειδικά προστατευμένα". Αυτό το είδος ονοματολογίας ορίζεται στο νόμο 15/1999 με σκοπό την προστασία της ιδιωτικής ζωής των ευαίσθητων πληροφοριών των ασθενών. Η συγκατάθεση του ασθενούς απαιτείται για τη διαχείριση και την πρόσβαση στα δεδομένα αυτά, εκτός από την περίπτωση έκτακτης ανάγκης όπου υπάρχει κίνδυνος για τη ζωή του ασθενούς. Στις Ηνωμένες Πολιτείες, ο νόμος περί φορητότητας και λογοδοσίας για την ασφάλιση υγείας (HIPAA) ρυθμίζει και καθορίζει τις απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής των δεδομένων των ασθενών. Αυτός ο νόμος περιλαμβάνει δύο ενότητες σχετικά με την αποφυγή της κακής χρήσης προσωπικών πληροφοριών: τον Κανόνα Προστασίας Προσωπικών Δεδομένων και τον Κανόνα Ασφαλείας. Ο κανόνας περί προστασίας της ιδιωτικής ζωής του HIPAA ορίζει ότι πρέπει να διατίθενται οι πληροφορίες προστατευμένης υγείας (PHI) προκειμένου να παρέχεται η ιατρική περίθαλψη στον

ασθενή είτε με δικαστική απόφαση είτε με εξουσιοδότηση του ασθενούς. Αυτός ο κανόνας προσθέτει ότι οι φορείς που χρησιμοποιούν τις πληροφορίες για την υγεία πρέπει να ενημερώσουν τον ασθενή σχετικά με τη χρήση του PHI τους. Επιπλέον, ο Κανόνας Προστασίας Προσωπικών Δεδομένων απαιτεί οι οντότητες που έχουν πρόσβαση στο PHI να χρησιμοποιούν το ελάχιστο ποσό των δεδομένων ασθενών που είναι απαραίτητες για την κάλυψη των αναγκών τους. Ο κανόνας ασφαλείας HIPAA ορίστηκε το 2003 και συμπληρώνει τον κανόνα προστασίας προσωπικών δεδομένων, προσθέτοντας αρκετούς όρους για την αντιμετώπιση της ψηφιοποίησης των πληροφοριών για την υγεία των ασθενών. Διαθέτει τρία είδη εγγυήσεων ασφάλειας: διοικητικές, τεχνικές και φυσικές.

Έτσι, όπως υπογραμμίζεται παραπάνω, οι πάροχοι υπηρεσιών υγείας πρέπει να εγγυώνται και να διατηρούν την ασφάλεια και το απόρρητο των EHR και στη συνέχεια να εφαρμόζουν τους απαιτούμενους μηχανισμούς ασφαλείας για να διατηρούν τις πληροφορίες των ασθενών ασφαλείς στο Cloud.

4.3 Απαιτήσεις ασφάλειας ηλεκτρονικών δεδομένων υγείας και ιδιωτικού απορρήτου

Πριν από τη μετακίνηση των ηλεκτρονικών αρχείων υγείας (EHRs) στο Cloud, τα ίδια τα συστήματα ΕΔΑ πρέπει να ορίσουν αρκετές εγγυήσεις για τη διατήρηση ευαίσθητων πληροφοριών για τους ασθενείς. Ο συνδυασμός αυτών των απαιτήσεων ασφαλείας με τις απαιτήσεις των συστημάτων Cloud θα εγγυάται την προστασία της ιδιωτικής ζωής και την ασφάλεια των EHR που φιλοξενούνται στο Cloud. Τα θέματα ασφάλειας και ιδιωτικού απορρήτου που πρέπει να αντιμετωπίσει ένα σύστημα που βασίζεται σε σύννεφα για την προστασία των αρχείων ασθενών αναλύονται



στην επόμενη ενότητα. Οι απαιτήσεις για τη διασφάλιση ενός EHR περιγράφονται παρακάτω:

- **Εξουσιοδοτημένη πρόσβαση**: Προκειμένου να αναπτυχθεί ένα σύστημα εγκεκριμένου ελέγχου, είναι απαραίτητο να αναπτυχθεί ένα σύστημα ταυτοποίησης τόσο για τους ασθενείς όσο και για τους παρόχους υγειονομικής περίθαλψης. Αυτή η αναγνώριση πρέπει να είναι φορητή μεταξύ των διαφόρων οντοτήτων που έχουν πρόσβαση στα δεδομένα των ασθενών. Αυτό το σύστημα μπορεί να επιτευχθεί με το αναγνωριστικό ταυτότητας κάθε ασθενούς. Όσον αφορά τον έλεγχο ταυτότητας, ένα κεντρικό σύστημα βασισμένο σε ένα δημόσιο κλειδί είναι βιώσιμο. Πρέπει να αναπτυχθεί ένας έλεγχος πρόσβασης βάσει ρόλων (RBAC), προκειμένου να επιτραπεί σε εξουσιοδοτημένο προσωπικό την πρόσβαση σε συγκεκριμένα δεδομένα βάσει του ρόλου τους.

- **Εμπιστευτικότητα:** Για να διασφαλιστεί η εμπιστευτικότητα της διαδικασίας επικοινωνίας, χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης. Ωστόσο, το πρόβλημα εμπιστευτικότητας σε ένα κατανεμημένο σύστημα προκύπτει επειδή δεν είναι δυνατό το σύστημα πομπού πληροφοριών να επαληθεύσει ότι η εμπιστευτικότητα δεν έχει εκτεθεί στο λήπτη.

- **Συγκατάθεση του ασθενούς:** Σύμφωνα με τη νομοθεσία, οι ασθενείς πρέπει να επιτρέπουν ή να μην επιτρέπουν την πρόσβαση σε κλινικές πληροφορίες, εκτός από καταστάσεις έκτακτης ανάγκης. Αυτή η συγκατάθεση μπορεί να

είναι σιωπηρή ή ρητή. Ένα άλλο γεγονός που πρέπει να ληφθεί υπόψη είναι η ανάγκη να αποκτηθεί πρόσβαση στην οντότητα που φιλοξενείται στο EHR από άλλη εξωτερική. Η διαδικασία αυτή θα πρέπει να έχει τη συγκατάθεση του ασθενούς, αλλά σε περίπτωση έκτακτης ανάγκης, πρέπει να παρέχεται μηχανισμός ασφαλείας για την αποφυγή αυτού του περιορισμού χωρίς τη συγκατάθεση του ασθενούς.

- **Συνάφεια:** Όλο το ιατρικό προσωπικό που συμμετέχει στη διαδικασία διάγνωσης και θεραπείας έχει πρόσβαση στο EHR. Το διοικητικό προσωπικό θα έχει πρόσβαση στις κλινικές πληροφορίες εάν η λειτουργία τους είναι σχετική με την ιατρική διαδικασία.Συνεπώς, μόνο το σχετικό προσωπικό θα έχει πρόσβαση στις πληροφορίες του ασθενούς. Για να διασφαλιστεί ότι μόνο αυτό το επίπεδο προσωπικού μπορεί να έχει πρόσβαση στα δεδομένα, πρέπει να αναπτυχθεί ένα σύστημα ελέγχου πρόσβασης.Δεδομένης της δυσκολίας προσδιορισμού της συνάφειας των πληροφοριών, είναι προτιμότερο να υπάρχει προεπιλεγμένη πρόσβαση στις άδειες και, εάν χρειάζεται, να μελετώνται πιθανές καταχρήσεις.

- **Ιδιοκτησία πληροφοριών:** Η ιδιοκτησία του HS δεν είναι σαφώς καθορισμένη. Το ιατρικό προσωπικό είναι υπεύθυνο για αυτές τις πληροφορίες. Ωστόσο, οι ίδιοι οι ασθενείς έχουν το δικαίωμα πρόσβασης στις κλινικές τους πληροφορίες.

- **Συνοχή πληροφοριών:** Σε ένα σχέδιο διαλειτουργικότητας, πρέπει να δημιουργηθεί ένας μηχανισμός κοινοποίησης

διόρθωσης προκειμένου να επιδειχθούν αλλαγές στις πληροφορίες. Αυτό το σύστημα πρέπει να επιτρέπει την πρόσβαση στις προηγούμενες εκδόσεις των EHR, εάν είναι απαραίτητο.

- **Έλεγχοι:** Ένα μητρώο ελέγχου πρέπει να περιλαμβάνει όλες τις προσβάσεις στις πληροφορίες και όλες τις αλλαγές που έχουν πραγματοποιηθεί στα NAP. Αυτό το σύστημα επιτρέπει την παρακολούθηση της πρόσβασης και αποτελεί ένα ισχυρό εργαλείο για την εξασφάλιση ασφαλούς συστήματος. Αυτό το σύστημα ελέγχου πρέπει να πληροί τις απαιτήσεις διαλειτουργικότητας.

- **Αρχειοθέτηση:** Τα ιατρικά αρχεία πρέπει να αρχειοθετούνται για ορισμένο χρονικό διάστημα, σύμφωνα με τη νομοθεσία της αντίστοιχης χώρας. Μετά από αυτό το χρονικό διάστημα, τα ιατρικά δεδομένα ενδέχεται να διαγραφούν. Ωστόσο, αυτό δεν συνιστάται όταν πρόκειται για τη διαχείριση και την πρακτική του EHR, όπου ο στόχος είναι να διατηρούνται οι πλήρεις ιατρικές πληροφορίες για τον ασθενή για τη ζωή του / της. Ωστόσο, από υλικοτεχνικής απόψεως, αυτό θα είχε τεράστιες μακροπρόθεσμες απαιτήσεις αποθήκευσης

4.3.1 Τα κύρια χαρακτηριστικά της ηλεκτρονικής υγείας

- Αποδοτικότητα (Efficiency): Ένας τρόπος μείωσης του κόστους είναι η αποφυγή διπλών ή μη απαραίτητων διαγνωστικών μέσω επικοινωνίας ανάμεσα στους φορείς υγείας και τον ασθενή.
- Βελτίωση ποιότητας περίθαλψης: Η αύξηση της αποδοτικότητας δεν μειώνει

μόνο το κόστος αλλά βελτιώνει ταυτόχρονα και την ποιότητα.

- Επιστημονική τεκμηρίωση: Οι ενέργειες της ηλεκτρονικής υγείας πρέπει να τεκμηριώνονται με την έννοια ότι η αποδοτικότητά τους πρέπει να αποδεικνύεται με επιστημονικές μεθόδους.
- Ενδυνάμωση πολιτών και ασθενών: Καθιστώντας τις βάσεις δεδομένων υγείας και τον προσωπικό ηλεκτρονικό ιατρικό φάκελο προσβάσιμο από το διαδίκτυο, ανοίγονται νέοι ορίζοντες για ανθρωποκεντρικά συστήματα υγείας και διευκολύνεται ο ασθενής στις επιλογές του.
- Διευκόλυνση της ανταλλαγής της πληροφορίας και της επικοινωνίας με πρότυπο τρόπο ανάμεσα στους φορείς υγείας. Με αυτό τον τρόπο υπάρχει μια μορφή διαλειτουργικότητας. Δίνεται η δυνατότητα προσπέλασης και ελέγχου σε δεδομένα όλων των συστημάτων με την ταυτόχρονη ύπαρξη ενός ενιαίου σημείου διαχείρισης και διοίκησης.
- Επέκταση της εμβέλειας της ιατρικής περίθαλψης πέρα από τα συμβατικά όρια, τόσο με την γεωγραφική όσο και με την μεταφορική έννοια του όρου. Οι πολίτες έχουν τη δυνατότητα να χρησιμοποιούν online ιατρικές υπηρεσίες που παρέχονται από διεθνείς παροχείς.
- Ασφάλεια: Η ηλεκτρονική υγεία περιλαμβάνει νέες μορφές αλληλεπίδρασης ασθενή – ιατρού και δημιουργεί νέες προκλήσεις σε θέματα ασφαλείας όπως το ιατρικό απόρρητο.
- Ισότητα: Μια από τις υποσχέσεις της ηλεκτρονικής υγείας είναι η πιο ισότιμη ιατρική περίθαλψη.
- Εκπαίδευση ιατρών και παραιατρικού προσωπικού από online πηγές αλλά και των πολιτών (π.χ. ιατρικές πληροφορίες πρόληψης).
- Ενθάρρυνση σχέσεων ασθενή και επαγγελματία υγείας, ώστε οι αποφάσεις να λαμβάνονται με κοινό τρόπο.

4.4 Θέματα ασφάλειας και ιδιωτικού απορρήτου λύσεων υγείας που βασίζονται σε σύννεφα

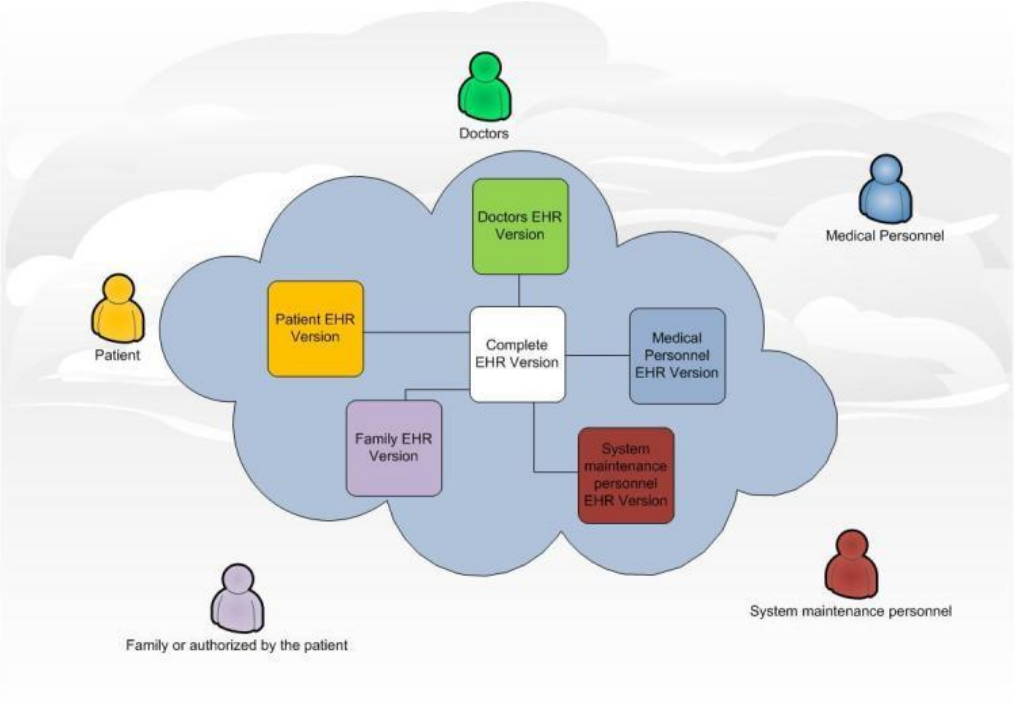
Η ανάπτυξη λύσεων υγείας που βασίζονται στο σύννεφο αποτελεί ένα σημαντικό βήμα στην ανάπτυξη της ηλεκτρονικής υγείας. Τα συστήματα που βασίζονται σε σύννεφα επιτρέπουν τη δημιουργία κλιμακούμενων περιβαλλόντων προσαρμοσμένων στις ανάγκες των χρηστών. Αυτή η συνολική προσαρμογή συμπληρώνεται από την εξοικονόμηση που προσφέρει ένα σύστημα πληρωμής ανά χρήση, όπως το Cloud computing. Ένα άλλο μεγάλο πλεονέκτημα προέρχεται από το γεγονός ότι, όταν τα EHR φιλοξενούνται στο Cloud, το ιατρικό προσωπικό ή οι ασθενείς έχουν την δυνατότητα να έχουν πρόσβαση στις πληροφορίες ανά πάσα στιγμή από όπου και αν έχουν σύνδεση στο Διαδίκτυο. Επί του παρόντος, με την παγκόσμια οικονομική κρίση, η εξοικονόμηση χρημάτων θα μπορούσε να είναι ένας από τους σημαντικότερους λόγους που θα οδηγούσε μια εταιρεία να μετακινήσει το ηλεκτρονικό σύστημα υγείας της στο Cloud. Επομένως, οι πάροχοι υπηρεσιών Cloud πρέπει να επωφεληθούν από αυτό το γεγονός όταν πωλούν τους υποψήφιους πελάτες τους για τα πλεονεκτήματα των συστημάτων που βασίζονται σε Cloud. Προκειμένου να διασφαλιστεί η ασφάλεια των συστημάτων τους, οι παροχείς υπηρεσιών Cloud πρέπει να εγκαταστήσουν αρκετούς μηχανισμούς ασφαλείας για να διατηρήσουν την ασφάλεια, την ιδιωτικότητα και την ασφάλεια των δεδομένων των πελατών τους.

Ένα NAP που βασίζεται σε σύννεφο πρέπει να διατηρεί το ίδιο επίπεδο ασφάλειας δεδομένων με τα δεδομένα που είναι αποθηκευμένα στους διακομιστές του παρόχου υγειονομικής περίθαλψης. Οι ασθενείς και το ιατρικό προσωπικό θα πρέπει να γνωρίζουν ότι τα προσωπικά τους στοιχεία θα αποθηκεύονται με τρίτο πάροχο. Ο πάροχος πρέπει να εγγυάται την ίδια ασφάλεια και ιδιωτικότητα που είχαν τα EHR στους τοπικούς διακομιστές. Ο ασθενής, προφανώς, δεν εμπλέκεται στη διαδικασία μεταφοράς των ευαίσθητων πληροφοριών τους στο Cloud, αλλά οι πληροφορίες πρέπει να κοινοποιούνται στους ασθενείς από τους παρόχους

υγειονομικής περίθαλψης σχετικά με τη μετάδοση δεδομένων. Αυτές οι επικοινωνίες δεν είναι απλές ειδοποιήσεις. Αντίθετα, οι ασθενείς θα πρέπει να ενημερώνονται για όλα τα πλεονεκτήματα που προσφέρει ένα σύστημα που βασίζεται στο σύννεφο για τη διαχείριση των ιατρικών τους πληροφοριών. Οι ασθενείς πρέπει να γνωρίζουν ότι η ευθύνη διαχείρισης δεδομένων βρίσκεται και στα δύο μέρη: τον παροχέα υπηρεσιών Cloud και, με πιο ενεργό τρόπο, τον πάροχο υγειονομικής περίθαλψης ή το κλινικό κέντρο. Ωστόσο, υπάρχουν ζητήματα ασφάλειας που πρέπει να λαμβάνονται υπόψη τόσο από τους παρόχους όσο και από τους πελάτες ενός συστήματος με HER που βασίζεται σε σύννεφο.

4.5 Πρόσβαση βάσει ρόλων

Υπάρχουν πολλά διαφορετικά είδη προσωπικού που θα έχουν πρόσβαση στο αρχείο υγείας των ασθενών, από τους ίδιους τους ασθενείς έως τους τεχνικούς που είναι υπεύθυνοι για τη διαχείριση των εξυπηρετητών του παροχέα. Οι ιατροί, το ιατρικό προσωπικό ή οι υπάλληλοι του παροχέα υπηρεσιών Cloud θα μπορούσαν να έχουν πρόσβαση σε αυτά τα δεδομένα. Για να διασφαλιστεί η προστασία της ιδιωτικής ζωής των δεδομένων των ασθενών, απαιτείται ένα σύστημα πρόσβασης βασισμένο σε ρόλους, επειδή ένας γιατρός μπορεί να έχει διαφορετικές απαιτήσεις πρόσβασης στις πληροφορίες για τους ασθενείς από ό, τι άλλο τεχνικό προσωπικό. Προκειμένου να ξεπεραστεί αυτό το πρόβλημα, πρέπει να αντιστοιχιστεί ένας κωδικός ή αριθμός αναγνώρισης σε κάθε άτομο που έχει πρόσβαση στις αποθηκευμένες πληροφορίες. Ανάλογα με τον αριθμό ταυτότητας, ο χρήστης θα ανήκουν σε μια ομάδα και κάθε είδους ομάδα θα έχει πρόσβαση σε ένα συγκεκριμένο μέρος των πληροφοριών ασθενούς. Για παράδειγμα, οι ασθενείς και οι γιατροί θα έχουν πρόσβαση σε ολόκληρο το αρχείο υγείας, ενώ το προσωπικό που είναι υπεύθυνο για τη συντήρηση της πλατφόρμας θα έχει πρόσβαση μόνο στις πληροφορίες που χρειάζονται για τη σωστή λειτουργία του συστήματος. Με αυτό το σύστημα βασισμένο στο ρόλο, η προστασία της ιδιωτικής ζωής των ασθενών είναι σχετικά εγγυημένη.



Εικόνα 33 Σύστημα βασισμένο σε ρόλους με διάφορες εκδόσεις ηλεκτρονικών αρχείων καταγραφής υγείας διαθέσιμες ανάλογα με το είδος του χρήστη του Health Cloud

4.6 Μηχανισμοί ασφάλειας δικτύων

Ο κύριος κίνδυνος για τις πληροφορίες θα είναι πιθανώς "εκτός" της πλατφόρμας Cloud. Το προσωπικό του παροχέα δεν είναι η κύρια απειλή που πρέπει να φοβηθεί κανείς. Είναι σημαντικό να γνωρίζουμε ότι όταν μεταφέρονται τα δεδομένα των ασθενών στο Cloud, οι πάροχοι υγειονομικής περίθαλψης εκθέτουν αυτές τις πληροφορίες σε διάφορες εξωτερικές απειλές, επειδή τα δεδομένα είναι τώρα διαθέσιμα μέσω του Internet .Ως εκ τούτου, η ευθύνη πρέπει να βρίσκεται στον ίδιο τον πάροχο Cloud για να προστατεύσει την ασφάλεια και το απόρρητο των πληροφοριών παρέχοντας την απαραίτητη ασφάλεια για να αποφύγει τις εξωτερικές επιθέσεις να κλέψουν ή ακόμη και να διαγράψουν τις πληροφορίες.

4.7 Κρυπτογράφηση δεδομένων και Ψηφιακή υπογραφή

Όλες οι ευαίσθητες πληροφορίες για τους ασθενείς θα πρέπει να αποθηκεύονται με ασφάλεια σε ιατρικό ιατρικό αρχείο, έτσι ώστε οι ιατρικές πληροφορίες να μπορούν να μοιράζονται από διάφορους γιατρούς ή ιατρικό προσωπικό. Προκειμένου να εξασφαλιστεί αυτή η συναλλαγή, οι πληροφορίες πρέπει να κρυπτογραφούνται και να ελέγχονται σωστά.

Η ψηφιακή υπογραφή είναι ένα πολύ χρήσιμο εργαλείο που παρέχει αυθεντικότητα, ακεραιότητα και μη επανάληψη. Με αυτόν τον μηχανισμό ασφαλείας, εξασφαλίζεται η αυθεντικότητα του ψηφιακού αρχείου. θα είναι πολύτιμη η ανάπτυξη αυτού του είδους του συστήματος στο Health Cloud προκειμένου να αποφευχθούν οι ψευδείς συναλλαγές δεδομένων. Για τα μηνύματα που αποστέλλονται μέσω ενός μη ασφαλούς καναλιού, η ψηφιακή υπογραφή δίνει στον παραλήπτη τη διαβεβαίωση ότι ένα μήνυμα ή αρχείο έχει αποσταλεί από τον διεκδικημένο αποστολέα. Υπάρχουν πολλοί κρυπτογραφικοί λογάριθμοι για την ανάπτυξη αυτού του είδους εργαλείου ασφαλείας.

Πρέπει να εισαχθεί ένα κατάλληλο σύστημα κρυπτογράφησης προκειμένου να επιτευχθεί εμπιστευτικότητα σε ένα σύστημα ηλεκτρονικού αρχείου υγείας. Τα δεδομένα κρυπτογραφούνται στους διακομιστές και ο ίδιος ο πάροχος αποθηκεύει τα κλειδιά κρυπτογράφησης. Τα συστήματα κρυπτογράφησης πρέπει να εγγυώνται ότι το απόρρητο του ασθενούς προστατεύεται, αν υποτεθεί ότι ο ασθενής αποθηκεύει το κλειδί με ασφάλεια. Προτείνεται επίσης η επιλεκτική κρυπτογράφηση των δεδομένων των ασθενών για να μειωθεί η υπολογιστική επιβάρυνση. Η κρυπτογράφηση εφαρμόζεται στη συνέχεια μόνο σε εκείνα τα στοιχεία που επιλέγονται από τον ασθενή.

- **Ορισμένα επιθυμητά χαρακτηριστικά για κατάλληλη διαχείριση κλειδιών :**

- ο αριθμός των κλειδιών που κατέχουν τόσο οι ασθενείς όσο και οι γιατροί δεν πρέπει να είναι μεγάλος.

- τα κλειδιά θα πρέπει να είναι εύκολα αποθηκευμένα και να καταναλώνουν χαμηλή πολυπλοκότητα χώρου.
- η επικαιροποίηση των κλειδιών θα πρέπει να είναι βολική και αποδοτική όσον αφορά την πολυπλοκότητα του χρόνου.
- κανένα από τα κλειδιά δεν πρέπει να περιέχει οποιαδήποτε προσωπική πληροφορία των μερών.
- όλα τα κλειδιά θα πρέπει να εντοπιστούν και να ανακληθούν όταν λήξουν ή όταν ο χρήστης εγκαταλείψει την ομάδα.

Όταν ο όγκος δεδομένων είναι μεγάλος όπως π.χ εικόνα δεδομένων, η ασύμμετρη κρυπτογραφία μπορεί να είναι αναποτελεσματική. Αυτό το πρόβλημα μπορεί να είναι ιδιαίτερα σοβαρό εάν οι ιατρικές εγγραφές με δεδομένα απεικόνισης έχουν πρόσβαση μέσω μιας υπολογιστικής συσκευής χαμηλής απόδοσης, όπως π.χ ένας φορητός ψηφιακός βοηθός (PDA) . Επομένως, συνιστάται μια συμμετρική μέθοδος κρυπτογράφησης για λόγους αποτελεσματικότητας όπου είναι μια υβριδική λύση Υποδομής Δημόσιου Κλειδιού .

Δημόσιο κλειδί:

Γενικά τα δεδομένα κρυπτογραφούνται στους διακομιστές και ο ίδιος ο πάροχος αποθηκεύει τα κλειδιά κρυπτογράφησης.

Οι λειτουργίες δημόσιου κλειδιού είναι βραδύτερες από τα συμμετρικά πρωτεύοντα κλειδιά και όταν απαιτούνται δυνατότητα αναζήτησης ή κρυφές ετικέτες φαίνεται ότι έχουν εγγενείς αδυναμίες στην ιδιωτική ζωή . Από την άλλη πλευρά, εάν ο ίδιος ο διακομιστής διατηρεί το ιδιωτικό κλειδί, τότε τα βασικά συμμετρικά σχήματα είναι επίσης ευάλωτα, καθώς το κλειδί μπορεί να κλαπεί μαζί με τα κρυπτογραφημένα δεδομένα. Τα κλειδιά κρυπτογράφησης μπορούν επίσης να φιλοξενούνται σε ένα ξεχωριστό φυσικό διακομιστή για να αποφευχθεί η αποκρυπτογράφηση των δεδομένων ασθενούς, εάν η μηχανή αποθήκευσης δεδομένων υποπέσει σε κίνδυνο.

Η Υποδομή Δημόσιου Κλειδιού (PKI) αναφέρεται σε ένα σύνολο ισχυρών υπηρεσιών ασφάλειας, οι οποίες στηρίζονται σε θεμελιώδεις μηχανισμούς κρυπτογραφίας. Αυτοί οι μηχανισμοί του δημόσιου κλειδιού είναι ο έλεγχος αυθεντικότητας, ακεραιότητας και η διατήρηση της εμπιστευτικότητας, μέσω της χρήσης ψηφιακών υπογραφών, ψηφιακών πιστοποιητικών, συμμετρικής και ασύμμετρης κρυπτογράφησης. Χάρη σε αυτούς τους μηχανισμούς, μπορούν να επιτευχθούν οι βασικοί στόχοι ασφάλειας των πληροφοριακών συστημάτων, που είναι η εγγύηση της αυθεντικότητας, διαφύλαξη της ακεραιότητας και η τήρηση της εμπιστευτικότητας. Είναι απαραίτητη για να δημιουργήσει ένα αξιόπιστο περιβάλλον για ασφαλείς συναλλαγές και επικοινωνίες τόσο για άτομα όσο και για οργανισμούς. Καθώς όλο και περισσότεροι οργανισμοί παγκοσμίως αρχίζουν να επενδύουν σε αυτό, η ανάγκη για ταυτοποίηση και πιστοποίηση στις ηλεκτρονικές συναλλαγές έχει γίνει πολύ σημαντική.

Οι Αρχές Πιστοποίησης ελέγχουν την υποδομή ασφάλειας που χρησιμοποιεί η Ασύμμετρη Κρυπτογραφία. Σε ένα δίκτυο με υποδομή Δημοσίου Κλειδιού υπάρχουν σχέσεις εμπιστοσύνης. Οι εγγραφόμενοι δημιουργούν σχέση εμπιστοσύνης με την Αρχή Πιστοποίησης CA. Οι CAs με τη σειρά τους δημιουργούν σχέση εμπιστοσύνης με άλλες Αρχές Πιστοποίησης για να κάνουν δυνατή την ασφαλή επικοινωνία μεταξύ διαφορετικών περιοχών στα πλαίσια του PKI. Όταν η συναλλαγή γίνεται μεταξύ δύο πλευρών που είναι άγνωστες μεταξύ τους, ένα πιστοποιητικό υπογεγραμμένο και επιβεβαιωμένο είναι αρκετό για να δημιουργηθεί σχέση εμπιστοσύνης μεταξύ των δύο αυτών πλευρών.

Οι υπηρεσίες πιστοποίησης που απαιτούνται για την πιστοποίηση ιατρικού προσωπικού σε ένα δίκτυο υγειονομικής περίθαλψης βασίζονται στην Υποδομή Δημόσιου Κλειδιού.

Ένα τέτοιο δίκτυο αποτελείται :

- Αρχές Πιστοποίησης (CAs), οι οποίες ελέγχουν και διαχειρίζονται την Υποδομή Δημοσίου Κλειδιού, εκδίδουν πιστοποιητικά ιατρικού προσωπικού, και επιβάλλουν πολιτικές στην περιοχή τους. Το σύστημα ασφαλείας του δικτύου υγείας μπορεί ανάλογα με την πολιτική πιστοποίησης να έχει μια ή

περισσότερες Αρχές Πιστοποίησης.

- Αρχές εγγραφής (RAs), που ενεργούν εκ μέρους των Αρχών Πιστοποίησης (CAs) για να δηλώνουν τους επαγγελματίες υγείας στην περιοχή του δικτύου που διαχειρίζεται η Αρχή Πιστοποίησης.
- Συστήματα διαχείρισης πιστοποιητικών (Certificate management systems/CMS) για τη διαχείριση των πιστοποιητικών των επαγγελματιών υγείας καθ' όλη τη διάρκεια που είναι σε ισχύ. Οι Αρχές Πιστοποίησης χρησιμοποιούν και ελέγχουν τα συστήματα διαχείρισης πιστοποιητικών (CMS).
- Καταλόγους X.500 (directories), όπου αποθηκεύονται τα πιστοποιητικά των επαγγελματιών υγείας όπως επίσης και δημόσια πληροφορία για τους κατόχους των πιστοποιητικών και χρησιμοποιούνται κατά την επαλήθευση των ψηφιακών πιστοποιητικών.

Ανάλογα με την πολιτική της, η Αρχή Πιστοποίησης του ιατρικού δικτύου μπορεί να επιτρέπει τη χρήση του ίδιου κλειδιού σε εφαρμογές διαφορετικού τύπου, ή να χρησιμοποιούνται διαφορετικά κλειδιά σε διαφορετικές εφαρμογές. Συνίσταται η χρησιμοποίηση διαφορετικών κλειδιών για λόγους μεγαλύτερης ασφάλειας. Σε αυτήν την περίπτωση η Αρχή Πιστοποίησης πρέπει να εκδίδει ένα ξεχωριστό πιστοποιητικό, που να είναι ανάλογο με τους σκοπούς χρήσης του κάθε δημόσιου κλειδιού του επαγγελματία υγείας. Ακριβώς το τι δεδομένα χρειάζονται για να φτιαχτεί ένα πιστοποιητικό, εξαρτάται από τη χρήση του δημόσιου κλειδιού που πιστοποιεί.

4.8 Παρακολούθηση της πρόσβασης στο σύστημα

Προκειμένου να διασφαλιστεί η αξιοπιστία και η αυθεντικότητα των δεδομένων, το υγειονομικό προσωπικό που δημιουργεί ή επικαιροποιεί την ηλεκτρονική καταγραφή πρέπει να το υπογράψει ψηφιακά.

Κάθε πρόσβαση στην πλατφόρμα θα πρέπει να παρακολουθείται για να δημιουργηθεί ένα ημερολόγιο όλων των ανθρώπων που είχαν πρόσβαση στο

σύστημα. Σε περίπτωση συμβάντος, μπορείτε να συμβουλευτείτε το ημερολόγιο για να λύσετε ή να μάθετε την αιτία του προβλήματος. Θα ήταν πολύτιμη η δημιουργία ενός αρχείου καταγραφής για την παρακολούθηση κάθε ενημέρωσης και την αλλαγή σε κάθε ιατρικό αρχείο.

4.9 Προτάσεις πριν γίνει μετακίνηση ηλεκτρονικών αρχείων υγείας στο Cloud

Οι κύριες ανησυχίες των παρόχων υγειονομικής περίθαλψης που σχεδιάζουν να μεταφέρουν πληροφορίες ασθενούς στο Cloud είναι η ασφάλεια των δεδομένων και η ιδιωτικότητα. Η μετεγκατάσταση δεδομένων στο Cloud σημαίνει ότι ένα τρίτο μέρος έχει πλέον τον έλεγχο των δεδομένων που φιλοξενούνται από το Cloud. Προκειμένου να αντιμετωπιστούν οι κίνδυνοι που θα μπορούσαν να προκύψουν, οι πελάτες Cloud θα πρέπει να είναι καλά ενημερωμένοι πριν από τη μεταφορά δεδομένων στο Cloud. Προκειμένου να διευκολυνθεί αυτή η διαδικασία, οι ίδιοι οι πελάτες του παρόχου υπηρεσιών Cloud θα πρέπει να ενημερώνονται για τις υπηρεσίες που προσφέρει ο πάροχος Cloud και για τους μηχανισμούς ασφαλείας που είναι εγκατεστημένοι στους διακομιστές του παροχέα. Οι πελάτες Cloud πρέπει να απαιτούν πλήρη διαφάνεια από τον παροχέα υπηρεσιών Cloud. Η γνώση αυτού του είδους των πληροφοριών είναι κρίσιμη για να είναι σε θέση να επιλέξει τον καταλληλότερο πάροχο για τις ανάγκες του πελάτη.

4.10 Διάφορα ζητήματα ασφάλειας που πρέπει να λαμβάνει υπόψη ο πελάτης κατά την επιλογή του καταλληλότερου παροχέα

- **Ασφάλεια δεδομένων:** Επειδή ένας πάροχος Cloud θα έχει πρόσβαση σε όλες τις πληροφορίες σχετικά με τους ασθενείς, τα σχέδια έργων κ.λπ., είναι απαραίτητο να ελέγξει τη φήμη του παρόχου στην αγορά. Ο πάροχος πρέπει να εγγυηθεί ότι οι πληροφορίες των πελατών του δεν θα καταστρατηγηθούν από κανένα μη εξουσιοδοτημένο προσωπικό. Ο πάροχος υγειονομικής περίθαλψης πρέπει να ελέγξει για τις υπηρεσίες προστασίας δεδομένων και λειτουργικής ακεραιότητας που προσφέρει ο πάροχος. Επιπλέον, είναι πολύτιμο να γνωρίζουμε τη γεωγραφική θέση των διακομιστών όπου θα φιλοξενούνταν τα δεδομένα του πελάτη. Εν συντομία, οι πελάτες πρέπει να απαιτούν πλήρη διαφάνεια.

- **Κανονιστική Συμμόρφωση:** Είναι σημαντικό να επιλέξετε παρόχους με πιστοποιήσεις ασφαλείας και να είστε έτοιμοι για εξωτερικούς ελέγχους. Είναι σημαντικό ο πάροχος να εγγυάται τη συνέχεια της υπηρεσίας σε περίπτωση που ο πάροχος έχει κάποιο πρόβλημα. Ο πελάτης πρέπει να διασφαλίσει ότι ο παροχέας λειτουργεί στη χώρα όπου θα προσφέρεται η υπηρεσία.Η καταγραφή δεδομένων και η παρακολούθηση δεδομένων αποτελούν σημαντικά εργαλεία που πρέπει να προσφέρουν οι παροχείς υπηρεσιών Cloud προκειμένου να βελτιωθεί η ασφάλεια της υπηρεσίας.

- **Έλεγχος ταυτότητας χρήστη:** Επειδή τα δεδομένα επεξεργάζονται εξωτερικά από τρίτους, υπάρχει πάντα κάποιος εγγενής κίνδυνος. Ο πελάτης πρέπει να γνωρίζει το προσωπικό που θα διαχειρίζεται τις ιατρικές πληροφορίες και ποια πρότυπα

πρόσβασης θα ακολουθήσει ο πάροχος. Ο πελάτης πρέπει να ενημερώνεται για τα συστήματα πρόσβασης που βασίζονται σε ρόλους καθώς και για το σύστημα χειρισμού κωδικών που έχει διαμορφωθεί από τον πάροχο.

- **Διαχωρισμός δεδομένων:** Ο πάροχος όχι μόνο χειρίζεται τα δεδομένα που αποθηκεύονται στο Cloud αλλά διαχειρίζεται τα δεδομένα άλλων εταιρειών που έχουν προσλάβει τις υπηρεσίες του.Επομένως, είναι σημαντικό να γνωρίζουμε τους μηχανισμούς που εφαρμόζει ο πάροχος του Cloud για να διαχωρίσει τα δεδομένα όλων των εταιρειών που μοιράζονται τους ίδιους διακομιστές. Οι πελάτες πρέπει να ενημερώνονται για τη διαθεσιμότητα των δεδομένων που εγγυάται ο πάροχος.

- **Νομικά ζητήματα:** Ένα νομικό πλαίσιο πρέπει να καθοδηγεί τις πολιτικές του παρόχου Cloud. Οι συμφωνίες δικαιωμάτων πνευματικής ιδιοκτησίας μεταξύ των δύο μερών πρέπει να είναι πρωταρχικής σημασίας. Ενώ ο παροχέας έχει το δικαίωμα στην υποδομή και τις εφαρμογές του, ο πελάτης έχει το δικαίωμα στα δεδομένα του και στα υπολογιστικά του αποτελέσματα.

4.11 Μετακίνηση Ηλεκτρονικών Αρχείων Υγείας στο Σύννεφο: Παράδειγμα Απαιτήσεων Ασφαλείας της Εταιρείας Cloud

Οι πάροχοι υγειονομικής περίθαλψης που αποφασίζουν να μετακινήσουν τους HER (Ηλεκτρονικών αρχείων υγείας) τους στο Cloud θα πρέπει να γνωρίζουν αυτά τα είδη μηχανισμών ασφαλείας πριν μεταναστεύσουν τα αρχεία τους. Υπάρχουν αρκετές γνωστές εταιρείες παροχής υπηρεσιών Cloud, για παράδειγμα, οι υπηρεσίες Amazon Web Services, το Microsoft Cloud, το GoGrid ή το Salesforce, με παρόμοιους όρους ασφάλειας όπως εξηγείται παρακάτω.

- **Πιστοποίηση τρίτου μέρους**

Προκειμένου να διασφαλιστεί η ασφάλεια των δεδομένων και να τηρηθούν οι απαιτήσεις των πολιτικών απορρήτου, ο πάροχος Cloud πρέπει να συμμορφώνεται με διάφορες πιστοποιήσεις και απαιτήσεις τρίτων.

- **SAS70 τύπου II** Δήλωση σχετικά με τα ελεγκτικά πρότυπα αριθ. 70: Δήλωση ελέγχου που παρέχει καθοδήγηση στους ελεγκτές υπηρεσιών κατά την αξιολόγηση του εσωτερικού ελέγχου ενός φορέα παροχής υπηρεσιών και την έκδοση έκθεσης ελεγκτή υπηρεσίας.

- **Επίπεδο 1 PCI DSS** Ο πάροχος Cloud θα πρέπει να πιστοποιηθεί με το πρότυπο PCI Data Security ως κοινόχρηστος φορέας παροχής υπηρεσιών φιλοξενίας.

- **ISO 27001** Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που καλύπτει την υποδομή, τα κέντρα δεδομένων και τους όρους παροχής υπηρεσιών.

- **FISMA** Πιστοποίηση για τη λειτουργία του νόμου για την ομοσπονδιακή διαχείριση της ασφάλειας πληροφοριών (FISMA) Low Level, ο οποίος είναι ομοσπονδιακός νόμος των ΗΠΑ που θεσπίστηκε το 2002. Αναγνωρίζει τη σημασία της ασφάλειας των πληροφοριών στην οικονομία και τα συμφέροντα της εθνικής ασφάλειας των Ηνωμένων Πολιτειών.

➢ Παρακολούθηση

Ο πάροχος θα πρέπει να περιλαμβάνει αυτοματοποιημένα εργαλεία παρακολούθησης για την παροχή υψηλού επιπέδου υπηρεσιών και διαθεσιμότητας του συστήματος. Αυτά τα εργαλεία πρέπει να είναι διαθέσιμα στο διαδίκτυο για εσωτερική και εξωτερική χρήση. Οι συναγερμοί ειδοποίησης μπορούν να διαμορφωθούν όταν οποιαδήποτε τροποποίηση των δεδομένων γίνεται από το προσωπικό συντήρησης ή από τους ίδιους τους χρήστες. Αυτά τα εργαλεία θα βοηθήσουν στην παρακολούθηση όλων των αλλαγών πληροφοριών που έγιναν στα αποθηκευμένα δεδομένα cloud. Οποιοδήποτε περιστατικό με τα αποθηκευμένα δεδομένα θα παρακολουθείται.

➢ Πληροφορία και επικοινωνία

Για να χρησιμοποιήσει την πλατφόρμα Cloud ως κανάλι επικοινωνίας όπου το προσωπικό μπορεί να ενημερωθεί για όλα όσα συμβαίνουν, ο πάροχος Cloud θα πρέπει να χρησιμοποιήσει διάφορες μεθόδους εσωτερικής επικοινωνίας για να

βοηθήσει τους υπαλλήλους να κατανοήσουν τους ρόλους και τις ευθύνες τους, επικοινωνούν σημαντικά γεγονότα, εάν είναι απαραίτητο. Αυτές οι μέθοδοι επικοινωνίας θα μπορούσαν να περιλαμβάνουν προγράμματα προσανατολισμού και κατάρτισης για νεοπροσλαμβανόμενο προσωπικό, τηλεδιάσκεψη και ηλεκτρονικό ταχυδρομείο, μεταξύ άλλων.

- **Κύκλος ζωής υπαλλήλου μια πλατφόρμας παροχής cloud**

Στην πλατφόρμα Cloud δημιουργούνται πολλές πολιτικές για τη διαχείριση της πρόσβασης των χρηστών. Ο πάροχος υπηρεσιών Cloud θα πρέπει να απαιτεί από το προσωπικό με πιθανή πρόσβαση στα δεδομένα ασθενούς να υπόκειται σε εκτεταμένο έλεγχο ιστορικού (όπως επιτρέπεται από το νόμο) ανάλογα με τη θέση και το επίπεδο πρόσβασης στα δεδομένα.

- **Πολιτικές κύκλου ζωής του υπαλλήλου μιας πλατφόρμας παροχής Cloud**:

- **Προβλέψεις λογαριασμών** Ο ίδιος ο πάροχος του Cloud αναλαμβάνει την ευθύνη της πρόβλεψης της πρόσβασης των εργαζομένων και των εργολάβων. Αυτή η πρόσβαση στους πόρους που φιλοξενούνται στην πλατφόρμα Cloud πρέπει να εγκριθεί ρητά από τον ιδιοκτήτη ή το διαχειριστή δεδομένων.

- **Αναθεώρηση λογαριασμού** Κάθε λογαριασμός πρόσβασης εξετάζεται σε πλατφόρμες Cloud κάθε 90 ημέρες.

- **Αφαίρεση πρόσβασης** Ο λογαριασμός πρόσβασης κάθε υπαλλήλου ανακαλείται αυτόματα όταν ολοκληρωθεί.

- **Πολιτική κωδικού πρόσβασης** Η πρόσβαση στην πλατφόρμα πραγματοποιείται από τα αναγνωριστικά χρήστη και τους κωδικούς πρόσβασης για την εξακρίβωση της ταυτότητας των χρηστών σε υπηρεσίες, πόρους και συσκευές, καθώς και για την έγκριση του κατάλληλου επιπέδου πρόσβασης σε κάθε χρήστη.

- **Ασφάλεια από εξειδικευμένο προσωπικό**

Το κτίριο του κέντρου δεδομένων θα πρέπει να ελέγχεται αυστηρά και να εξασφαλίζεται με βιντεοεπιτήρηση, εξειδικευμένο προσωπικό ασφαλείας, συστήματα ανίχνευσης εισβολών και άλλα ηλεκτρονικά μέσα. Το εξουσιοδοτημένο προσωπικό θα πρέπει να περάσει από τα στοιχεία ελέγχου ταυτότητας για πρόσβαση στα δάπεδα του κέντρου δεδομένων.

- **Περιβαλλοντικές διασφαλίσεις**

Πρέπει να χρησιμοποιηθούν καινοτόμες αρχιτεκτονικές και μηχανικές προσεγγίσεις στα κέντρα βάσης δεδομένων, ώστε να αποφευχθούν εξωτερικοί παράγοντες που θα μπορούσαν να τους προκαλέσουν βλάβη .

- **Περιβαλλοντικές διασφαλίσεις εγκατεστημένες σε κέντρα δεδομένων:**

Ανίχνευση και κατάσβεση πυρκαγιάς Τα αυτόματα συστήματα ανίχνευσης και καταστολής πυρκαγιάς εγκαθίστανται στους χώρους των κέντρων δεδομένων για την εξάλειψη του κινδύνου πυρκαγιάς.

Εξουσία	24/7 συστήματα ηλεκτρικής ενέργειας που εγγυώνται την αδιάλειπτη λειτουργία της υπηρεσίας.
Κλίμα και θερμοκρασία	Προκειμένου να αποφευχθεί η υπερθέρμανση των διακομιστών, απαιτείται κλιματισμός. Αυτό αποτελεί κρίσιμη μέριμνα για τη διαχείριση του κέντρου δεδομένων και καταναλώνει πολλή ενέργεια.
Διαχείριση	Συστήματα παρακολούθησης για τον έλεγχο της κατάστασης του εξοπλισμού βάσης δεδομένων.

- **Διαχείριση Διαμόρφωσης**

Η εταιρεία θα πρέπει να γνωστοποιεί όλες τις ενημερώσεις τόσο στην υποδομή όσο και στο ίδιο το λογισμικό, ώστε να ελαχιστοποιείται ο αντίκτυπος στον πελάτη και την υπηρεσία. Η διαδικασία ενημέρωσης του λογισμικού θα πρέπει να σχεδιάζεται έτσι ώστε να αποφεύγεται η ακούσια διακοπή των υπηρεσιών και να διατηρείται η ακεραιότητα των υπηρεσιών προς τον πελάτη. Πριν από την ενημέρωση του λογισμικού, αυτές οι ενημερώσεις πρέπει να αναθεωρηθούν, να πειραματιστούν και να εγκριθούν. Το προσωπικό του φορέα Cloud θα διαχειρίζεται την υποδομή του κέντρου δεδομένων και θα είναι υπεύθυνο για τη διαχείριση φιλοξενίας, την επεκτασιμότητα του συστήματος, τη διαθεσιμότητα και τον έλεγχο και τη διαχείριση της ασφάλειας.

- **Διαχείριση επιχειρηματικής συνέχειας**

Ο πάροχος υπηρεσιών Cloud πρέπει να εγγυηθεί τη διαθεσιμότητα της προσφερόμενης υπηρεσίας. Προκειμένου να διασφαλιστεί η διαθεσιμότητα και η

συνέχεια του συστήματος, η εταιρεία θα πρέπει να αντιμετωπίσει τα ζητήματα ασφάλειας:

- **Διαθεσιμότητα** Τα κέντρα δεδομένων είναι χτισμένα σε ομάδες ανά περιφέρεια. Σε περίπτωση αποτυχίας ενός από αυτά τα κέντρα δεδομένων, οι αυτοματοποιημένες διεργασίες μετακινούν την επισκεψιμότητα δεδομένων πελατών μακριά από την πληγείσα περιοχή.

- **Απόκριση σε περίπτωση συμβάντος** Πρέπει να προσφέρεται τεχνική υποστήριξη και κάλυψη για την επίλυση κάθε είδους προβλήματος 24/7/365 (24 ώρες την ημέρα, 7 ημέρες την εβδομάδα και 365 ημέρες το χρόνο).

- **Εταιρική αναθεώρηση εκτελεστικής εξουσίας** Μια εταιρεία Cloud πρέπει να ελέγχεται περιοδικά και να υποστηρίζεται από μια ομάδα εσωτερικού ελέγχου.

➢ Δημιουργία αντιγράφων ασφαλείας

Προκειμένου να διασφαλιστεί η ύπαρξη δεδομένων ασθενούς που είναι αποθηκευμένα στο Cloud, ο πάροχος πρέπει να αποθηκεύσει περιττά τα δεδομένα αυτά. Τα πολλαπλά αντίγραφα αυτών των δεδομένων πρέπει να αποθηκεύονται σε διαφορετικά κέντρα δεδομένων σε διάφορες τοποθεσίες.

- **Αποθήκευση υπηρεσιών αποθήκευσης**

Όταν μια υπηρεσία αποθήκευσης Cloud έρχεται στο τέλος της ωφέλιμης ζωής της, ο πάροχος θα πρέπει να εγγυηθεί ότι τα δεδομένα που αποθηκεύονταν εκεί ήταν απομακρυσμένα από τους διακομιστές του. Επιπλέον, ο πάροχος πρέπει να διασφαλίσει ότι το μη εξουσιοδοτημένο προσωπικό δεν έχει αντιγράψει αυτά τα δεδομένα.

- **Ασφάλεια δικτύου**

Η ίδια η πλατφόρμα δεν είναι το μόνο στοιχείο που πρέπει να εξασφαλίζεται από τον πάροχο. Ο παροχέας του Cloud πρέπει επίσης να ασφαλίσει το δίκτυο. Ο πάροχος δικτύου πρέπει να εγγυάται σημαντική προστασία από τα παραδοσιακά ζητήματα ασφάλειας δικτύων.

- **Προστασία από θέματα ασφάλειας δικτύων:**

- **Επιθέσεις DDoS** Οι τεχνικές μετριασμού της Distributed Denial of Service (DDoS) περιλαμβάνονται στην πλατφόρμα Amazon Web Services (AWS) για να αποφευχθεί αυτό το είδος επίθεσης.

- **Οι επιθέσεις MITM** Οι επιθέσεις «άνθρωπος στη μέση» (MITM) αποφεύγονται επειδή όλα τα τελικά σημεία του AWS είναι ασφαλή από το «Ασφαλής στρώση υποδοχών» (SSL), το οποίο παρέχει έλεγχο ταυτότητας διακομιστή.

- **IP spoofing** Η πλατφόρμα κυκλοφορίας ελέγχεται από μια υποδομή τείχους προστασίας. Στη συνέχεια, τα αποθηκευμένα δεδομένα δεν μπορούν να στείλουν παραποιημένα

δεδομένα δικτύου.

- **Λιμάνι σάρωσης** Οι μη εξουσιοδοτημένες ανιχνεύσεις λιμένων από πελάτες αποτελούν παραβίαση της πολιτικής χρήσης του παροχέα. Κάθε παράβαση που αναφέρεται πρέπει να διερευνηθεί.

➢ Κύρια ευρήματα

Η μετεγκατάσταση ηλεκτρονικών φακέλων υγείας (EHR) στο Cloud μπορεί να αποτελέσει ένα μεγάλο βήμα στην ψηφιοποίηση των ιατρικών δεδομένων. Τα πλεονεκτήματα όπως η κλιμάκωση, το οικονομικό μοντέλο αμοιβής ανά χρήση και η συμμετοχή του ασθενούς ως ενεργού μέρους της διαδικασίας διαχείρισης της πληροφόρησης για την υγεία μπορούν να υποθέσουν μια αλλαγή μοντέλου στη διαχείριση των ιατρικών αρχείων. Πρέπει να ληφθούν υπόψη αρκετές απαιτήσεις όταν έρθει η ώρα για τη μετανάστευση ευαίσθητων και ιδιωτικών δεδομένων στο Cloud. Από αυτές τις απαιτήσεις, η ασφάλεια και η ιδιωτικότητα των δεδομένων είναι οι σημαντικότερες. Κατά την αποθήκευση των ευαίσθητων δεδομένων των αρχείων υγείας των ασθενών, οι πάροχοι υπηρεσιών Cloud και οι πάροχοι υπηρεσιών υγείας πρέπει να διασφαλίζουν την ιδιωτικότητα και την εμπιστευτικότητα των δεδομένων που φιλοξενούνται από το Cloud. Για να διευκολυνθεί αυτή η διαδικασία, οι πάροχοι υγειονομικής περίθαλψης, είτε ιδιωτικά είτε δημόσια κλινικά κέντρα, που αποφάσισαν να αναπτύξουν αυτό το είδος συστήματος, πρέπει να ενημερώσουν τους ασθενείς τους για την αλλαγή του τρόπου διαχείρισης και αποθήκευσης των δεδομένων τους. Επιπλέον, μια σχέση εμπιστοσύνης μεταξύ του παρόχου υγειονομικής περίθαλψης και του παρόχου υπηρεσιών Cloud αποτελεί βασικό παράγοντα αυτής της διαδικασίας. Προκειμένου να επιτευχθεί αυτή η εμπιστοσύνη, ο πάροχος Cloud πρέπει να εγγυηθεί ότι υπάρχουν μηχανισμοί ασφαλείας για την προστασία της ασφάλειας και της

ιδιωτικότητας των αποθηκευμένων δεδομένων. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. πρέπει να ενημερώνουν τους ασθενείς τους σχετικά με την αλλαγή του τρόπου διαχείρισης και αποθήκευσης των δεδομένων τους. Επιπλέον, μια σχέση εμπιστοσύνης μεταξύ του παρόχου υγειονομικής περίθαλψης και του παρόχου υπηρεσιών Cloud αποτελεί βασικό παράγοντα αυτής της διαδικασίας. Προκειμένου να επιτευχθεί αυτή η εμπιστοσύνη, ο πάροχος Cloud πρέπει να εγγυηθεί ότι υπάρχουν μηχανισμοί ασφαλείας για την προστασία της ασφάλειας και της ιδιωτικότητας των αποθηκευμένων δεδομένων. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. πρέπει να ενημερώνουν τους ασθενείς τους σχετικά με την αλλαγή του τρόπου διαχείρισης και αποθήκευσης των δεδομένων τους. Επιπλέον, μια σχέση εμπιστοσύνης μεταξύ του παρόχου υγειονομικής περίθαλψης και του παρόχου υπηρεσιών Cloud αποτελεί βασικό παράγοντα αυτής της διαδικασίας. Προκειμένου να επιτευχθεί αυτή η εμπιστοσύνη, ο πάροχος Cloud πρέπει να εγγυηθεί ότι υπάρχουν μηχανισμοί ασφαλείας για την προστασία της ασφάλειας και της ιδιωτικότητας των αποθηκευμένων δεδομένων. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. μια σχέση εμπιστοσύνης μεταξύ του παρόχου υγειονομικής περίθαλψης και του παρόχου υπηρεσιών Cloud αποτελεί βασικό παράγοντα αυτής της διαδικασίας. Προκειμένου να επιτευχθεί αυτή η εμπιστοσύνη, ο πάροχος Cloud πρέπει να εγγυηθεί ότι υπάρχουν μηχανισμοί ασφαλείας για την προστασία της

ασφάλειας και της ιδιωτικότητας των αποθηκευμένων δεδομένων. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. μια σχέση εμπιστοσύνης μεταξύ του παρόχου υγειονομικής περίθαλψης και του παρόχου υπηρεσιών Cloud αποτελεί βασικό παράγοντα αυτής της διαδικασίας. Προκειμένου να επιτευχθεί αυτή η εμπιστοσύνη, ο πάροχος Cloud πρέπει να εγγυηθεί ότι υπάρχουν μηχανισμοί ασφαλείας για την προστασία της ασφάλειας και της ιδιωτικότητας των αποθηκευμένων δεδομένων. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο. Απαιτείται εξωτερική εταιρεία για τον έλεγχο του παρόχου πλατφόρμας Cloud προκειμένου να επιδείξει διαφάνεια στη διαδικασία διαχείρισης πληροφοριών. Οι νομοθετικοί μηχανισμοί σχετικά με την ασφάλεια των δεδομένων μπορεί να είναι σημαντικοί. Η σύγκριση των όρων ασφάλειας πολλών εταιρειών υπολογιστικού νέφους θα είναι πολύτιμη για να επιλέξετε τον καταλληλότερο πάροχο.

5ο Κεφάλαιο: Μυστική κοινή χρήση δεδομένων υγείας

5.1 Μυστική κοινή χρήση δεδομένων υγείας σε πολλούς παρόχους υπηρεσιών σύννεφου

Η επιτάχυνση της υιοθέτησης του cloud computing μεταξύ των επιχειρήσεων οφείλεται στα πολλαπλά οφέλη που προσφέρει η τεχνολογία, ένα από τα οποία είναι η απλούστευση της ανταλλαγής πληροφοριών μεταξύ των οργανώσεων, η οποία είναι υψίστης σημασίας για την υγειονομική περίθαλψη. Ωστόσο, η μετακίνηση ευαίσθητων αρχείων υγείας στο νέφος εξακολουθεί να συνεπάγεται σοβαρούς κινδύνους για την ασφάλεια και την ιδιωτική ζωή.

Αυτή η αρχιτεκτονική διαθέτει μυστική κοινή χρήση ως σημαντικό μέτρο διανομής των αρχείων υγείας ως θραύσματα σε διαφορετικές υπηρεσίες σύννεφων, οι οποίες μπορούν να προσφέρουν υψηλότερο πλεονασμό ,πρόσθετη ασφάλεια και προστασία της ιδιωτικής ζωής σε περίπτωση συμβιβασμού κλειδιών, αλλοιωμένων κρυπτογραφημένων αλγορίθμων ή της ανασφαλούς εφαρμογής τους. Η σχετικά αυτή νέα τεχνολογία μπορεί να απλοποιήσει την ανταλλαγή πληροφοριών μεταξύ διαφορετικών επιχειρηματικών εταίρων, κάτι που έχει μεγάλη σημασία για την υγειονομική περίθαλψη. Στις μέρες μας η ανταλλαγή ιατρικών αρχείων μεταξύ των παρόχων υγειονομικής περίθαλψης μπορεί ακόμα να είναι πολύ συμβατική και πρακτική. Επίσης, τα φυσικά ιατρικά αρχεία που μοιράζονται μεταξύ των νοσοκομείων μπορεί να περιλαμβάνουν αναγνωριστικά στοιχεία ασθενών και εξαιρετικά ευαίσθητες πληροφορίες. Εάν μεταδίδονται κατά περιστασιακό τρόπο, μπορεί να παραβιαστεί η ιδιωτικότητα του ασθενούς.

Τα ηλεκτρονικά αρχεία υγείας σε ένα περιβάλλον υπολογιστικού νέφους προσελκύουν μεγάλη προσοχή τόσο από την ακαδημαϊκή κοινότητα όσο και από τους επαγγελματίες. Στη συνέχεια, ορίζουμε ένα ηλεκτρονικό αρχείο υγείας ως

υποσύνολο ηλεκτρονικού ιατρικού φακέλου που μοιράζεται στα ιατρικά κέντρα από τους ιατρούς. Η προσέγγιση του cloud computing δεν παρέχει απλώς επαρκείς δυνατότητες αποθήκευσης δεδομένων και διευκολύνει την αποθήκευση των δεδομένων υγείας σε ένα κεντρικό σημείο. Χαρακτηρίζεται επίσης ως ενίσχυση της μεταφοράς, διαθεσιμότητας και ανάκτησης των ιατρικών αρχείων, παρέχοντας μια εύκολη και πανταχού παρούσα πρόσβαση σε δεδομένα υγείας, βελτιώνοντας και ενισχύοντας τις ιατρικές υπηρεσίες, ανοίγοντας νέες ευκαιρίες επιχειρηματικών μοντέλων καθώς και αυξάνοντας την υιοθεσία από τους χρήστες. Τα γνωστά πλεονεκτήματα του cloud computing, όπως η μείωση του κόστους, η μέτρηση και η ευέλικτη χρήση των πόρων του, αναφέρονται επίσης συχνά σε σχέση με τα συστήματα καταγραφής της υγείας.

Το νέο υποσχόμενο πρότυπο του cloud computing αντιμετωπίζει επίσης πολλές προκλήσεις ασφάλειας και ιδιωτικότητας, οι οποίες εγείρουν μεγάλες ανησυχίες μεταξύ των ασθενών και των ιατρών, και ειδικότερα ο κίνδυνος να χάσουν τον έλεγχο των δεδομένων. Ωστόσο, λίγες από αυτές τις προσεγγίσεις μέχρι στιγμής λαμβάνουν υπόψη τον κίνδυνο συμβιβασμού. Εάν ένα ηλεκτρονικό αρχείο υγείας αποθηκεύεται σε κρυπτογραφημένη μορφή σε πάροχο σύννεφου, αλλά το κλειδί αποκρυπτογράφησης διακυβεύεται οποιαδήποτε στιγμή στο μέλλον, ο πάροχος θα μπορούσε να έχει πλήρη πρόσβαση στα ευαίσθητα δεδομένα ασθενούς. Οι λανθασμένοι αλγόριθμοι κρυπτογράφησης και οι επιρρεπείς σε λάθη υλοποιήσεις παρουσιάζουν παρόμοιους κινδύνους. Με βάση αυτές τις παρατηρήσεις, διερευνούμε τις απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής και τους αντίστοιχους μηχανισμούς.

5.1.1 Στόχοι στην ασφάλεια και την ιδιωτικότητα

Στόχος μας είναι να ικανοποιήσουμε με την αρχιτεκτονική μας τους κύριους στόχους ασφάλειας και προστασίας της ιδιωτικής ζωής, οι οποίοι προέρχονται από την μελέτη περίπτωσής μας :

Έλεγχος πρόσβασης για τη διατήρηση της εμπιστευτικότητας και την ακεραιότητα του περιεχομένου του ηλεκτρονικού αρχείου υγείας, εσωτερικά και για τη διοργάνωση συνεργατών.

- Εμπιστευτικότητα και ακεραιότητα του περιεχομένου των ηλεκτρονικών αρχείων έναντι εξωτερικών συμβαλλομένων, συμπεριλαμβανομένων των παρόχων cloud.
- Εμπιστευτικότητα της ύπαρξης ενός ηλεκτρονικού αρχείου για έναν συγκεκριμένο ασθενή.
- Η έλλειψη σχέσης μεταξύ των ηλεκτρονικών αρχείων υγείας και των ασθενών.
- Εμπιστευτικότητα των αναγνωριστικών ασθενούς και απουσία τους από τις τοποθεσίες ή τα δεδομένα υγείας. Συγκεκριμένα, θα πρέπει επίσης να ενισχύσουμε την εμπιστευτικότητα του ασθενούς όσον αφορά το ενδεχόμενο προφίλ των επισκέψεών του σε κέντρα υγείας. Για να επιτευχθεί αυτό, θα πρέπει να ελαχιστοποιηθεί η χρήση του PID και άλλων "εσωτερικών αναγνωριστικών" στην επικοινωνία με εξωτερικά μέρη, όπως οι πάροχοι συννέφου, π.χ. με τη μετατροπή τους σε "εξωτερικά αναγνωριστικά".
- Αυθεντικότητα των ηλεκτρονικών αρχείων υγείας κατά την αποθήκευση και μετάδοση.
- Διαθεσιμότητα και εξουσιοδότηση αρχειοθέτησης ηλεκτρονικών αρχείων υγείας από τους παρόχους σύννεφου.

- Αποδοτικότητα, δυνατότητα κλιμάκωσης και χρηστικότητα.

Εκτός από αυτήν την άποψη περισσότερο με βάση τα δεδομένα, την κλασική ασφάλεια, τα μέτρα δικτύου που περιγράφονται πρέπει να προστατεύουν όλες τις επικοινωνίες.

5.2 Μυστική κοινή χρήση των δεδομένων Υγείας του Internet of Things(IoT)

Παρόλο που το IoT χρησιμοποιείται ευρέως σε πολλά θέματα, το σύστημα υγειονομικής περίθαλψης κερδίζει περισσότερη προσοχή επειδή αφορά τη ζωή των ανθρώπων. Στον κλάδο της υγειονομικής περίθαλψης, το IoT αυξάνει την αποτελεσματικότητα, μειώνει το κόστος και επικεντρώνεται στην καλύτερη φροντίδα των ασθενών. Εάν η πρόθεση είναι να υπάρχει ως επίκεντρο η υγειονομική περίθαλψη των ασθενών, το IoT βοηθά να παρακολουθείται ο ασθενής συνεχώς τόσο στο περιβάλλον του νοσοκομείου όσο και από απόσταση.

Συγκεκριμένα, τα δεδομένα που συγκεντρώνονται και αναλύονται από το έξυπνο σύστημα έχουν σκοπό να οδηγήσουν στην αποτελεσματικότητα, στη διατήρηση της συμμόρφωσης, και να βοηθήσουν τους ανθρώπους της υγειονομικής περίθαλψης για την προώθηση της έρευνας, της διαχείρισης και φροντίδας. Η αυθεντικοποίηση των συσκευών IoT είναι πολύ αποτελεσματική καθώς υπάρχουν πολλές συσκευές που αναπτύσσονται για τη συσσώρευση των δεδομένων υγειονομικής περίθαλψης ενός ασθενούς.

5.2.1 Αρχιτεκτονική υγειονομικής υποστήριξης βάση το IoT

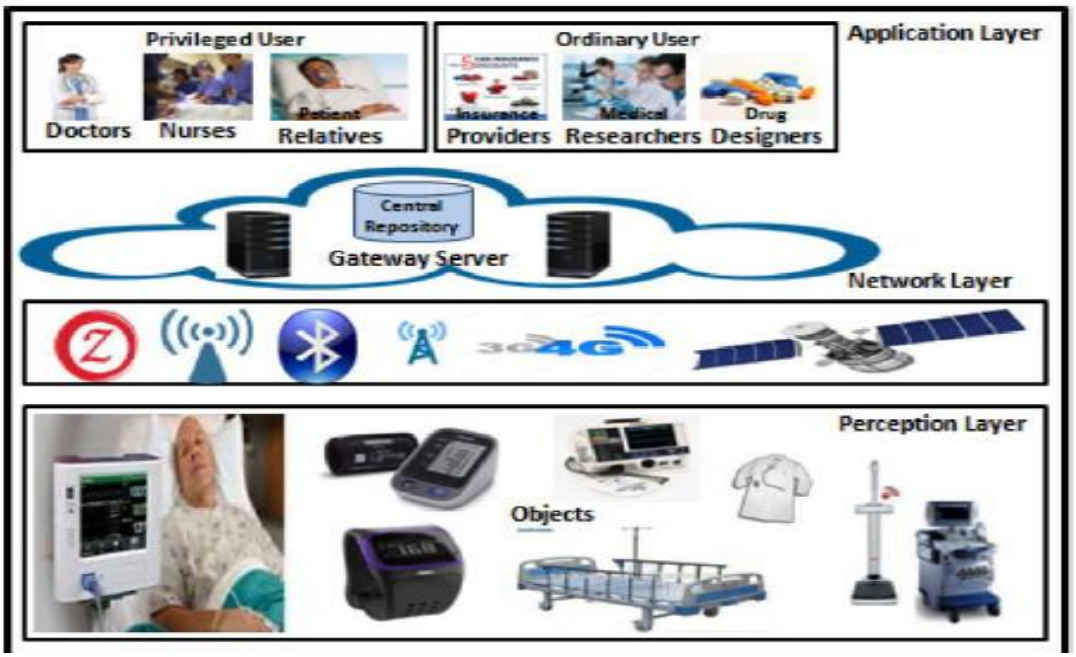
Πρόκειται για έναν αρχιτεκτονικό σχεδιασμό με βάση τα στρώματα που παρουσιάζονται στην εικόνα 33 και κάθε στρώμα έχει διαφορετικές τεχνολογίες αλληλεπίδρασης, πρωτόκολλα, σκοπούς και λειτουργίες.

1 Επίπεδο αντιλήψεων

Οι συσκευές που έχουν αναπτυχθεί σε ένα δωμάτιο του συστήματος υγειονομικής περίθαλψης, έχουν την αίσθηση του φυσικού περιβάλλοντος και συλλέγουν δεδομένα σε πραγματικό χρόνο. Οι ετικέτες RFID, οι αισθητήρες και το IPV6 χρησιμοποιούνται για την αναγνώριση των ιατρικών συσκευών. Οι τεχνολογίες ZigBee, Bluetooth και 3G / 4G χρησιμοποιούνται για επικοινωνία.

2 Επίπεδο δικτύου

Αυτό το στρώμα χειρίζεται την επικοινωνία των δεδομένων που συλλέγονται στο Cloud Central Servers (CCS), Gateway Servers (GS) και διαφορετικές εφαρμογές. Ενσύρματα ή ασύρματα χρησιμοποιούνται για πρόσβαση στο δίκτυο μέσω πύλης και η διευθυνσιοδότηση και η δρομολόγηση των πακέτων δεδομένων αντιμετωπίζονται από τα πρωτόκολλα δρομολόγησης, όπως το Low-energy adaptive clustering hierarchy (LEACH) και το Routing Protocol for Low-Power and Lossy Networks (RPL).



Εικόνα 34 Αρχιτεκτονική σε ένα έξυπνο σύστημα υγειονομικής περίθαλψης

3 Επίπεδο εφαρμογής

Οι πληροφορίες που διαβιβάζονται στη βάση δεδομένων είναι διαθέσιμες και δημοσιεύονται. Επιπλέον, η συλλογή και το φιλτράρισμα των δεδομένων, η ανάλυση δεδομένων και η επικοινωνία των πληροφοριών που προκύπτουν από την εφαρμογή γίνονται σε αυτό το στρώμα.

5.2.2 Ροή εργασιών υγειονομικής περίθαλψης

Κάθε συσκευή στο προτεινόμενο σύστημα θεωρείται ως μεμονωμένος κόμβος που συνδέονται μεταξύ τους με άμεσο Ethernet ή Wi-Fi, Near Field Communication, Bluetooth, ZigBee ή άλλες τεχνολογίες. Οι ιατρικοί σύμβουλοι, οι ιατροί μπορούν να επιλέξουν ιατρείο για ιατρική περίθαλψη. Ο επισκέπτης μπορεί να κάνει κράτηση για την παραμονή του στο νοσοκομείο. Η πληροφόρηση σχετικά με τη φυσική κατάσταση του ασθενούς είναι αποδεδειγμένη από τη στιγμή που τα στοιχεία αυτά είναι γνωστά.

Είδη συσκευών:

- Συσκευή χρήστη (UD) και
- Ιατρικές συσκευές (MD)

Η συσκευή χρήστη (UD) μπορεί να είναι ένα desktop, laptop, tablet ή κινητό τηλέφωνο χρησιμοποιώντας το οποίο οι χρήστες έχουν πρόσβαση στην ιατρική ενημέρωση του ασθενή από τα ιατρικά βοηθήματα (MD) στο δωμάτιο των ασθενών που καταγράφουν διάφορες παραμέτρους της υγείας του ασθενούς. Όταν ένας χρήστης επιθυμεί να έχει πρόσβαση στις πληροφορίες που καταγράφονται από οποιαδήποτε από τις ιατρικής συσκευής, ο χρήστης πρέπει να υποβληθεί σε διαδικασία ελέγχου ταυτότητας. Οι συνεχείς ιατρικές πληροφορίες και δεδομένα ροής των ασθενών αποθηκεύονται στο Cloud Central Repository (CCR) και τα μεταδεδομένα τους όπως οι λεπτομέρειες CCR αποθηκεύονται στον Gateway Server (GS). Ο διακομιστής Gateway Server είναι συνδεδεμένος με το σύστημα εντολών και

αποστέλλεται μέσω του διακομιστή Gateway Server. Γίνεται παρακολούθηση δεδομένων streaming από όλες τις εγκατεστημένες μονάδες και το κεντρικό αποθετήριο Cloud (CCR) για μελλοντική αναφορά. Τα στοιχεία ελέγχου ταυτότητας διατηρούνται επίσης σε αυτό το Cloud Central Repository (CCR).

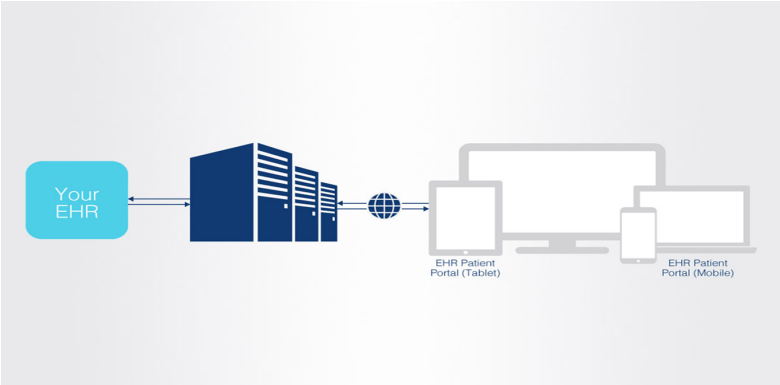
5.3 Ηλεκτρονικά αρχεία υγείας: Πώς μοιράζονται τα συστήματα

Πολλά ηλεκτρονικά συστήματα αρχείων καταγραφής υγείας είναι χτισμένα έτσι ώστε να μην μπορούν να μοιράζονται πληροφορίες μεταξύ τους. Αντίθετα, αυτά τα ηλεκτρονικά αρχεία, ως κεντρικά αποθετήρια πληροφοριών ασθενών, πρέπει να είναι σε θέση να αποστέλλουν δεδομένα σε άλλα την τεχνολογία πληροφοριών για την υγεία και να λαμβάνει δεδομένα από άλλα I.T για την υγεία, συμπεριλαμβανομένων των εργαστηρίων, των φαρμακείων, των συστημάτων τιμολόγησης και άλλων ηλεκτρονικών αρχείων υγείας.

Το ομοσπονδιακό πρόγραμμα παροχής κινήτρων στους παρόχους για να αποκτήσουν και να χρησιμοποιήσουν ουσιαστικά τα ομοσπονδιακά πιστοποιημένα ηλεκτρονικά αρχεία υγείας έχει ωθήσει σε μεγάλο βαθμό την υιοθεσία. Η πιστοποίηση απαιτεί από τα συστήματα να διαθέτουν θεμελιώδες δυνατότητες ανταλλαγής δεδομένων - διαλειτουργικότητα - χρησιμοποιώντας εθνικά πρότυπα, με περισσότερα από 500 ηλεκτρονικά συστήματα αρχείων καταγραφής υγείας να πιστοποιούνται τώρα για αυτές τις δυνατότητες.

Επίσης τα συμπεράσματα των εμπειρογνωμόνων σχετικά με την πολιτική ότι τα κρίσιμα εμπόδια στη διαλειτουργικότητα δεν είναι τεχνικά, αυτά τα εμπόδια περιλαμβάνουν την έλλειψη ισχυρής επιχειρησιακής περίπτωσης για τους παρόχους να μοιράζονται πληροφορίες, διακυμάνσεις στον κρατικό νόμο και έλλειψη υποδομής για τη σύνδεση ηλεκτρονικών αρχείων υγείας και άλλων τεχνολογιών πληροφοριών για την υγεία.

5.4 Προκλήσεις διαλειτουργικότητας των EHR(ηλεκτρονικών αρχείων υγείας)που πρέπει να επικεντρωθούν στις εταιρίες πληροφορικής:



Τα EHRs δεν είναι απλώς ψηφιακές εκδόσεις των φακέλων υγείας. Παρόλο που τα συστήματα αυτά παρέχουν πολλαπλά οφέλη - όπως βελτιωμένα δεδομένα για τους ασθενείς και αυξημένη παραγωγικότητα στην υγειονομική περίθαλψη - εξακολουθούν να υπάρχουν εγγενείς προκλήσεις όσον αφορά τη διαλειτουργικότητα. Δεν είναι μυστικό ότι τα δεδομένα περί υγειονομικής περίθαλψης στα περισσότερα EHRs παρέμειναν πλεγμένα και δεν ενσωματώθηκαν. Το καθαρό αποτέλεσμα της μη ολοκλήρωσης είναι η μείωση της αποτελεσματικότητας, το υψηλότερο κόστος και τα αρνητικά αποτελέσματα. Λόγω της κακής εκτέλεσης της ενσωμάτωσης της ηλεκτρονικής μάθησης, πολλές εταιρείες υγείας εξακολουθούν να υφίστανται τεράστιες απώλειες. Παρακάτω εξετάζουμε τις κορυφαίες προκλήσεις διαλειτουργικότητας που πρέπει να αντιμετωπιστούν:

- **Κανόνες περί απορρήτου και εμπιστευτικότητας των δεδομένων των ασθενών**

Ένα αποτελεσματικό σύστημα διαλειτουργικότητας θα πρέπει να εξετάσει τον τρόπο με τον οποίο θα εφαρμόζονται οι κανόνες περί απορρήτου και εμπιστευτικότητας των δεδομένων των ασθενών σε διάφορα κράτη. Αυτό οφείλεται στο ότι διάφορα κράτη ενδέχεται να διστάζουν να μοιραστούν τα δεδομένα της υγειονομικής περίθαλψης ως αποτέλεσμα της έλλειψης διαβεβαίωσης όσον αφορά τους ασθενείς που μοιράζονται δεδομένα.

- **Ευχέρεια του EHR:**

Ενώ υπάρχουν πρότυπα υγειονομικής περίθαλψης για την ηλεκτρονική ανταλλαγή δεδομένων, οι περισσότεροι επαγγελματίες υγείας συμφωνούν ότι δεν επαρκούν για την επίτευξη της πλήρους διαλειτουργικότητας του EHR. Επομένως, οποιοσδήποτε πωλητής ολοκλήρωσης της EHR πρέπει να κατανοήσει τον τελικό μηχανισμό ολοκλήρωσης όπως ο HL7(Επίπεδο υγείας επτά) που κατανοεί η πλειονότητα των παρόχων υγειονομικής περίθαλψης. Στην πραγματικότητα, ο κινητήρας διασύνδεσης HL7 μπορεί να βοηθήσει να συνδεθεί οποιοδήποτε EHR παλαιού τύπου με οποιοδήποτε πρωτόκολλο επικοινωνίας ανταλλαγής μηνυμάτων για βελτιωμένη ανταλλαγή δεδομένων υγειονομικής περίθαλψης. Δεδομένου ότι τα περισσότερα νοσοκομεία και οι πάροχοι υγειονομικής περίθαλψης έχουν διαφορετικά πρότυπα, η χρήση του HL7 μπορεί να συμβάλει στην ενσωμάτωση με το EHR με αποτελεσματικό και απρόσκοπτο τρόπο.

- **Σύνδεση/ταίριασμα ασθενούς**

Η διαδικασία αντιστοίχισης των αρχείων των ασθενών εξακολουθεί να αποτελεί μείζονα ανησυχία για τα περισσότερα EHRs. Αυτό οφείλεται στο γεγονός ότι τα διαφορετικά συστήματα υγειονομικής περίθαλψης χρησιμοποιούν διαφορετικά δημογραφικά δεδομένα που αντιστοιχούν στους ασθενείς με τα αρχεία της υγείας τους. Στις περισσότερες από αυτές τις περιπτώσεις, δημιουργούνται συνήθως ανακριβή αποτελέσματα όπου οι ασθενείς έχουν διαφορετικά ονόματα, ημερομηνίες γέννησης και ακόμη και ηλικίες.

- **Απόκτηση δεδομένων, μετατροπή και τυποποίηση**

Το γεγονός ότι οι πρακτικές τεκμηρίωσης του παρόχου ποικίλλουν από τον έναν πωλητή στον άλλο σημαίνει ότι τυχόν δεδομένα που ενδέχεται να καταγραφούν στο EHR, μπορούν να ερμηνεύονται διαφορετικά από διαφορετικό EHR. Έτσι, ισχυρότερες μέθοδοι για δεδομένα σε μια εφαρμογή που δεν ενσωματώνει μόνο τα συστήματα EHRs, αλλά επίσης εξασφαλίζει ότι είναι απαραίτητη η συλλογή δεδομένων, οι διαδικασίες εξαγωγής, η μορφή και η τυποποίηση.

- **Τεχνικές παραλλαγές στην ανάπτυξη των EHR**

Υπάρχουν χιλιάδες EHRs έξω με κάθε σύστημα που έχει διαφορετική τεχνολογική αρχιτεκτονική, μοντέλα υπηρεσιών και ακόμη και δυνατότητες. Αυτό καθιστά δύσκολο για οποιονδήποτε πωλητή ολοκλήρωσης να αναπτύξει ένα κοινό σχήμα διαλειτουργικότητας για την ανταλλαγή δεδομένων υγειονομικής περίθαλψης.

Έτσι για να μπορέσουμε να αποκομίσουμε τα μέγιστα οφέλη από την ολοκλήρωση, πρέπει να αντιμετωπιστούν οι προαναφερθείσες προκλήσεις.

5.5 Μέτρα ασφαλείας

Υποθέτουμε ότι όλοι οι συμμετέχοντες οργανισμοί, όπως τα κέντρα υγείας ή οι πάροχοι σύννεφου, έχουν κοινό συμφέρον για τη διασφάλιση της υποδομής και των δεδομένων έναντι εξωτερικών αντιπάλων τρίτων. Ως εκ τούτου, θα είναι εφικτή η καθιέρωση κοινών και συνεργατικών μηχανισμών ασφαλείας, παρόλο που πολλές πρακτικές και διαδικαστικές προκλήσεις θα μπορούσαν να προκύψουν κατά την εφαρμογή τους σε συγκεκριμένα σενάρια χρήσης. Συγκεκριμένα, αναλαμβάνουμε μια συνεργατική υποδομή για έλεγχο ταυτότητας πελατών και υπηρεσιών. Αυτό θα μπορούσε να περιλαμβάνει μια κεντρική Αρχή Πιστοποίησης (CA), ένα δέντρο ή ένα

"δάσος" των αρχών πιστοποίησης που σχηματίζουν μια υποδομή δημόσιου κλειδιού (PKI) ή ένα πλήρως συνδεδεμένο ιστό εμπιστοσύνης μεταξύ όλων των συμμετεχόντων οργανισμών. Οποιοδήποτε πρόγραμμα ή υπηρεσία πελάτη μπορεί να πιστοποιηθεί, εμποδίζοντας μη εξουσιοδοτημένα τρίτα μέρη να συμμετάσχουν στο σύστημα απλά υιοθετώντας μια ψευδή ταυτότητα.

5.5.1 Συστήματα και μέθοδοι για ασφαλή κοινή χρήση δεδομένων

Πρόκειται για άλλο ένα τρόπο μυστικής κοινής χρήσης που σχετίζεται γενικά με μεθόδους και συστήματα ανταλλαγής δεδομένων.

- Μία υλοποίηση όπου σχετίζεται γενικά με μια μέθοδο για την κρυπτογράφηση δεδομένων χρησιμοποιώντας ένα διακριτό κλειδί επιπέδου αρχείου. Αυτό το κοινόχρηστο κλειδί σε επίπεδο αρχείου επιτρέπει την κοινή χρήση μεμονωμένων αρχείων που προστατεύονται από ένα κλειδί ομάδας εργασίας χωρίς να εκθέσει το κλειδί ομάδας εργασίας σε τρίτες οντότητες. Το κοινόχρηστο κλειδί σε επίπεδο αρχείου μπορεί να δημιουργηθεί χρησιμοποιώντας ένα κλειδί ομάδας εργασίας που σχετίζεται με μοναδικές πληροφορίες του αρχείου.

- Άλλη μία μέθοδος για ασφαλή κοινή χρήση αρχείων είναι να παράσχει ένα κρυπτογραφικό σύστημα όπου ένας ή περισσότεροι ασφαλείς εξυπηρετητές ή μια μηχανή εμπιστοσύνης αποθηκεύουν κρυπτογραφικά κλειδιά και δεδομένα ταυτότητας χρήστη. Το σύστημα μπορεί να αποθηκεύει δεδομένα σε μία ή περισσότερες συσκευές αποθήκευσης σε ένα σύννεφο. Το νέφος μπορεί να περιλαμβάνει συσκευές ιδιωτικής αποθήκευσης προσβάσιμες μόνο σε ένα συγκεκριμένο σύνολο χρηστών ή συσκευές δημόσιας αποθήκευσης προσβάσιμες σε οποιοδήποτε σύνολο χρηστών που προσυπογράφουν στον παροχέα αποθήκευσης. Οι χρήστες έχουν πρόσβαση στη λειτουργικότητα των συμβατικών κρυπτογραφικών συστημάτων μέσω

της πρόσβασης στο δίκτυο στη μηχανή εμπιστοσύνης, ωστόσο, ο μηχανισμός εμπιστοσύνης δεν απελευθερώνει πραγματικά κλειδιά και άλλα δεδομένα ελέγχου ταυτότητας και επομένως τα κλειδιά και τα δεδομένα παραμένουν ασφαλή. Αυτή η κεντρική αποθήκευση των κλειδιών και των στοιχείων ελέγχου ταυτότητας για διακομιστές παρέχει ασφάλεια, φορητότητα, διαθεσιμότητα και ευκολία. Επειδή οι χρήστες μπορούν να είναι βέβαιοι ή να εμπιστεύονται το κρυπτογραφικό σύστημα για την πραγματοποίηση ταυτότητας χρηστών και εγγράφων και άλλων κρυπτογραφικών λειτουργιών, μπορεί να ενσωματωθεί στο σύστημα ένα ευρύ φάσμα λειτουργιών. Για παράδειγμα, ο πάροχος μηχανισμού εμπιστοσύνης μπορεί να εξασφαλίσει την απόρριψη της συμφωνίας, για παράδειγμα, πιστοποιώντας την ταυτότητα των συμμετεχόντων στη συμφωνία, υπογράφοντας ψηφιακά τη συμφωνία εξ ονόματος ή για τους συμμετέχοντες και αποθηκεύοντας ένα αρχείο της συμφωνίας που υπογράφηκε ψηφιακά από κάθε συμμετέχοντα. Επίσης, το κρυπτογραφικό σύστημα μπορεί να παρακολουθεί συμφωνίες και να αποφασίζει να εφαρμόζει διαφορετικούς βαθμούς εξακρίβωσης της γνησιότητας, με βάση, για παράδειγμα, την τιμή, τον χρήστη, τον προμηθευτή, τη γεωγραφική θέση, τον τόπο χρήσης ή τα συναφή.

Υπάρχουν αρκετές ασφαλείς μέθοδοι για την ανάπτυξη και προστασία κλειδιών ομάδας εργασίας. Η επιλογή της μεθόδου που πρέπει να χρησιμοποιηθεί για μια συγκεκριμένη εφαρμογή εξαρτάται από διάφορους παράγοντες όπως η αποθήκευση κλειδιού βασισμένου σε υλικό και βασική αποθήκευση βασισμένη σε λογισμικό. Αυτοί οι παράγοντες μπορεί να περιλαμβάνουν το επίπεδο ασφάλειας που απαιτείται, το κόστος, την ευκολία και τον αριθμό των χρηστών στην ομάδα εργασίας.

- Οι κλασικές έννοιες μοιράσματος μυστικών τυπικά δεν είναι κλειδωμένες. Έτσι, ένα μυστικό σπάει σε μετοχές ή ανακατασκευάζεται από αυτά, με τέτοιο τρόπο που δεν απαιτεί ούτε από τον αντιπρόσωπο ούτε από την ομάδα να ανακατασκευάσει το μυστικό, να κατέχει οποιοδήποτε είδος συμμετρικού ή ασύμμετρου κλειδιού. Ενώ ο αναλυτής ασφαλών δεδομένων που περιγράφεται εδώ, είναι προαιρετικά κλειδωμένος. Ο αντιπρόσωπος

μπορεί να παρέχει ένα συμμετρικό κλειδί που μπορεί να απαιτηθεί για την ανάκτηση δεδομένων, εάν χρησιμοποιείται για κοινή χρήση δεδομένων. Ο αναλυτής ασφαλών δεδομένων μπορεί να χρησιμοποιήσει το συμμετρικό κλειδί για να διασκορπίσει ή να διανείμει μοναδικά τμήματα του μηνύματος που πρόκειται να ασφαλιστούν σε δύο ή περισσότερα μερίδια.

- Η **μέθοδος ασφαλούς αναλυτή** μπορεί να ενσωματωθεί σε οποιαδήποτε δικτυακή εφαρμογή προκειμένου να αυξηθεί η ασφάλεια, η ανοχή σφάλματος, η ανωνυμία ή οποιοσδήποτε κατάλληλος συνδυασμός των προαναφερθέντων. Ο αναλυτής ασφαλών δεδομένων της παρούσας εφεύρεσης μπορεί να χρησιμοποιηθεί για την υλοποίηση μιας λύσης ασφαλείας δεδομένων υπολογιστικού νέφους. Μπορεί να χρησιμοποιηθεί για την προστασία των πόρων του cloud computing και των δεδομένων που μεταδίδονται μεταξύ του νέφους και ενός τελικού χρήστη ή μιας συσκευής. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για να διασφαλίσει την αποθήκευση δεδομένων στο σύννεφο, τα δεδομένα σε κίνηση από και προς το σύννεφο, την πρόσβαση στο δίκτυο στο σύννεφο, τις υπηρεσίες δεδομένων στο σύννεφο, την πρόσβαση σε υπολογιστικούς πόρους υψηλής απόδοσης το σύννεφο και οποιεσδήποτε άλλες λειτουργίες στο σύννεφο. Σε μερικές ενσωματώσεις, ο ασφαλής ανιχνευτής μπορεί πρώτα να τυχαιοποιήσει τα αρχικά δεδομένα και στη συνέχεια να διαχωρίσει τα δεδομένα σύμφωνα είτε με μια τυχαία είτε με καθοριστική τεχνική.

Το κύριο κλειδί του αναλυτή:

Αυτό το κλειδί είναι ένα μεμονωμένο κλειδί που σχετίζεται με την εγκατάσταση του αναλυτή ασφαλών δεδομένων. Είναι εγκατεστημένο στον εξυπηρετητή στον οποίο έχει αναπτυχθεί ο αναλυτής ασφαλών δεδομένων. Υπάρχει μια ποικιλία επιλογών που είναι κατάλληλες για την ασφάλεια αυτού του κλειδιού, όπως για παράδειγμα μια έξυπνη κάρτα, ξεχωριστό αποθηκευτικό κλειδί υλικού, τυποποιημένα αποθηκευμένα κλειδιά, προσαρμοσμένα αποθηκευτικά κλειδιά ή μέσα σε έναν ασφαλή πίνακα βάσεων δεδομένων.

5.6 Super Users - το μυστικό όπλο για την εκπαίδευση InfoSec για την παροχή ασφάλειας στην υγειονομική περίθαλψη

Πλειοψηφία οργανώσεων υγειονομικής περίθαλψης κάνουν χρήση σούπερ χρηστών για την κατάρτιση Ηλεκτρονικής Αρχής Υγείας (EMS). Μελέτες έχουν δείξει ότι η αποτελεσματική χρήση σούπερ χρηστών μπορεί να αυξήσει την ικανοποίηση των τελικών χρηστών με το EHR, να βελτιώσει την παραγωγικότητα του προσωπικού, να βελτιώσει τη συνολική ικανοποίηση από την εργασία και να προσφέρει μια σταδιοδρομία για το κλινικό προσωπικό με τεχνολογία ενδιαφέροντος και δεξιοτήτων. Επίσης έχει αποδειχθεί ότι βελτιώνει το συνολικό EHR παρέχοντας καλύτερη ανατροφοδότηση στην IS(InfoSec) και καλύτερα τεκμηριωμένα αιτήματα βελτίωσης.

Κάποιες κορυφαίες οργανώσεις υγειονομικής περίθαλψης ήδη συνδέουν τη χρήση της ηλεκτρονικής μάθησης και την εκπαίδευση στην ασφάλεια πληροφοριών. Έτσι, μαζί με την εκπαίδευση ηλεκτρονικού "ψαρέματος" (fishing training) και άλλες εκπαιδευτικές προσπάθειες των τελικών χρηστών, ορισμένοι οργανισμοί έχουν καταλάβει ότι οι σούπερ χρήστες μπορεί να είναι ένα από τα λιγότερο αξιοποιημένα περιουσιακά στοιχεία για την ενίσχυση της ασφάλειας των πληροφοριών στην επιχείρηση.

Με τους περισσότερους ορισμούς, οι άριστοι χρήστες είναι εκείνοι οι τελικοί χρήστες που καταλαβαίνουν τη χρήση τεχνολογίας στο έργο τους και που είναι ενθουσιασμένοι με την ανταλλαγή αυτών των γνώσεων με τους συναδέλφους τους. Αυτοί οι τελικοί χρήστες μπορούν να αξιοποιήσουν αποτελεσματικά την ασφάλεια πληροφοριών και την εκπαίδευση για την προστασία της ιδιωτικής ζωής στο πλαίσιο της κατάρτισης των τελικών χρηστών τους.

Έχοντας πολύ καλά εκπαιδευμένους ειδικούς που προπονούν προσωπικό σε βασικές πληροφορίες, όπως η διατήρηση μυστικών κωδικών πρόσβασης, η μη κατανομή λογαριασμών χρηστών, η αποσύνδεση του EHR όταν δεν χρησιμοποιούνται, η κατάλληλη χρήση του EHR για τη διατήρηση της ιδιωτικότητας και της ασφάλειας μπορεί να είναι ισχυρή. Σκεφτείτε την εκθετική επίδραση αυτού του τύπου εκπαίδευσης σε σχέση με τις τυπικές προσπάθειες κατάρτισης στον τομέα της ασφάλειας των πληροφοριών. Τα τυποποιημένα στοιχεία της κατάρτισης για την ασφάλεια των πληροφοριών μπορούν εύκολα να ενσωματωθούν στην εκπαίδευση των υπερήχων. Μόλις εκπαιδεύονται σούπερ χρήστες, μπορούν να συνεχίσουν να διαδίδουν αυτή τη γνώση μέσω των καθημερινών αλληλεπιδράσεων με τους συναδέλφους τους.

Επίσης οι επαγγελματίες της ασφάλειας της πληροφόρησης της υγείας πρέπει να εξετάζουν τους κλινικούς εκπαιδευτικούς τους και τις ομάδες κατάρτισης τους για βοήθεια στην προσθήκη θεμελιωδών στοιχείων ασφάλειας πληροφοριών σε προγράμματα κλινικής κατάρτισης.

Αυτοί οι χρήστες είναι σε καλύτερη θέση να παρέχουν ανατροφοδότηση στην IS και στην ομάδα InfoSec σχετικά με τα μέτρα ασφαλείας. Πληροφορίες Sec πρέπει πάντα να είναι μια ισορροπία μεταξύ της διαχείρισης κινδύνου και των επιχειρησιακών αναγκών. Έχοντας τους εξελιγμένους σούπερ χρήστες που παρέχουν ανατροφοδότηση, μπορούμε να παρακολουθούμε συνεχώς τους ελέγχους ασφαλείας για τη διασφάλιση ότι δεν παρεμποδίζουν αδικαιολόγητα κλινικές ή επιχειρηματικές δραστηριότητες. Χωρίς αυτόν τον κρίσιμο βρόχο ανατροφοδότησης, πιθανότατα θα δημιουργηθεί υπερβολικά περιοριστική ασφάλεια, προκαλώντας εναλλακτικές λύσεις όπως κοινή χρήση userid και καταγραφή κωδικών πρόσβασης που έχουν κολληθεί στην κάτω πλευρά ενός πληκτρολογίου.

Συμπεράσματα

Είναι σαφές ότι, η χρήση του cloud computing έχει γρήγορα επεκταθεί μέσω των διαδικτυακών εφαρμογών, κάνοντας τη ζωή του κάθε ανθρώπου πιο εύκολη, ικανοποιώντας τις απαιτήσεις επιχειρήσεων και καταναλωτών. Η χρήση της τεχνολογίας του cloud computing σε μια υγειονομική περίθαλψη μπορεί να βελτιώσει σημαντικά την πρόσβαση στις πληροφορίες, η οποία μπορεί να γίνει πολύ πιο εύκολη.

Η κλιμάκωση, που είναι το κλειδί του cloud computing, μπορεί να προσφέρει περισσότερους πόρους που απαιτούνται για ορισμένες λειτουργίες ανά πάσα στιγμή. Η συνεργασία μεταξύ των μονάδων υγειονομικής περίθαλψης αποτελεί μια ευκαιρία που προσφέρεται από το cloud computing για το προσωπικό της υγειονομικής περίθαλψης. Με αυτήν την τεχνολογία μπορεί να ελεγχθεί η διαθεσιμότητα ιατρού, ειδικού ιατρού, προϊόντος ή υπηρεσίας σε διαφορετικές χρονικές στιγμές και σε διαφορετικές περιπτώσεις. Τα ζητήματα ασφάλειας και προστασίας της ιδιωτικής ζωής του cloud computing καθυστερούν τη γρήγορη υιοθέτησή του, αλλά έχει γίνει πολύ δημοφιλής και έπρεπε να παράσχουμε μηχανισμούς ασφαλείας για να εξασφαλίσουμε την ασφαλή υιοθέτησή του.

Παρόλο που η χρήση του cloud computing έχει αυξηθεί ραγδαία, η ασφάλεια του cloud computing εξακολουθεί να θεωρείται το σημαντικότερο ζήτημα στο περιβάλλον του cloud computing. Επιπλέον, η εισβολή των δεδομένων οδηγεί σε πολλά προβλήματα τους χρήστες του cloud computing που έχει τη δυνατότητα να γίνει πρωτοπόρος στην προώθηση μιας ασφαλούς, εικονικής και οικονομικά βιώσιμης λύσης στο μέλλον.

Επίσης, υποστηρίζεται η μετάβαση σε multi-cloud χάρη στην ικανότητά του να μειώνονται οι κίνδυνοι ασφαλείας που κυριαρχούν στο cloud computing. Η αρχιτεκτονική Multi-Cloud παρέχει ένα περιβάλλον όπου οι επιχειρήσεις μπορούν να δημιουργήσουν ασφαλή και ισχυρά περιβάλλοντα cloud πέρα από την παραδοσιακή υποδομή. Προφανώς απαιτείται μια λεπτομερή ανάλυση και σύγκριση των διαφορετικών στρατηγικών προγραμματισμού για περαιτέρω

έρευνα, για λόγους πληρότητας, προκειμένου να αναδειχθούν περισσότερο τα κύρια οφέλη ή το περιβάλλον του multi-cloud.

Στην συνέχεια, ο αλγόριθμος μυστικής κατανομής του Adi Shamir έχει μια καλή βάση που παρέχει μια εξαιρετική πλατφόρμα για τις εφαρμογές και έχει μεγάλη σημασία για πολλούς νέους τομείς. Προέχει απ' όλες τις μεθόδους μυστικής κοινής χρήσης μέχρι στιγμής, λόγω της παροχής των τριών κυριότερων χαρακτηριστικών ασφάλειας που αναζητεί κάθε χρήστης και οργανισμός από τους παρόχους του cloud computing.

Λύση/Πρόταση Βελτίωσης

Με βάση τα παραπάνω σαν λύση θα μπορούσε να είναι ένας συνδυασμός του συστήματος μυστικής κοινής χρήσης που προτείνει ο Shamir και μιας μεθόδου για ασφαλή κοινή χρήση αρχείων όπου μια μηχανή εμπιστοσύνης αποθηκεύει κρυπτογραφικά κλειδιά και δεδομένα ταυτότητας χρήστη. Με την μεν μέθοδο του Shamir πραγματοποιείται η αποθήκευση πληροφοριών που είναι ιδιαίτερα ευαίσθητες και εξαιρετικά σημαντικές διότι τα συστήματα μυστικής κατανομής αντιμετωπίζουν αυτό το πρόβλημα και επιτρέπουν την επίτευξη υψηλών επιπέδων εμπιστευτικότητας και αξιοπιστίας και με την μέθοδο μιας μηχανής εμπιστοσύνης δεν απελευθερώνονται πραγματικά κλειδιά και άλλα δεδομένα ελέγχου ταυτότητας και επομένως τα κλειδιά και τα δεδομένα παραμένουν ασφαλή παρέχοντας ασφάλεια, φορητότητα, διαθεσιμότητα και ευκολία.

Επιπλέον, χρειάζεται αυστηρός έλεγχος πρόσβασης με «**δακτυλικό αποτύπωμα»** ή αλλιώς «**έξυπνη κάρτα**» για τους επαγγελματίες υγείας και αυστηρός έλεγχος από το σύστημα με όλα τα στοιχεία και του εσωτερικού ιατρικού προσωπικού και των εξωτερικών παραγόντων, όπως είναι οι ασφαλιστικές εταιρείες και περιορισμένη πρόσβαση στους ασθενείς και τις ασφαλιστικές εταιρείες.

Η έξυπνη κάρτα του επαγγελματία υγείας σαν μια προσωπική κάρτα, αποτελεί αναμφισβήτητα ένα ισχυρό θεμέλιο των διαδικασιών περίθαλψης τόσο για τους ασθενείς – ασφαλισμένους όσο και για τους παρόχους υγείας προστατεύοντας τις εμπλεκόμενες πληροφορίες της διεπαφής τους από μη εξουσιοδοτημένους χρήστες.

Λόγω του ότι λειτουργεί ως κλειδί, επιτρέπει στον κάτοχο της να ξεκλειδώσει τα προσωπικά ιατρικά δεδομένα των ασθενών, τα οποία είναι αποθηκευμένα είτε στην κάρτα είτε σε ένα δίκτυο υγείας (e- health network). Η χρήση της γίνεται παγκοσμίως για την ασφαλή προστασία της ταυτότητας των ασθενών και απαιτείται ένα ισχυρό τοπικό σύστημα, το οποίο θα αποτελείται από κάρτες, σταθμούς εργασίας των χρηστών, computer servers, αναγνώστες καρτών και ολοκληρωμένο σύστημα διαχείρισης καρτών.

Επίσης, ο κάθε επαγγελματίας υγείας δε θα μπορεί να έχει γενικά άλλη και απλή πρόσβαση σε άλλου ιατρού τα κρίσιμα/ευαίσθητα αρχεία αλλά μόνο με «ειδική άδεια πρόσβασης» κατόπιν επαφής με τον ίδιο τον επαγγελματία υγείας που είναι στη κατοχή του τα αρχεία αυτά. Το ηλεκτρονικό αρχείο υγείας του ασθενούς θα περιέχει το ιστορικό εν μέρη και ονομαστικά μόνο και τα στοιχειά του ιδίου του ασθενούς ή ένα ειδικό αριθμό μητρώου ασθενή. Ακόμα, όλα τα νοσοκομεία/κέντρα υγείας μπορούν να έχουν τα δικά τους συστήματα ξεχωριστά αλλά όλα ένα και μόνο ίδιο πρόγραμμα στο λογισμικό τους το όποιο θα μπορούν να ανταλλάσουν με αυτό πληροφορίες μεταξύ τους και θα υπάρχει διαθεσιμότητα αρχείων κατόπιν όμως των παραπάνω αυστηρών προϋποθέσεων ώστε να λειτούργει σωστά και ασφαλές. Όσο πιο αυστηρές είναι οι προϋποθέσεις για πρόσβαση στο cloud τόσο πιο αυξημένη είναι η ακεραιότητα των δεδομένων, η εμπιστευτικότατα και η αξιοπιστία. Αν και με αυτό το τρόπο η διαθεσιμότητα κατά κάποια έννοια θα είναι πιο αυστηρή αλλά το σύστημα θα είναι πιο ασφαλής.

Βιβλιογραφία

1. F. Gens. (2009, Feb.). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”,*IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

2. J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” *Infoworld*,
Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity- risks-853?page=0,1> [Mar. 13, 2009].

3. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

4. ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for informationsecurity." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].

5. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.

6. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

7. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

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

9. S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.

10. M. A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security
Problem” In PROC APSEC 2010 Cloud Workshop. 2010.

11. Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]

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

13. A Platform Computing Whitepaper. “Enterprise Cloud Computing: Transforming IT.” *Platform Computing*, pp6, 2010.

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

15. M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. “What’s Inside the Cloud? An Architectural Map of the Cloud Landscape.” *IEEE Xplore*, pp 23-31, Jun. 2009.

16. C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. “Business Models in the Service World.” *IT Professional*, vol. 11, pp. 28-33, 2009.

17. N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. “On Technical Security Issues in Cloud Computing” In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.

18. N. Leavitt. “Is Cloud Computing Really Ready for Prime Time?” *Computer*, vol. 42, pp. 15- 20, 2009.

19. M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.

20. C. Soghoian. “Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era” The Berkman Center for Internet & Society Research Publication Series. Available: http://cyber.law.harvard.edu/publications [Aug.22, 2009].

21. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

22. Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, “A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing”, School of Information and Communication Technology, CQ University QLD 4702, Australia. Received 15 August 2011. Revised 11 January 2012. Accepted 18 January 2012. Available online 27 January 2012.

23. C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

24. Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, “Security and Privacy in Cloud Computing: A Survey”, Sixth International Conference on Semantics, Knowledge and Grids, August 2010.

25. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds”,2012 ,45th Hawaii International Conference on System Sciences.

26. M. Vukolic,"The Byzantine empire in theintercloud", ACM SIGACT News, 41,2010, pp.105-111.

27. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

28. K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.187-198.

29. H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

30. C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

31. G. Chockler, R. Guerraoui, I. Keidar, and M. Vukoli´c, “Reliable distributed storage,” IEEE Computer, vol. 42, no. 4, pp. 60–67, 2009.

32. F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. WorkshopDependabilityof Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.

33. H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

34. Adi Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.

35. Md Kausar Alam, Sharmila Banu K, “An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds”, International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

36. Swapnila S Mirajkar, Santoshkumar Biradar, “Using Secret Sharing Algorithm for Improving Security in Cloud Computing”,International Journal of Advanced Research in Computer Science & Technology, Vol. 2, Issue 2, Ver. 3

37. *S.Jaya Nirmala , S.Mary Saira Bhanu, Ahtesham Akhtar Patel , "A comparative study of the secret sharingalgorithms for secure data in the cloud",* International Journal on Cloud Computing: Services and Architecture, Vol.2, No.4, August 2012

38. *Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing",* School of Information and Communication Technology, CQ University QLD 4702, Australia. 15 August 2011.

39. *Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey" ,*Sixth International Conference on Semantics, Knowledge and Grids, August 2010.

40. *Midong Yhou, Zygmunt J. Hass, Securing Ad-Hoc Networks, IEEE Networks Special Issue on Network Security,* November/December 1999.

41. *Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security:* C. Asmuth and J. Bloom, A Modular Approach to Keysafeguarding. IEEE Transactions on Information Theory, 29 (2), 208–210, 1983.

42. S. Basu, A. Karp, J. Li, J. Pruyne, J. Rolia, and S. Singhal, et al., Fusion: Managing Healthcare Records at Cloud Scale. IEEE Computer, Special Issue on Move Toward Electronic Health Records, 2012.

43. A.N. Bessani, M.P. Correia, B. Quaresma, F. Andre, and P. Sousa, Depsky: dependable and secure storage in a cloud-of-clouds. In: Proceedings of the Sixth European Conference on Computer Systems, pp. 31–46, 2011.

44. G. Blakley, Safeguarding Cryptographic Keys. Proceedings of AFIPS National Computer Conference, 1979.

45. L. Chen and D.B. Hoang, Novel Data Protection Model in Healthcare Cloud. IEEE International Conference on High Performance Computing and Communications, 2011.

46. T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, and T.-C. Lin, Secure Dynamic Access Control Scheme of PHR in Cloud Computing. Journal of Medical Systems, 36, 4005–4020, 2012a.

47. Y.-Y. Chen, J.-C. Lu, and J.-K. Jan, A Secure EHR System Based on Hybrid Clouds. Journal of Medical Systems, 36, 3375–3384, 2012b.

48. M. Deng, M. Petkovié, M. Nalin, and I. Baroni, A Home Healthcare System in the Cloud - Addressing Security and Privacy Challenges, in Proceedings of the IEEE 4th International Conference on Cloud Computing, 2011.

49. M. Deng, M. Nalin, M. Petkovié, I. Baroni, and A. Marco, Towards Trustworthy Health Platform Cloud, Secure Data Management, Lecture Notes in Computer Science, 7482, 162-175, 2012.

50. D. Eastlake and P. Jones, US Secure Hash Algorithm 1 (SHA1), RFC 3174, IETF, 2001.

51. D.F. Ferraiolo, D.R. Kuhn, and R. Chandramouli, Role-Based Access Control. Artech House, 2007, 2007.

52. B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, A Comparison of Security Requirements Engineering Methods. Requirements Engineering Journal, Volume 15, Number 1, 7–40, 2010.

53. B. Fabian, T. Ermakova, and C. Müller, SHARDIS – A Privacy-Enhanced Discovery Service for RFID-Based Product Information. IEEE Transaction on Industrial Informatics, 8 (3), 707–718, 2012.

54. R. Geambasu, T. Kohno, A.A. Levy, and H.M. Levy, Vanish: Increasing Data Privacy with Self-Destructing Data. 18th Usenix Security Symposium, 2009.

55. A.R. Hevner, S.T. March, J. Park, and S. Ram, Design Science in Information Systems Research. MIS Quarterly, 28, 75-105, 2004.

56. H. Krawczyk, Distributed Fingerprints and Secure Information Dispersal. 12th Annual ACM Symposium on Principles of Distributed Computing. ACM, 207–218, 1993.

57. H. Krawczyk, Secret Sharing Made Short. 13th Annual International Cryptology Conference on Advances in Cryptology, 136–146, 1994.

58. S. Kunz, S. Evdokimov, B. Fabian, B. Stieger, and M. Strembeck, Role-Based Access Control for Information Federations in the Industrial Service Sector. 18th European Conference on Information Systems (ECIS 2010), 2010.

59. M. Li, S. Yu, K. Ren, and W. Lou, Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. SecureComm 2010, LNICST 50, 89-106, 2010.

60. Z.-R. Li, E.-C. Chang, K.-H. Huang, and F. Lai, A Secure Electronic

Medical Record Sharing Mechanism in the Cloud Computing Platform. 15th IEEE International Symposium on Consumer Electronics, 2011a.

61. M. Li, S. Yu, N. Cao, and W. Lou, Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing. 31st International Conference on Distributed Computing System (ICDCS), 2011b.

62. M. Li, S. Yu, Y. Zheng, K Ren, and W. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption. IEEE Transactions on Parallel and Distributed Systems, 2012.

63. Y. Liu, Y. Wang, and Y. Jin, Research on the Improvement of MongoDB Auto-Sharding in Cloud Environment. 7th International Conference on Computer Science and Education, 2012.

64. H. Loehr, A.-R. Sadeghi, and M. Winandy, Securing the E-Health Cloud. ACM International Health Informatics Symposium (IHI '10), 2010.

65. B.N. Mills and T. Znati, Increasing DHT Data Security by Scattering Data. ICCCN, 430-434, 2008.
66. Nematzadeh and L.J. Camp, Threat Analysis of Online HealthInformation System. 3rd International Conference on Pervasive Technologies Related to Assistive Environments, 2010.

67. OASIS, Web Services Security v1.1.1. https://www.oasisopen.org/standards#wssv1.1.1, 2012.

68. OMG, Business Process Model and Notation. http://www.bpmn.org/, 2012.

69. K. Peffers, T. Tuunanen, M.A. Rothenberger, and S. Chatterjee, A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24 (3), 3, 45-77, 2008.

70. M. Rabin, Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. Journal of the ACM 36, 335-348, 1989.

71. R. Rodrigues and B. Liskov, High Availability in DHTs: Erasure Coding vs. Replication. 4th International Workshop on Peer-to-Peer Systems, 2005.Adi Shamir, How to Share a Secret. Communications of the ACM 22 (11), 612-613, 1979.

72. S.S.Y. Shim, G. Bhalla, and V. Pendyala, Federated Identity Management. IEEE

Computer 38 (12), 120-22, 2005.

73. S.G. Shini, T. Thomas, and K. Chithraranjan, Cloud Based Medical Image Exchange-Security Challenges, in Proceedings of the International Conference on Modelling, Optimization and Computing, 2012.

74. W. Stallings, Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010.

75. R. Stinson, An Explication of Secret Sharing Schemes. Des. Codes Cryptography 2 (4), 357-390, 1992.

76. R. Thomas and R. Sandhu, Task-Based Authorization Controls (TBAC), IFIP WG11.3 Conference on Database Security, 1997.

77. TRESOR, http://www.cloud-tresor.com/, 2013.

78. J. Vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. 17th European Conference on Information Systems (ECIS), 2009.

79. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. IEEE INFOCOM'10, 2010.

80. R. Zhang and L. Liu, Security Models and Requirements for Healthcare Application Clouds. IEEE 3rd International Conference on Cloud Computing, 2010.

Διαδίκτυο

- https://patents.google.com/patent/US8255529B2/en
- https://patents.google.com/patent/US8407284B2/en
- https://www.nytimes.com/2014/11/18/opinion/electronic-health-records-how-systems-share.html