Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων
Τμήμα Ψηφιακών Συστημάτων

Επίπεδο: Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Ψηφιακών Συστημάτων

Θέματα ασφαλείας κατά τη μετάβαση σε Cloud υποδομές

Επιβλέπον Καθηγητής: Χ. Ξενάκης

Ονοματεπώνυμο	E-mail	Α.Μ.
Ορέστης Αναστάσιος Γκιόκας	orestisgiokas@gmail.com	MTE2106

Πειραιάς
26/06/2023

Περίληψη

Το υπολογιστικό νέφος (cloud computing) είναι ένα μοντέλο διαχείρισης πόρων που επιτρέπει την άνετη, κατ' απαίτηση πρόσβαση σε μια κοινόχρηστη δεξαμενή υπολογιστικών πόρων. Λόγω των πολλαπλών οφελών που προσφέρει αυτή η τεχνολογία, πολλοί οργανισμοί, μεταξύ των οποίων Δημόσιοι αλλά και Στρατιωτικοί φορείς μελετούν ή και προβαίνουν στην μετάβαση των πληροφοριακών υποδομών τους στο υπολογιστικό νέφος. Ωστόσο παρά τις θετικές πτυχές της, αυτή η τεχνολογία ενδεχομένως να ενέχει κινδύνους και αδυναμίες οι οποίες να την καθιστούν ακατάλληλη για χρήση από συγκεκριμένους φορείς. Η μελέτη αυτή στοχεύει στην ανάλυση αυτών των αδυναμιών, τη σύγκριση των υπηρεσιών διαφορετικών παρόχων υπηρεσιών νέφους, αλλά και τους λόγους για τους οποίους ένας φορέας θα μπορούσε να μεταβεί ή όχι σε υποδομές νέφους.

Περιεχόμενα

Λίστα εικόνων

Ακρωνύμια

ADVOS	Anti-DDoS Virtualized Operating System
API	Application Programming Interface
ARP	Address Resolution Protocol
AWS	Amazon Web Services
CA	Certificate Authority
CESWP	Cloud-Enabled Space Weather Platform
CPU	Central Processing Unit
CSP	Cloud Service Provider
CSRF	Cross Site Request Forgery
DoS	Denial of Service
DP	Data Processor
FaaS	Function as a Service
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
JSON	JavaScript Object Notation
KVM	Kernel Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MT	Magnetotellurics
OS	Operating System
OWASP	Open Web Application Security Project
PaaS	Platform as a Service

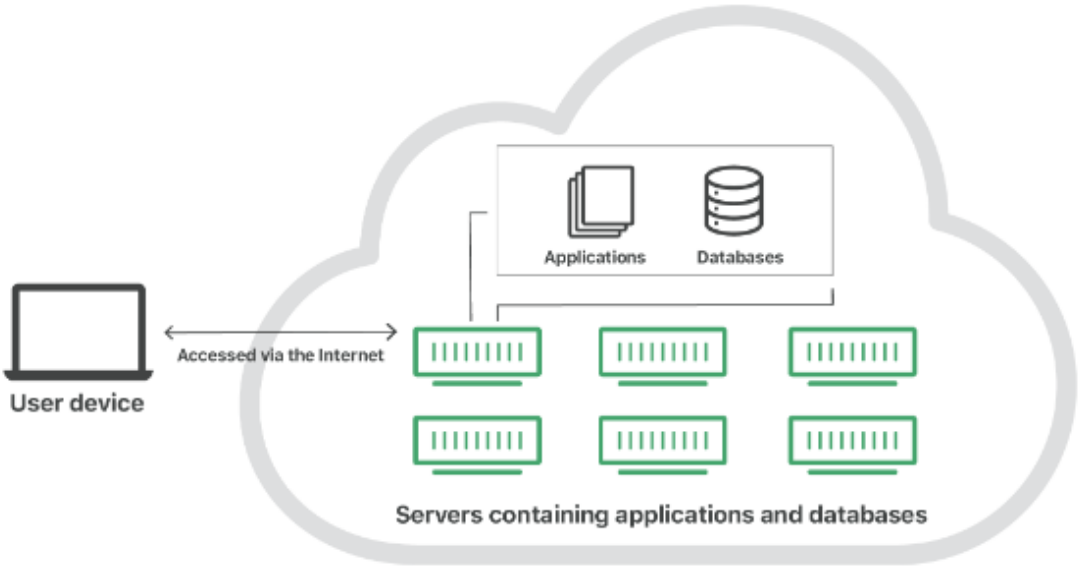
PKI	Public Key Infrastructure
QoS	Quality of Service
RA	Registration Authority
RBAC	Role Based Access Control
REST API	REpresentational State Transfer API
SaaS	Software as a Service
SLA	Service Level Agreement
SLA	Service Level Agreement
SMI	Service Measurement Index
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPM	Statistical Parametric Mapping
SQL	Structured Query Language
SVM	Secure Virtual Machine
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Processing Module
TVDc	Trusted Virtual Datacenter
UC	Utility Computing
USF	University of San Francisco
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
XML	Extensible Markup Language
XSS	Cross-Site Scripting

1

Εισαγωγή

1.1 Η έννοια του υπολογιστικού νέφους

Το υπολογιστικό νέφος (cloud computing) αναφέρεται σε διακομιστές στους οποίους γίνεται πρόσβαση μέσω διαδικτύου, καθώς και στο λογισμικό και τις βάσεις δεδομένων που εκτελούνται σε αυτούς τους διακομιστές. Οι διακομιστές νέφους βρίσκονται σε κέντρα δεδομένων σε όλο τον κόσμο. Χρησιμοποιώντας το υπολογιστικό νέφος, οι χρήστες και οι εταιρείες δεν χρειάζεται να διαχειρίζονται οι ίδιοι φυσικούς διακομιστές ή να εκτελούν εφαρμογές λογισμικού στα δικά τους μηχανήματα.[1]



Εικόνα 1: Το υπολογιστικό νέφος

Το υπολογιστικό νέφος επιτρέπει στους χρήστες να έχουν πρόσβαση στα ίδια αρχεία και εφαρμογές από σχεδόν οποιαδήποτε συσκευή, επειδή ο υπολογισμός και η αποθήκευση πραγματοποιούνται σε διακομιστές σε ένα κέντρο δεδομένων, αντί τοπικά στη συσκευή του χρήστη.

Για τις επιχειρήσεις, η μετάβαση στο νέφος αφαιρεί ορισμένα κόστη πληροφορικής και γενικά έξοδα: για παράδειγμα, δεν χρειάζεται πλέον να ενημερώνουν και να συντηρούν τους δικούς τους διακομιστές, καθώς θα το κάνει ο πάροχος νέφους τον οποίο χρησιμοποιούν. Αυτό έχει αντίκτυπο ιδιαίτερα στις μικρές επιχειρήσεις που μπορεί να μην ήταν σε θέση να αντέξουν οικονομικά τη δική τους εσωτερική υποδομή, αλλά μπορούν να αναθέσουν σε εξωτερικούς συνεργάτες τις ανάγκες υποδομής τους μέσω του νέφους. Το νέφος μπορεί επίσης να διευκολύνει τις εταιρείες να λειτουργούν διεθνώς, επειδή οι εργαζόμενοι και οι πελάτες μπορούν να έχουν πρόσβαση στα ίδια αρχεία και εφαρμογές από οποιαδήποτε τοποθεσία.

1.2 Πώς λειτουργεί το υπολογιστικό νέφος

Το υπολογιστικό νέφος λειτουργεί πάνω σε μια τεχνολογία που ονομάζεται εικονικοποίηση (virtualization). Η εικονικοποίηση επιτρέπει τη δημιουργία ενός προσομοιωμένου, ψηφιακού «εικονικού» υπολογιστή που συμπεριφέρεται σαν να ήταν ένας φυσικός υπολογιστής με το δικό του υλικό. Ο τεχνικός όρος για έναν τέτοιο υπολογιστή είναι εικονική μηχανή (Virtual Machine). Όταν υλοποιούνται σωστά, οι εικονικές μηχανές στον ίδιο κεντρικό υπολογιστή τοποθετούνται διαφορετικά σε sandbox[1] η μία από την άλλη, επομένως δεν αλληλεπιδρούν καθόλου μεταξύ τους. Τα αρχεία και οι εφαρμογές από μια εικονική μηχανή δεν είναι ορατά στις άλλες εικονικές μηχανές, παρόλο που βρίσκονται σε την ίδια φυσική μηχανή.

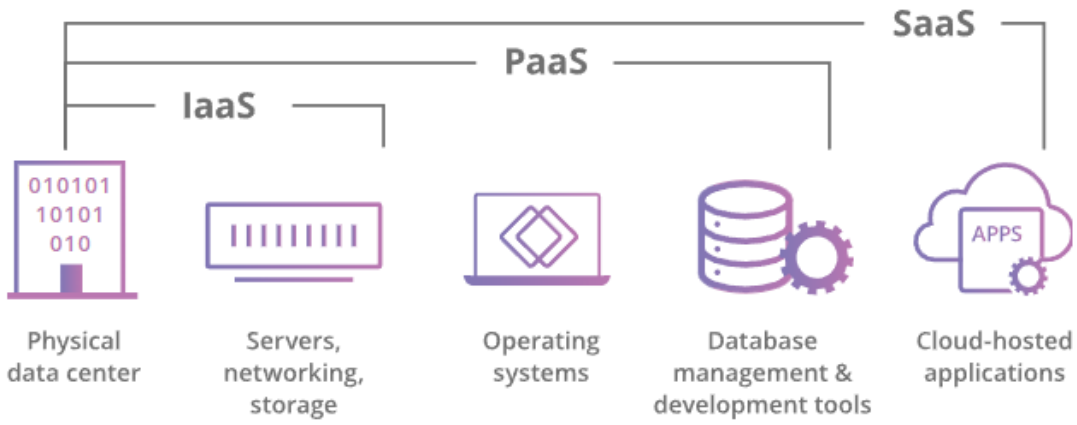
Οι εικονικές μηχανές κάνουν επίσης πιο αποτελεσματική χρήση του υλικού που τις φιλοξενεί. Με την εκτέλεση πολλών εικονικών μηχανών ταυτόχρονα, ένας διακομιστής γίνεται «πολλοί διακομιστές» και ένα κέντρο δεδομένων γίνεται μια

[1] Απομονωμένο υπολογιστικό περιβάλλον όπου ένα πρόγραμμα εκτελείται χωρίς να έχει πρόσβαση σε ολόκληρο τον υπολογιστή για λόγους ασφαλείας και δοκιμών.

ολόκληρη σειρά από κέντρα δεδομένων, ικανά να εξυπηρετήσουν πολλούς οργανισμούς. Έτσι, οι πάροχοι μπορούν να προσφέρουν τη χρήση των διακομιστών τους σε πολύ περισσότερους πελάτες ταυτόχρονα από ό,τι θα μπορούσαν διαφορετικά, και μπορούν να το κάνουν με χαμηλό κόστος.

Ακόμα κι αν μεμονωμένοι διακομιστές σταματήσουν να λειτουργούν, οι διακομιστές νέφους γενικά είναι πάντα συνδεδεμένοι και πάντα διαθέσιμοι. Οι πάροχοι δημιουργούν αντίγραφα ασφαλείας των υπηρεσιών τους σε πολλαπλά μηχανήματα και σε πολλές περιοχές.

1.3 Κύριες υπηρεσίες του υπολογιστικού νέφους



Εικόνα 2: Κύριες υπηρεσίες νέφους

- **Infrastructure-as-a-Service (IaaS):** Σε αυτό το μοντέλο, μια εταιρεία νοικιάζει τους διακομιστές και τον χώρο αποθήκευσης που χρειάζεται από έναν πάροχο. Στη συνέχεια χρησιμοποιεί αυτήν την υποδομή για να δημιουργήσει τις εφαρμογές της. Το IaaS είναι σαν μια εταιρεία που μισθώνει ένα οικόπεδο στο οποίο μπορεί κάποιος να χτίσει ό,τι θέλει — αλλά πρέπει να παρέχει τον δικό του δομικό εξοπλισμό και υλικά. Οι πάροχοι IaaS περιλαμβάνουν τις DigitalOcean, Google Compute Engine και OpenStack. Παλαιότερα, τα SaaS, PaaS και IaaS ήταν τα τρία κύρια μοντέλα υπολογιστικού νέφους και ουσιαστικά όλες οι υπηρεσίες νέφους χωρούσαν σε μία από αυτές τις κατηγορίες.

- **Platform-as-a-Service (PaaS):** Σε αυτό το μοντέλο, οι εταιρείες δεν πληρώνουν για φιλοξενούμενες εφαρμογές. Αντίθετα πληρώνουν για τα πράγματα που χρειάζονται για να δημιουργήσουν τις δικές τους εφαρμογές. Οι προμηθευτές PaaS προσφέρουν όλα τα απαραίτητα για τη δημιουργία μιας εφαρμογής, συμπεριλαμβανομένων εργαλείων ανάπτυξης, υποδομής και λειτουργικών συστημάτων, μέσω του διαδικτύου. Το PaaS μπορεί να συγκριθεί με την ενοικίαση όλων των εργαλείων και του εξοπλισμού που απαιτούνται για την κατασκευή ενός σπιτιού, αντί της ενοικίασης του ίδιου του σπιτιού. Παραδείγματα PaaS παρόχων περιλαμβάνουν το Heroku και το Microsoft Azure.

- **Software-as-a-Service (SaaS):** Αντί οι χρήστες να εγκαθιστούν μια εφαρμογή στη συσκευή τους, οι εφαρμογές SaaS φιλοξενούνται σε διακομιστές νέφους και οι χρήστες έχουν πρόσβαση σε αυτές μέσω διαδικτύου. Το SaaS είναι σαν την ενοικίαση ενός σπιτιού: ο ιδιοκτήτης διατηρεί το σπίτι, αλλά ο ενοικιαστής συνήθως το χρησιμοποιεί σαν να του ανήκει. Παραδείγματα εφαρμογών SaaS περιλαμβάνουν τα Salesforce, MailChimp και Slack [2].

- **Function-as-a-Service (FaaS):** Το FaaS, γνωστό και ως υπολογισμός χωρίς διακομιστή, διασπά τις εφαρμογές νέφους σε ακόμη μικρότερα στοιχεία που εκτελούνται μόνο όταν χρειάζονται. Το FaaS μοιάζει με την ενοικίαση ενός δωματίου από ένα σπίτι: για παράδειγμα, ο ενοικιαστής πληρώνει μόνο για την τραπεζαρία την ώρα του δείπνου, την κρεβατοκάμαρα ενώ κοιμάται, το σαλόνι ενώ βλέπει τηλεόραση και όταν δεν χρησιμοποιούνται αυτά τα δωμάτια, δεν χρειάζεται να πληρώνει ενοίκιο για αυτά. Οι εφαρμογές FaaS ή εφαρμογές χωρίς διακομιστή εκτελούνται και αυτές σε διακομιστές, όπως και όλα τα μοντέλα υπολογιστικού νέφους. Αλλά ονομάζονται «χωρίς διακομιστή» επειδή δεν εκτελούνται σε αποκλειστικά μηχανήματα και επειδή οι εταιρείες που κατασκευάζουν τις εφαρμογές δεν χρειάζεται να διαχειρίζονται κανέναν διακομιστή. Επίσης, οι λειτουργίες χωρίς διακομιστή αυξάνονται ή επαναλαμβάνονται, καθώς περισσότεροι άνθρωποι χρησιμοποιούν την εφαρμογή.

2

Λόγοι μετάπτωσης στο υπολογιστικό νέφος

2.1 Εισαγωγή στο υπολογιστικό νέφος

Χωρίς αμφιβολία, το υπολογιστικό νέφος προσφέρει πλεονεκτήματα για τις επιχειρησιακές λειτουργίες:

- Μπορεί να συμβάλει στη μείωση του κόστους (για παράδειγμα, ρυθμίζοντας και διαμορφώνοντας ένα testbed[2] εφαρμογών ή παρέχοντας τη δυνατότητα πρόσθεσης και αφαίρεσης υπολογιστικής ισχύος όταν είναι αναγκαίο).
- Βοηθά στην επεξεργασία μεγάλων συνόλων δεδομένων πιο γρήγορα (εξισορροπώντας τον φόρτο εργασίας όπου και όταν χρειάζεται).
- Μπορεί να βοηθήσει έναν οργανισμό να ανταποκριθεί πιο γρήγορα στις μεταβαλλόμενες συνθήκες (με το να είναι σε θέση να εφαρμόζει επιχειρηματικά αναλυτικά πλάνα σε μεγαλύτερους όγκους δεδομένων με πιο γρήγορο τρόπο).

Υπάρχουν πολλοί παράγοντες ρίσκου, τεχνολογίας και επιχειρηματικών βλέψεων που μπορούν να έχουν βαθιά επίδραση στη συνολική επιτυχία των πρωτοβουλιών που

[2] Είναι ένα περιβάλλον εκτέλεσης το οποίο έχει ρυθμιστεί για δοκιμή. Το testbed αποτελείται από συγκεκριμένο υλικό, λογισμικό, λειτουργικό σύστημα, ρυθμίσεις δικτύου, το υπό δοκιμή προϊόν καθώς και άλλα λογισμικά απαραίτητα για τις δοκιμές.

έχουν να κάνουν με το νέφος σε έναν οργανισμό, πράγμα που σημαίνει ότι δεν υπάρχει μια ενιαία απάντηση για το εάν μια εφαρμογή «ταιριάζει» στο νέφος. Κάθε επιχείρηση πρέπει να αξιολογήσει το χαρτοφυλάκιο εφαρμογών της με βάση τις δικές της επιχειρηματικές τακτικές, τη στρατηγική τεχνολογίας και την στρατηγική ανάληψης κινδύνου [3].

Ένα από τα σημαντικά ζητήματα για τη μετάβαση στο νέφος είναι το ζήτημα της ασφάλειας στη χρήση τέτοιων υπηρεσιών. Αυτή η ασφάλεια περιλαμβάνει την ακεραιότητα των δεδομένων, την εμπιστευτικότητα και την προσβασιμότητα των δεδομένων [4], [5]. Οι απειλές για την ασφάλεια περιλαμβάνουν κακόβουλη δραστηριότητα και απώλεια εμπιστευτικότητας λόγω ανεπαρκούς χειρισμού δεδομένων.

Αυτός είναι ο λόγος για τον οποίο το θέμα της αξιολόγησης των κινδύνων γίνεται ακόμη πιο καίριο. Ένας σημαντικός αριθμός μελετών είναι αφιερωμένος σε αυτή την πτυχή, η πλειονότητα των οποίων περιγράφει τους κινδύνους εισαγωγής τεχνολογιών πληροφοριών, αλλά δεν καλύπτουν τις ιδιαιτερότητες της μετάβασης στο νέφος. Για παράδειγμα, τα μοντέλα κινδύνου Octave, Cramm και RiskWatch δεν λαμβάνουν υπόψη τον ειδικό χαρακτήρα του μοντέλου αλληλεπίδρασης (interface), με τα περιβάλλοντα νέφους, και συγκεκριμένα τη δυνατότητα απομακρυσμένης πρόσβασης στις υπηρεσίες. Επιπλέον, αυτές οι μέθοδοι παρέχουν μόνο ποιοτική αξιολόγηση του κινδύνου. Στο [6] οι συγγραφείς προτείνουν ένα ποσοτικό μοντέλο αξιολόγησης ασφάλειας των εφαρμογών νέφους, το οποίο επιτρέπει στους παρόχους και τους πελάτες να προσδιορίζουν το ύψος του κινδύνου που αναλαμβάνουν. Η απόφαση σύμφωνα με αυτή τη μέθοδο λαμβάνεται με βάση λεπτομερείς ποσοτικές αναλύσεις κινδύνων, και όχι βάσει ψυχολογικών παραγόντων (φόβος, φοβία, αντίληψη). Το πλεονέκτημα της μεθόδου έγκειται στο γεγονός ότι λαμβάνει υπόψη τον ετερογενή χαρακτήρα των απαιτήσεων ασφαλείας, την αρχιτεκτονική του συστήματος, τις απειλές και τη δραστηριότητα του εισβολέα.

Αξίζει να σημειωθεί ότι η αξιολόγηση του κινδύνου εισαγωγής εφαρμογών νέφους δεν είναι η μόνη πτυχή που επηρεάζει τη διαδικασία λήψης αποφάσεων σχετικά με τη μεταφορά των εταιρικών εφαρμογών στο νέφος. Για παράδειγμα, είναι σημαντικό να αξιολογηθεί η λογικότητα της μετάβασης από την άποψη της επιχειρηματικής αξίας των εφαρμογών για μια επιχείρηση και των διαφόρων τεχνικών δυνατοτήτων. Αυτό το ζήτημα δεν εξετάζεται στις προαναφερθείσες μεθόδους. Επιπλέον, κατά τη λήψη απόφασης σχετικά με τη μετάβαση του υπολογιστικού περιβάλλοντος της εταιρείας

στο νέφος, η ευκαιρία να αξιολογηθεί κατά πόσο η μετακίνηση ευσταθεί είναι σημαντική, επειδή οι εταιρείες λειτουργούν συχνότερα σε συνθήκες έλλειψης προϋπολογισμού πληροφορικής και πρέπει να είναι επιλεκτικές κατά τον εντοπισμό εφαρμογών για μετάβαση.

2.2 Infrastructure as a Service (IaaS)

Το Infrastructure-as-a-Service (IaaS) μπορεί να οριστεί ως η χρήση διακομιστών, αποθήκευσης και εικονικοποίησης για την παροχή υπηρεσιών παρόμοιες με καθημερινές, χρήσιμες εφαρμογές για χρήστες. Η υποδομή αποτελείται από την εγκατάσταση, τα δίκτυα επικοινωνίας, τους φυσικούς κόμβους υπολογισμού και τη δεξαμενή εικονικών υπολογιστικών πόρων που διαχειρίζεται ένας πάροχος υπηρεσιών.

Ο σκελετός της υπηρεσίας αποτελείται από στοιχεία που υπάγονται στον έλεγχο του χρήστη και περιλαμβάνει τις εικονικές μηχανές με τα λειτουργικά τους συστήματα, την αποθήκευση και τη διαχείριση αυτών [11]. Το IaaS παρέχει στους χρήστες μια υπηρεσία βασισμένη στον ιστό που μπορεί να χρησιμοποιηθεί για τη δημιουργία, την καταστροφή και τη διαχείριση εικονικών μηχανών και αποθήκευσης. Μπορεί να χρησιμοποιηθεί για τη μέτρηση της χρήσης πόρων για μια χρονική περίοδο, η οποία με τη σειρά της μπορεί να χρεωθεί στους χρήστες στην προσυμφωνημένη τιμή. Απαλλάσσει τους χρήστες από την ευθύνη διαχείρισης της φυσικής και εικονικής υποδομής, ενώ διατηρεί τον έλεγχο του λειτουργικού συστήματος, της διαμόρφωσης και του λογισμικού που εκτελείται στις εικονικές μηχανές.

Μία από τις προκλήσεις που αντιμετωπίζει σήμερα η διοίκηση ενός οργανισμού είναι η απόφαση να λειτουργήσει ένα αυτοδιαχειριζόμενο ιδιωτικό νέφος (private cloud) εσωτερικής εγκατάστασης, είτε να εγγραφεί σε μια φιλοξενούμενη υπηρεσία (hosted service) ή κάποιο συνδυασμό των δύο. Σύμφωνα με τις παρατηρήσεις του Oppenheimer, η αυτοφιλοξενία (self-hosting) της υποδομής μπορεί να είναι πιο οικονομική για ανάγκες μεγάλου εύρους ζώνης και τον υπολογισμό των εντατικών φορτίων, ενώ το αντίθετο φαίνεται να ισχύει για την ελαφριά και διακοπτόμενη χρήση [12]. Παρά τον φόρτο εργασίας, υπάρχουν ακόμη άλλοι παράγοντες που πρέπει να ληφθούν υπόψη, συμπεριλαμβανομένων των πολιτικών ασφαλείας, της διακυβέρνησης

(data governance), της φυσικής τοποθεσίας των δεδομένων και ούτω καθεξής, όταν λαμβάνεται η απόφαση για μια φιλοξενούμενη ή αυτοφιλοξενούμενη λύση.

Η ασφάλεια είναι μια μεγάλη ανησυχία στο IaaS, ειδικά αν σκεφτεί κανείς ότι τα υπόλοιπα μοντέλα υπηρεσιών νέφους τρέχουν πάνω από αυτή την υποδομή και τα σχετικά επίπεδα. Σε ένα κοινό περιβάλλον, μια εταιρεία μπορεί να φιλοξενεί φόρτους εργασίας και δεδομένα πολλών άλλων εταιρειών. Σε αυτές τις περιπτώσεις, μπορεί να εκθέσει όλα τα μέρη σε υψηλότερο κίνδυνο που σχετίζεται με την ασφάλεια ή το απόρρητο. Για παράδειγμα, χρησιμοποιώντας εικονικοποίηση, ο hypervisor[3] έχει προνομιακή πρόσβαση στους φυσικούς πόρους του υλικού. Ενώ ένας διαχειριστής συστημάτων μπορεί να μην έχει πρόσβαση στο λειτουργικό σύστημα που εκτελείται μέσα στην εικονική μηχανή ενός πελάτη, όπως εξηγείται από τους Dawoud et al., ορισμένοι hypervisors έχουν πρόσβαση σε ένα προνομιούχο domain[4] που μπορεί να πέσει θύμα επίθεσης προκειμένου να αποκτηθεί πρόσβαση στην ενεργή μνήμη μιας εικονικής μηχανής [13]. Σε περίπτωση που ένας hypervisor έχει παραβιαστεί, μπορεί να είναι δυνατή η υποκλοπή των περιεχομένων της μνήμης, της κίνησης εικονικού δικτύου και άλλων μορφών επικοινωνίας που συμβαίνουν στο πεδίο ελέγχου του [13].

Η προσεκτική ανάθεση ρόλων στο προσωπικό, συμπεριλαμβανομένης της λεπτομερούς καταγραφής δικαιωμάτων, και η εφαρμογή της αρχής ασφαλείας των ελάχιστων προνομίων (least privilege policy) θα ήταν μια καλή αρχή για την αντιμετώπιση των προκλήσεων ασφαλείας της πλατφόρμας. Μπορεί επίσης να είναι επωφελής η εξάλειψη ή η αλλαγή του σκοπού των προνομιακών ομάδων χρηστών έτσι ώστε να μετριαστεί ο κίνδυνος κατασκοπείας του hypervisor από το backend[5]. Όσον αφορά στο δίκτυο επικοινωνίας, η κρυπτογράφηση των δεδομένων που πρέπει να ασφαλιστούν εντός του λειτουργικού συστήματος του επισκέπτη (guest), όπως με τη χρήση VPN, μπορεί να είναι επωφελής για την προστασία από τυχόν τρέχοντα ή μελλοντικά exploit[6] στο επίπεδο εικονικοποίησης [13].

[3] Ένας hypervisor ή VMM (Virtual Machine Monitor), είναι λογισμικό που δημιουργεί και εκτελεί εικονικές μηχανές (VM). Ένας hypervisor επιτρέπει σε έναν κεντρικό υπολογιστή να υποστηρίζει πολλαπλά Guest VMs μοιράζοντας εικονικά τους πόρους του, όπως τη μνήμη και την επεξεργαστική ισχύ.

[4] Αναφέρεται σε ένα διαμορφώσιμο σύνολο πόρων, συμπεριλαμβανομένης της μνήμης, των εικονικών CPU, των συσκευών δικτύου και των συσκευών δίσκου, στις οποίες εκτελούνται εικονικές μηχανές.

[5] Το backend αναφέρεται σε τμήματα μιας εφαρμογής ή στον κώδικα ενός προγράμματος που του επιτρέπουν να λειτουργεί και στα οποία δεν μπορεί να έχει πρόσβαση ο χρήστης.

[6] Ένα exploit είναι ένα κομμάτι λογισμικού, ένα κομμάτι δεδομένων ή μια ακολουθία εντολών που εκμεταλλεύεται ένα σφάλμα ή μια ευπάθεια σε μια εφαρμογή ή ένα σύστημα για να προκαλέσει ακούσια ή απρόβλεπτη συμπεριφορά.

2.2.1 Η περίπτωση του Cloud-Enabled Space Weather Platform (CESWP)

Ως προς τις ανάγκες της εργασίας, έχει ενδιαφέρον ένα case study που σχετίζεται με το IaaS, όπως περιγράφεται από τους Toews, et al.. Η μελέτη αφορούσε ένα έργο για τη δημιουργία ενός περιβάλλοντος κοινότητας (community environment) ή υβριδικού νέφους για μια διεθνή ομάδα φυσικών. Αυτοί οι επιστήμονες χρειάζονταν πρόσβαση σε υπολογιστική ισχύ για να σχεδιάσουν, να αναπτύξουν και να προσομοιώσουν διάφορα μοντέλα. Χρησιμοποιώντας τις υπάρχουσες διαδικασίες τους οι φυσικοί, παρατήρησαν αρκετές προκλήσεις τις οποίες το έργο προσπάθησε να τα ξεπεράσει. Η ομάδα ανέπτυξε μια υποδομή νέφους που βασιζόταν στο μοντέλο υπηρεσιών IaaS. Ως πλαίσιο, επέλεξαν μια δέσμη λογισμικού που ονομάζεται Eucalyptus, η οποία ήταν συμβατή τόσο με τη διεπαφή (interface) προγραμματισμού εφαρμογών Kernel Virtual Machine (KVM) όσο και με τη διεπαφή προγραμματισμού εφαρμογών Amazon Web Services (AWS) [14]. Οι υπολογιστικοί κόμβοι για το νέφος διασκορπίστηκαν γεωγραφικά για να μειωθεί ο λανθάνοντας χρόνος (latency) και να βελτιωθεί η εμπειρία για τους τελικούς χρήστες που διέμεναν σε διάφορες χώρες σε όλο τον κόσμο. Επειδή το υλικό ήταν ομαδοποιημένο σε συμπλέγματα που μπορούσαν να μοιραστούν, εξάλειψε την ανάγκη να προμηθεύονται μεμονωμένους υπολογιστές κάθε φορά που προέκυπτε ανάγκη.

Αντίθετα, οι παροχές θα μπορούσαν να προστίθενται όποτε προέκυπτε ανάγκη στο σύνολο των πόρων του νέφους. Από την άποψη της συντήρησης, οι φυσικοί δεν χρειαζόταν πλέον να διατηρούν το δικό τους υλικό διακομιστή, καθώς τους πόρους του νέφους διαχειρίζονταν κεντρικά τα διάφορα ιδρύματα ως ένα ενιαίο σύμπλεγμα υπολογιστών. Ως αποτέλεσμα, οι ερευνητές είχαν πλέον πρόσβαση σε τεράστιους πόρους για να εκτελέσουν τις προσομοιώσεις τους αντί να περιμένουν τον υπολογισμό πλέγματος (grid computing). Εάν αυτοί οι πόροι δεν επαρκούσαν, θα μπορούσαν να αγοράσουν περισσότερους χρησιμοποιώντας τις Υπηρεσίες Ιστού της Amazon (Amazon Web Services). Η ομάδα δημιούργησε επίσης διάφορα εργαλεία διαχείρισης, όπως μια «εφαρμογή ιστού GUI (Graphical User Interface) [14]», η οποία ουσιαστικά επέτρεψε την «εκμετάλλευση» της υπηρεσίας του IaaS –με βάση τον προηγούμενο ορισμό– και διευκόλυνε τη χρήση του νέφους.

Σε αυτό το έργο, επέλεξαν να τρέξουν μόνο δύο συγκεκριμένα λειτουργικά συστήματα στις εικονικές μηχανές για να απλοποιήσουν τη διαχείριση και να παρέχουν ομοιομορφία. Οι χρήστες μπορούσαν να έχουν πρόσβαση στο νέφος μέσω πληθώρας συσκευών, όπως έξυπνα τηλέφωνα, ταμπλέτες και ούτω καθεξής.

Ένα από τα ζητήματα που αντιμετώπισε η ομάδα ήταν ο αριθμός των διαθέσιμων διευθύνσεων IPv4 που περιόριζε τον αριθμό των εικονικών μηχανών οι οποίες θα μπορούσαν να έχουν άμεση πρόσβαση μέσω του διαδικτύου. Παρατήρησαν επίσης ότι καθώς η δημοτικότητα και η ζήτηση για τις υπηρεσίες αυξανόταν, μπορεί τελικά να αντιμετωπίσουν ένα ζήτημα υπερσυνδρομής που θα έπρεπε να καταπολεμηθεί. Στο τέλος, δήλωσαν ότι το Eucalyptus δεν ήταν «κατάλληλο» για το περιβάλλον νέφους τους και θα επανεκτιμούσαν διάφορα διαθέσιμα πλαίσια για να βρουν κάτι πιο κατάλληλο [14].

Αυτή η συζήτηση για το IaaS και η περίπτωση που αναλύθηκε άνωθεν, είναι ένα παράδειγμα για το πώς το υπολογιστικό νέφος μπορεί να ωφελήσει μια κοινότητα και επίσης παρέχει μερικά μαθήματα. Για παράδειγμα, μπορεί να διευκολύνει τη συνεργασία μεταξύ διαφορετικών ατόμων και ομάδων καθώς ξεπερνά τις προκλήσεις που ταλαιπωρούσαν τις υπάρχουσες λύσεις, επιτρέπει την πρόσβαση σε τεράστιους υπολογιστικούς πόρους με αποτελεσματικό τρόπο ενώ ταυτόχρονα απλοποιεί τη διαχείριση μέσω κεντρικά διαχειριζόμενων web εφαρμογών με δυνατότητα απομακρυσμένης πρόσβασης. Όταν σχεδιάζεται μια λύση που βασίζεται στο νέφος, οι οργανισμοί πρέπει να δημιουργούν καλά καθορισμένους στόχους και να αξιολογούν τον τρόπο με τον οποίο αυτοί επιτυγχάνονται σε όλη τη διαδικασία ανάπτυξης και εφαρμογής. Εάν αυτά δεν εκπληρώνονται αποτελεσματικά, θα πρέπει να γίνει επανεκτίμηση για τις μελλοντικές λύσεις.

2.3 Platform as a Service (PaaS)

Οι πάροχοι πλατφόρμας ως υπηρεσία (PaaS) προσφέρουν πρόσβαση σε APIs (Application Programming Interfaces), γλώσσες προγραμματισμού και ενδιάμεσο λογισμικό ανάπτυξης που επιτρέπει στους συνδρομητές να αναπτύσσουν εφαρμογές χωρίς εγκατάσταση ή διαμόρφωση του περιβάλλοντος ανάπτυξης. Έχοντας χτιστεί πάνω στο IaaS, το PaaS απολαμβάνει πολλά από τα ίδια πλεονεκτήματα, όπως το Utility Computing (UC)[7], την εικονικοποίηση υλικού, δυναμική κατανομή πόρων και χαμηλό κόστος επένδυσης. Τα προρυθμισμένα περιβάλλοντα ανάπτυξης και το κοινόχρηστο ή εικονικό λογισμικό μειώνουν τον χρόνο εγκατάστασης, διαχείρισης και συντήρησης που απαιτείται από τους προγραμματιστές ενώ εξαλείφει και την ανάγκη για διαχειριστές συστήματος. Χρησιμοποιώντας τα εργαλεία που περιλαμβάνονται στην πλατφόρμα του υπολογιστικού νέφους, οι προγραμματιστές μπορούν να δημιουργήσουν εφαρμογές και υπηρεσίες που εκμεταλλεύονται το εικονικό υλικό, το data redundancy[8] και την υψηλή διαθεσιμότητα[9] (high availability). Μόλις ολοκληρωθεί η ανάπτυξη, η εφαρμογή μπορεί να παραδοθεί στους χρήστες μέσω του διαδικτύου [15]. Το Google App Engine, το Microsoft Azure και το SalesForce.com είναι παραδείγματα παρόχων PaaS.

Μια πρόκληση που συναντάται συχνά κατά τη χρήση του PaaS είναι η συμβατότητα. Δεν υπάρχει λίστα χαρακτηριστικών, γλωσσών, API, λογισμικού, τύπων βάσεων δεδομένων, εργαλείων ή ενδιάμεσων προγραμμάτων που να είναι κοινά σε όλους τους παρόχους PaaS [16], γεγονός που καθιστά δύσκολη την επιλογή ή την αλλαγή παρόχου [17]. Οι πλατφόρμες που βασίζονται στο νέφος μπορούν να κατηγοριοποιηθούν ως πλήρους ή μερικού PaaS. Το πλήρες PaaS προσφέρει στον πελάτη τη δυνατότητα να αναπτύσσει λύσεις εξ ολοκλήρου μέσω μιας διεπαφής χρήστη που βασίζεται στον ιστό χωρίς να χρειάζεται ο προγραμματιστής να εγκαταστήσει οτιδήποτε άλλο εκτός από έναν thin client, όπως ένα πρόγραμμα περιήγησης ιστού. Μερικοί πάροχοι παρέχουν έναν αριθμό εργαλείων στον πελάτη ως

[7] Το Utility Computing είναι ένα μοντέλο παροχής υπηρεσιών στο οποίο ένας πάροχος υπηρεσιών καθιστά διαθέσιμους στον πελάτη υπολογιστικούς πόρους, κατ' απαίτηση, και τον χρεώνει μόνο για τον χρόνο κατά τον οποίο χρησιμοποίησε τους πόρους.
[8] Το data redundancy προκύπτει όταν το ίδιο κομμάτι δεδομένων υπάρχει σε πολλά μέρη.
[9] Η υψηλή διαθεσιμότητα (HA) είναι ένα χαρακτηριστικό ενός συστήματος που στοχεύει να εξασφαλίσει ένα συμφωνημένο επίπεδο λειτουργικής απόδοσης, συνήθως χρόνο λειτουργίας. Οι μεγάλοι πάροχοι υπόσχονται πάνω από 99.9% διαθεσιμότητα.

υπηρεσία, αλλά εξακολουθούν να απαιτούν από τον χρήστη να εγκαταστήσει εφαρμογές και να αναπτύξει λύσεις στις δικές του συσκευές. Το πλήρες PaaS είναι ιδιαίτερα επιρρεπές σε ζητήματα συμβατότητας και στην πιθανότητα να «παγιδευτεί» ένας οργανισμός στον πάροχο υπολογιστικού νέφους, αλλά, απαιτεί τη μικρότερη ποσότητα διαχείρισης και συντήρησης – από τις δύο κατηγορίες – και είναι έτοιμο για χρήση με τη συνδρομή.

Μια δεύτερη ανησυχία για τους πελάτες του PaaS είναι ότι οι προγραμματιστές λογισμικού παραμένουν επιφυλακτικοί όσον αφορά την επένδυση στην ανάπτυξη πάνω σε νέες πλατφόρμες καθώς και ως προς την εκμάθηση νέων API, επειδή εξακολουθούν να εξελίσσονται γρήγορα και το μέλλον ενός παρόχου μπορεί να είναι αβέβαιο. Αυτές οι ανησυχίες θα πρέπει να αμβλυνθούν με την πάροδο του χρόνου, καθώς οι πάροχοι αποκτούν σταθερές επιδόσεις και δημοτικότητα.

Είναι επίσης πλέον δυνατή η χρήση πρόσθετου ενδιάμεσου λογισμικού και API (Cloud Foundry, OpenShift [18]) για την ανάπτυξη εφαρμογών σε πλατφόρμες ανεξάρτητες από τον πάροχο, οι οποίες στη συνέχεια επιτρέπουν στον χρήστη να επιλέξει σε ποιον πάροχο νέφους θα αναπτυχθεί η εφαρμογή του .

Όπως και στο IaaS, η ασφάλεια παραμένει επίσης μια έντονη ανησυχία όταν χρησιμοποιείται ένα μοντέλο PaaS. Τα public clouds περιορίζουν τη δυνατότητα του καταναλωτή να προστατεύει τα ιδιόκτητα δεδομένα του, όπως θα μπορούσαν με την εταιρική υποδομή, και να ελέγχει τη γεωγραφική θέση αποθήκευσής τους [19]. Οι πλατφόρμες πρέπει συχνά να φιλοξενούν (host) υπηρεσίες που έχουν αυξημένα προνόμια (elevated privileges) προκειμένου να λειτουργούν αποτελεσματικά. Αυτά πρέπει να περιορίζονται αυστηρά από τον πάροχο PaaS, έτσι ώστε να μην υπάρχει πιθανότητα ο τελικός χρήστης να αποκτήσει πρόσβαση στην πλατφόρμα, την κυκλοφορία δικτύου, τη μνήμη ή τα δεδομένα άλλου χρήστη.

Το λογισμικό PaaS υπάρχει τόσο ως αποκλειστική τεχνολογία (Google App Engine) όσο και ως τεχνολογία ανοιχτού κώδικα (OpenShift). Οι πλατφόρμες ανοιχτού κώδικα κερδίζουν δημοτικότητα και οι εταιρείες ανάπτυξης των τεχνολογιών αυτών καθιστούν όλο και περισσότερο τον πηγαίο κώδικα τους δημόσια διαθέσιμο. Οι πλατφόρμες ανοιχτού κώδικα επιτρέπουν μεγαλύτερο βαθμό ελέγχου της ασφάλειας ή τουλάχιστον επιτρέπουν τον ενδελεχή έλεγχο των ισχυόντων μέτρων ασφαλείας από τρίτους.

Ενώ οποιοσδήποτε πάροχος PaaS θα πρέπει να περιγράφει τις ευθύνες ασφαλείας του σε μια SLA (Service Level Agreement), συνιστάται ανεπιφύλακτα η

δοκιμή και ο έλεγχος ασφάλειας από τρίτους, ανεξάρτητα από τους ισχυρισμούς του παρόχου.

2.3.1 Η περίπτωση του University of Adelaide

Η έρευνα στη γεωφυσική παρέχει μια ενδιαφέρουσα περίπτωση για τη μετάβαση σε μια λύση υπολογιστικού νέφους. Η Magnetotellurics (MT) είναι μια μέθοδος που χρησιμοποιείται από γεωφυσικούς για τον χαρακτηρισμό της υπόγειας σύνθεσης αρκετά χιλιόμετρα μέσα στη γη [20]. Χρησιμοποιώντας συγκεντρωτικά δεδομένα και έναν ορισμένο βαθμό διακύμανσης, οι γεωλογικοί εξερευνητές είναι σε θέση να δημιουργήσουν μια τρισδιάστατη χαρτογράφηση μιας υπόγειας περιοχής με τη βοήθεια λογισμικού και αλγορίθμων. Αυτό παρέχει μια πολύ πιο ακριβή εκτίμηση για τη θέση των γεωθερμικών πηγών, των ορυκτών και των υπόγειων υδάτινων οδών από προηγούμενες μεθόδους και δεν απαιτεί γεώτρηση για δείγματα.

Ωστόσο, οι αλγόριθμοι MT ενδέχεται να χρειαστούν αρκετές εβδομάδες για να ολοκληρωθούν με χρήση επιτραπέζιων υπολογιστών με έναν επεξεργαστή, μια σημαντική καθυστέρηση, ιδιαίτερα όταν ένα σύνολο δεδομένων τίθεται σε επεξεργασία πολλές φορές χρησιμοποιώντας προσαρμοσμένες μεταβλητές για να επιτευχθεί μια πιο εκλεπτυσμένη χαρτογράφηση. Ο μεγάλος όγκος δεδομένων σε συνδυασμό με την πολυπλοκότητα των υπολογισμών MT απαιτεί μεγάλο όγκο υπολογιστικών πόρων.

Ερευνητές στο Πανεπιστήμιο της Αδελαΐδας στην Αυστραλία είδαν τη δυνατότητα χρήσης IaaS για τη μείωση του χρόνου υπολογισμού της διαδικασίας χαρτογράφησης MT και επίσης το πλεονέκτημα της δυνατότητας εκτέλεσης των υπολογισμών από απομακρυσμένες τοποθεσίες μέσω διαδικτύου. Το υπάρχον πρόγραμμα FORTRAN που χρησιμοποιούσαν στο πανεπιστήμιο, περίπου 22.000 γραμμές κώδικα, μετατράπηκε σε μια εφαρμογή που υποστήριζε παράλληλη επεξεργασία και μπορούσε να εκτελεστεί AWS, την υπηρεσία υπολογιστικού νέφους IaaS της Amazon, καθώς και στο Microsoft Azure (το μοντέλο PaaS της Microsoft). Με το να μπορούν να

εκτελούν το πρόγραμμα παράλληλα και να κάνουν χρήση των υπολογιστικών πόρων IaaS, οι ερευνητές κατάφεραν να μειώσουν τον μέσο χρόνο επεξεργασίας στο ¼ του αρχικού, πράγμα που σημαίνει ότι τα αποτελέσματα μπορούσαν να ληφθούν σε ημέρες και όχι σε εβδομάδες, και επίσης κέρδισαν τη δυνατότητα εκτέλεσης πολλαπλών υπολογισμών MT ταυτόχρονα. Κατά τη μετάβαση στο νέφος υιοθέτησαν μια διεπαφή ιστού, η οποία ενίσχυσε περαιτέρω τη δυνατότητα χρήσης της λύσης.

Η μελέτη της συγκεκριμένης περίπτωσης καταδεικνύει ότι τα μοντέλα υπηρεσιών νέφους προσφέρουν μια εξαιρετική εναλλακτική σε μια ιδιόκτητη υπολογιστική υποδομή όταν εξετάζεται μια λύση που περιλαμβάνει διακοπτόμενους υπολογισμούς και μεγάλες απαιτήσεις πόρων. Παρόλο που η συμβατότητα μπορεί να είναι ένα πρόβλημα και η εκμάθηση νέων API απαιτεί κάποια επένδυση, αυτές οι ανησυχίες είναι παρόμοιες με αυτές που δημιουργούνται κάθε φορά που προκύπτει η ανάγκη για αναβάθμιση εφαρμογών παλαιού τύπου (legacy).

Παρόλο που οι προγραμματιστές του έργου υπολογισμού MT ήταν νέοι στην αρχιτεκτονική νέφους και επίσης δεν ήταν εξοικειωμένοι με την υπάρχουσα διαδικασία, κατάφεραν να εκπληρώσουν τους στόχους του έργου έγκαιρα και να επιτύχουν εξαιρετικά αποτελέσματα. Οι ανησυχίες των προγραμματιστών για την ασφάλεια σε πλατφόρμες υπολογιστικού νέφους δεν διαφέρουν από αυτές της παραδοσιακής ανάπτυξης όπου είναι δυνατή η εξωτερική πρόσβαση. Οι προγραμματιστές είναι υπεύθυνοι για τη σύνταξη ασφαλών εφαρμογών και οι εφαρμογές πρέπει να ελέγχονται διεξοδικά, ιδανικά από τρίτους. Τα μοντέλα πλήρους PaaS υιοθετούν στην πραγματικότητα την πλειονότητα των ανησυχιών ασφαλείας που σχετίζονται με την ανάπτυξη μιας λύσης στον πάροχο νέφους. Στην πραγματικότητα, η πλειονότητα των ανησυχιών για την ασφάλεια και το απόρρητο ειδικά για το υπολογιστικό νέφος θα πρέπει να είναι ευθύνη του παρόχου και αυτές οι ανησυχίες θα πρέπει να αντιμετωπιστούν στο εγγύς μέλλον καθώς η τυποποίηση συνεχίζεται και οι πελάτες απαιτούν περισσότερα σε επίπεδο SLA.

2.4 Software as a Service (SaaS)

Το Software-as-a-Service παρέχει στους συνδρομητές πρόσβαση σε λογισμικό ή υπηρεσίες που βρίσκονται στο νέφος και όχι στη συσκευή του χρήστη. Ο καταναλωτής μιας εφαρμογής SaaS χρειάζεται να τρέχει κάποιο thin-client λογισμικό, όπως ένα πρόγραμμα περιήγησης ιστού για πρόσβαση στην εφαρμογή που φιλοξενείται στο νέφος. Αυτό μειώνει τις απαιτήσεις υλικού για τους τελικούς χρήστες και επιτρέπει τον κεντρικό έλεγχο, την ανάπτυξη και τη συντήρηση του λογισμικού. [7].

Η ευελιξία μιας εφαρμογής που βασίζεται στο SaaS με κεντρική αποθήκευση δεδομένων μπορεί να εξαλείψει την ανάγκη των εργαζομένων να μεταφέρουν ευαίσθητα δεδομένα μαζί τους όταν ταξιδεύουν. Άλλα οφέλη ασφαλείας περιλαμβάνουν κοινό κόστος δοκιμών ασφαλείας, την ευκολία δημιουργίας ιστορικού ασφαλείας (security records), ασφαλείς εκδόσεις και ένα πιο αποτελεσματικά ρυθμισμένο σύστημα.

Ωστόσο, η βαθύτερη έρευνα καταλήγει στο συμπέρασμα ότι μαζί με την πιθανή εξοικονόμηση κόστους μιας λύσης SaaS, οι προκλήσεις μπορούν να γίνουν ένα κρίσιμο ζήτημα κατά την πραγματοποίηση μιας τέτοιας αλλαγής. Η Hurwitz & Associates κατέληξε επίσης στο συμπέρασμα ότι η εξοικονόμηση ενός μοντέλου SaaS μειώθηκε καθώς αυξανόταν ο αριθμός των εργαζομένων [7]. Επιπλέον, μια λύση SaaS προκαλεί επίσης πολλές ανησυχίες καθώς σχετίζεται με την ασφάλεια των εταιρικών δεδομένων. Το NetworkWorld παραπέμπει σε κανονισμούς όπως ο Federal Information Security Management Act που απαιτεί από τους πελάτες να διατηρούν ευαίσθητα δεδομένα εντός της χώρας (για εταιρείες με έδρα τις Ηνωμένες Πολιτείες) [8]. Ενώ η πρόσβαση σε δεδομένα από οπουδήποτε είναι βολική και μειώνει την ανάγκη των υπαλλήλων της επιχείρησης να μεταφέρουν ευαίσθητες πληροφορίες μαζί τους, ένα μη ασφαλές τελικό σημείο (endpoint) μπορεί να είναι μεγάλος κίνδυνος.

Για να κατανοήσει και να μετριάσει τους κινδύνους αυτών των ανησυχιών για την ασφάλεια, μια επιχείρηση που εξετάζει μια λύση SaaS πρέπει να κάνει τις σωστές ερωτήσεις όταν ερευνά έναν πάροχο. Η Messmer προτείνει ερωτήσεις όπως: Ποιοι υπάλληλοι του SaaS έχουν πρόσβαση επιπέδου διαχειριστή στη βάση δεδομένων; Τα δεδομένα διατηρούνται κρυπτογραφημένα; Διαχωρίζονται τα δεδομένα πελάτη; Ποιοι έλεγχοι ασφαλείας υπάρχουν; Ποιες είναι οι συμφωνίες υπηρεσιών (service level agreements); Ποιες πληροφορίες καταγράφονται στα αρχεία καταγραφής ελέγχου; Η

κατανόηση των πολιτικών ασφαλείας του παρόχου θα είναι κρίσιμη στη διαδικασία λήψης αποφάσεων.

2.4.1 Η περίπτωση του USF

Το USF (University of San Francisco) είναι το παλαιότερο πανεπιστήμιο της πόλης του Σαν Φρανσίσκο που αποτελείται από έξι πανεπιστημιουπόλεις που απασχολούν 1300 υπαλλήλους και αυτή τη στιγμή έχει εγγεγραμμένους πάνω από 8500 φοιτητές. Το πανεπιστήμιο υποστηρίζει επί του παρόντος πάνω από 1000 φορητές συσκευές μεταξύ των οποίων χρήστες εντός του φυσικού κτιρίου, χρήστες κινητών τηλεφώνων, απομακρυσμένους χρήστες φορητών υπολογιστών κ.α. [9]. Το USF εντόπισε μια σειρά από ανάγκες όσον αφορά την προστασία δεδομένων. Η πρώτη ήταν η παροχή αντιγράφων ασφαλείας κινητών συσκευών (laptops) στον τελικό χρήστη.

Οι χρήστες του USF είναι δημιουργοί δεδομένων μεγάλου όγκου με μεγάλο μέρος αυτών να βρίσκεται τοπικά στον υπολογιστή τους. Αυτά τα δεδομένα αποτελούν πνευματική ιδιοκτησία που απαιτείται να προστατεύεται. Επιπλέον, προσδιορίστηκε μια δεύτερη απαίτηση για τήρηση της νομοθεσίας της Καλιφόρνια που απαιτεί σε περίπτωση παραβίασης δεδομένων, κάθε επηρεαζόμενο άτομο να ειδοποιείται. Στην περίπτωση κλεμμένου φορητού υπολογιστή, μέχρι τότε, ήταν αδύνατο να γίνουν γνωστές αυτές τις πληροφορίες, καθώς τα δεδομένα που περιέχονταν στη συσκευή δεν ήταν ανακτήσιμα.

Μια άλλη ανάγκη που εντοπίστηκε ήταν η κατάλληλη προετοιμασία για την επανάκαμψη μετά από καταστροφή (disaster recovery). Δεδομένης της φυσικής του τοποθεσίας, το πανεπιστήμιο είχε βιώσει απώλεια της πανεπιστημιούπολης στο παρελθόν λόγω σεισμών και ως εκ τούτου αναγνωρίεζει την ανάγκη για αξιόπιστη υποστήριξη σε απομακρυσμένες περιοχές. Επίσης, εντοπίστηκε η αυξανόμενη ανάγκη για οικονομικά αποδοτικές λύσεις. [9].

Η παρούσα λύση πολλαπλών συστημάτων είχε πολλά μειονεκτήματα, συμπεριλαμβανομένου του υψηλού κόστους, των μεγάλων γενικών εξόδων διαχείρισης και της έλλειψης επαρκούς προστασίας δεδομένων τελικού χρήστη για φορητές συσκευές. Μια άλλη πρόκληση που εντοπίστηκε ήταν ο ρυθμός αύξησης των δεδομένων τελικού χρήστη που αντιμετώπιζε αυτήν τη στιγμή το USF. Έγινε προσπάθεια από το προσωπικό πληροφορικής του USF να εφαρμόσει μια εσωτερική λύση για την αντιμετώπιση αυτών των αναγκών, ωστόσο, μετά από σημαντική προσπάθεια, αυτή η λύση εφαρμόστηκε μόνο σε ένα μικρό ποσοστό χρηστών. Επιπλέον, αυτή η εσωτερική λύση δεν ήταν ικανή να ανταποκριθεί στους υψηλούς ρυθμούς δημιουργίας δεδομένων [9].

Με τις πρόσφατες εξελίξεις στις προσφορές Software-as-a-Service, το προσωπικό πληροφορικής της USF άρχισε να ερευνά λύσεις που βασίζονται στο νέφος. Μια εταιρεία που ονομάζεται Mozy επιλέχθηκε ως πάροχος SaaS για υπηρεσίες προστασίας δεδομένων. Η Mozy παρέχει υπηρεσίες προστασίας δεδομένων που βασίζονται στο νέφος για φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, διακομιστές και κινητές συσκευές. Η Mozy χρησιμοποιεί ένα pay-as-you-go μοντέλο που επέτρεψε στο USF να απολαμβάνει όλα τα οφέλη μιας λύσης SaaS, συμπεριλαμβανομένης της πληρωμής μόνο για ό,τι χρειάζεται (pay for what you need), ενώ χρεώσεις πραγματοποιήθηκαν μόνο την ημέρα έναρξης της υπηρεσίας για κάθε χρήστη. Για να αντιμετωπίσει τις ανησυχίες για την ασφάλεια των δεδομένων, η Mozy διαθέτει πέντε κέντρα δεδομένων παγκοσμίως, τα οποία επέτρεψαν την ευελιξία μεταξύ αναπαραγωγής δεδομένων και τοποθεσίας δεδομένων [9].

Μια επιχείρηση που κινείται προς μια λύση που βασίζεται στο νέφος μπορεί να αναμένει πολλές προκλήσεις και οφέλη. Πρέπει να διεξαχθεί ενδελεχής έρευνα για να διασφαλιστεί ότι ανησυχίες όπως η ασφάλεια των δεδομένων γίνονται σωστά κατανοητές και αντιμετωπίζονται. Στη μελέτη της περίπτωσης SaaS που παρουσιάστηκε, με την ανάπτυξη μιας λύσης προστασίας δεδομένων που βασίζεται στο SaaS, αυτός ο οργανισμός απολάμβανε πολλά από τα αναμενόμενα πλεονεκτήματα, όπως εξοικονόμηση κόστους, γρήγορη ανάπτυξη, χαμηλό αρχικό κόστος κεφαλαίου, διευρυμένες δυνατότητες και μια γρήγορη μέθοδο υλοποίησης των απαιτήσεων ενός έργου. Επιπλέον, επιλέγοντας μια λύση SaaS, ο οργανισμός βρίσκεται σε θέση να χειριστεί οποιαδήποτε ποσότητα νέων δεδομένων. Η μελέτη αυτής της

συγκεκριμένης περίπτωσης ήταν ένα καλό παράδειγμα μιας επιτυχημένης πραγματικής εφαρμογής υπολογιστών που βασίζεται σε νέφος και έδειξε ξεκάθαρα τις δυνατότητές του [10].

3

Θέματα ασφάλειας κατά τη μετάβαση στο νέφος

3.1 Τεχνικά προβλήματα

Οι νέες τεχνολογίες μαζί με τις υπηρεσίες νέφους και τα μοντέλα ανάπτυξης (deployment models) εισάγουν συγκεκριμένους κινδύνους και ευπάθειες για την ασφάλεια του νέφους εκτός από τους κοινούς κινδύνους με τη συμβατική IT υποδομή. Οι κίνδυνοι ασφάλειας στο υπολογιστικό νέφος μπορεί να διαφέρουν από τους κινδύνους της συμβατικής υποδομής πληροφορικής είτε ως προς τη φύση ή την ένταση είτε και τα δύο. Η συγκέντρωση πόρων (resource pooling) επιτρέπει τη χρήση της ίδιας δεξαμενής από πολλούς χρήστες μέσω πολλαπλών μισθώσεων και τεχνολογίες εικονικοποίησης. Αν και οι τεχνολογίες εισάγουν ταχεία ελαστικότητα και βέλτιστη διαχείριση των πόρων, εισάγουν επίσης ορισμένους κινδύνους στο σύστημα. Η πολλαπλή μίσθωση οδηγεί σε κινδύνους ορατότητας δεδομένων σε άλλους χρήστες.

Το χαρακτηριστικό αυτοεξυπηρέτησης κατ' απαίτηση (on-demand self service) παρέχεται στους πελάτες μέσω διεπαφών διαχείρισης που βασίζονται στο Web, μέθοδος η οποία αυξάνει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης στη διεπαφή διαχείρισης σε σχέση με τα παραδοσιακά συστήματα [21]. Ομοίως, το εικονικό περιβάλλον εισάγει το δικό του σύνολο κινδύνων και τρωτών σημείων που

περιλαμβάνει κακόβουλη συνεργασία μεταξύ εικονικών μηχανών (VM) και VM escape[10].

Αντίστοιχα, από την άποψη του μοντέλου υπηρεσίας του νέφους, τα μοντέλα υπηρεσιών εξαρτώνται το ένα από το άλλο. Οι εφαρμογές SaaS δημιουργούνται και αναπτύσσονται μέσω του PaaS και το PaaS εξαρτάται από το υποκείμενο IaaS. Αυτή η λειτουργική εξάρτηση των μοντέλων υπηρεσιών μεταξύ τους φέρνει και την εξάρτηση ασφαλείας. Για παράδειγμα, εάν ένας εισβολέας καταφέρει να πάρει τον έλεγχο του IaaS, το αποτέλεσμα θα είναι ένα παραβιασμένο PaaS που χρησιμοποιεί το IaaS. Ένα παραβιασμένο PaaS μπορεί να οδηγήσει σε παραβιασμένο SaaS. Εν ολίγοις, κάθε επίπεδο στην αρχιτεκτονική του νέφους δίνει πρόσβαση σε άλλα επίπεδα του μοντέλου.

Το μοντέλο ανάπτυξης ιδιωτικού νέφους κληρονομεί το ίδιο σύνολο τρωτών σημείων που διαθέτει η συμβατική υποδομή πληροφορικής. Ο λόγος είναι ότι το ιδιωτικό σύννεφο προορίζεται για τη χρήση ενός μόνο οργανισμού. Η παρουσία πολλών χρηστών που χρησιμοποιούν εικονικοποιημένους πόρους που μπορεί να αντιστοιχούν στον ίδιο φυσικό πόρο εισάγει πολλές ανησυχίες για την ασφάλεια. Ο τέλειος διαχωρισμός πολλών ενοικιαστών και κατανεμημένων πόρων είναι ένα πολύπλοκο έργο και χρειάζεται πολύ υψηλότερο επίπεδο ασφάλειας.

Ακολούθως παρουσιάζονται οι προκλήσεις ασφαλείας που αντιμετωπίζονται από το υπολογιστικό νέφος. Υπάρχουν πολυάριθμες εργασίες που εξετάζουν τις προκλήσεις ασφάλειας του νέφους από την άποψη του μοντέλου υπηρεσίας. Οι τρεις βασικότερες αφηρημένες περιοχές του νέφους στις οποίες εντοπίζονται προβλήματα ασφαλείας είναι: (α) αρχιτεκτονικά ζητήματα, (β) ζητήματα επικοινωνίας και (γ) συμβατικά και νομικά ζητήματα. Ορισμένες από τις τεχνολογίες στο υπολογιστικό νέφος δεν επηρεάζουν κάποιο συγκεκριμένο μοντέλο υπηρεσίας. Αντίθετα άλλες, επηρεάζουν περισσότερα από ένα μοντέλα, όπως η εικονικοποίηση που μπορεί να επηρεάσει τόσο το IaaS και PaaS.

[10] Στην ασφάλεια υπολογιστών, VM escape είναι η διαδικασία κατά την οποία ένα πρόγραμμα «βγαίνει» από την εικονική μηχανή στην οποία εκτελείται και αλληλεπιδρά με το λειτουργικό σύστημα του κεντρικού υπολογιστή. Μια εικονική μηχανή είναι μια εντελώς απομονωμένη εγκατάσταση λειτουργικού συστήματος σε ένα κανονικό λειτουργικό σύστημα κεντρικού υπολογιστή. Το 2008, μια ευπάθεια (CVE-2008-0923) στο VMware που ανακαλύφθηκε από την Core Security Technologies κατέστησε δυνατό το VM escape στο VMware Workstation 6.0.2 και 5.5.4.

3.2 Εικονικό Δίκτυο

Στα συστήματα υπολογιστικού νέφους, η επικοινωνία πραγματοποιείται όχι μόνο σε πραγματικά δίκτυα, αλλά σημαντικό ρόλο στην επικοινωνία παίζουν και τα εικονικά δίκτυα. Το εικονικό δίκτυο είναι ένα λογικό δίκτυο χτισμένο πάνω από ένα φυσικό δίκτυο. Τα εικονικά δίκτυα είναι υπεύθυνα για την επικοινωνία μεταξύ των VM. Τα στοιχεία δικτύου που βασίζονται σε λογισμικό (software-based network components), όπως γέφυρες, οι δρομολογητές και οι διαμορφώσεις δικτύου, υποστηρίζουν τη δικτύωση εικονικών μηχανών μέσω του ίδιου υπολογιστή. Τα εικονικοποιημένα δίκτυα δημιουργούν τις ακόλουθες προκλήσεις ασφαλείας στο περιβάλλον νέφους.

Οι μηχανισμοί ασφάλειας και προστασίας μέσω του φυσικού δικτύου δεν είναι σε θέση να παρακολουθούν την κίνηση μέσω εικονικού δικτύου. Αυτό γίνεται μια σοβαρή πρόκληση καθώς οι κακόβουλες δραστηριότητες των VM υπερβαίνουν την παρακολούθηση των εργαλείων ασφαλείας. Οι μηχανισμοί ανίχνευσης και πρόληψης εισβολής συνήθως εξαρτώνται από γνωστά μοτίβα στην κίνηση του δικτύου για να κρίνουν τις ανωμαλίες και να εντοπίσουν την πιθανότητα επίθεσης. Το εικονικό δίκτυο αποτελεί εμπόδιο στον στόχο τέτοιων προληπτικών μέτρων.

Το εικονικό δίκτυο είναι κοινόχρηστο μεταξύ πολλαπλών εικονικών μηχανών πράγμα το οποίο προκαλεί την πιθανότητα ορισμένων επιθέσεων, όπως, άρνηση Υπηρεσίας (DoS), πλαστογράφηση και sniffing[11] εικονικού δικτύου. Τα κρυπτογραφικά κλειδιά γίνονται ευάλωτα σε διαρροή, σε περίπτωση κακόβουλου sniffing και πλαστογράφησης εικονικού δικτύου.

3.3 Κακές παραμετροποιήσεις ασφάλειας

Οι διαμορφώσεις ασφαλείας της υποδομής δικτύου στο νέφος έχουν σημαντικό ρόλο για την παροχή ασφαλών υπηρεσιών στον χρήστη. Οι εσφαλμένες διαμορφώσεις

[11] Το sniffing είναι η πράξη υποκλοπής και παρακολούθησης της κυκλοφορίας σε ένα δίκτυο. Αυτό μπορεί να γίνει χρησιμοποιώντας λογισμικό που καταγράφει όλα τα πακέτα δεδομένων που περνούν μέσω μιας δεδομένης διεπαφής δικτύου ή χρησιμοποιώντας συσκευές υλικού που έχουν σχεδιαστεί ειδικά για αυτόν τον σκοπό.

μπορούν να θέσουν σε κίνδυνο την ασφάλεια των πελατών, των εφαρμογών και του συνόλου του συστήματος. Οι πελάτες αναθέτουν σε τρίτους τις εφαρμογές και τα δεδομένα τους στο νέφος με την εμπιστοσύνη ότι τα περιουσιακά τους στοιχεία είναι ασφαλή σε αυτό το περιβάλλον. Μια μικρή εσφαλμένη διαμόρφωση μπορεί να θέσει σε κίνδυνο την ασφάλεια του συστήματος. Οι διαμορφώσεις πρέπει να είναι σωστές όχι μόνο τη στιγμή της ανάπτυξης, εγκατάστασης και λειτουργίας της υποδομής του νέφους, αλλά και οι επακόλουθες αλλαγές στο δίκτυο θα πρέπει επίσης να διατηρούν τη διαμόρφωση συνεπή με τις πολιτικές ασφαλείας [23]. Πολύ συχνά, η αιτία της κακής παραμετροποίησης είναι το γεγονός πως οι διαχειριστές επιλέγουν ένα εργαλείο διαμόρφωσης με το οποίο είναι εξοικειωμένοι αλλά δεν καλύπτει απαραίτητα όλες τις απαιτήσεις ασφαλείας .

Η μετάβαση των VM, των δεδομένων και των εφαρμογών σε πολλούς φυσικούς κόμβους, οι αλλαγές στα μοτίβα στην κίνηση του δικτύου και η τοπολογία μπορούν να δημιουργήσουν την απαίτηση ποικίλων πολιτικών ασφαλείας [24]. Σε ένα τέτοιο σενάριο, η διαμόρφωση του νέφους θα πρέπει να γίνεται δυναμικά για να διασφαλίζεται η ασφάλεια. Ομοίως, οποιαδήποτε αδυναμία σε διαμορφώσεις συνεδριών και διαμορφώσεις πρωτοκόλλων μπορεί να αξιοποιηθεί για παραβίαση περιόδων σύνδεσης και για απόκτηση ευαίσθητων δεδομένων χρήστη [24].

3.4 Αποθήκευση δεδομένων

Το μοντέλο υπολογιστικού νέφους δεν παρέχει στους χρήστες πλήρη έλεγχο των δεδομένων. Αντίθετα από το συμβατικό υπολογιστικό μοντέλο, στο νέφος επιτρέπεται στους παρόχους υπηρεσιών να ασκούν έλεγχο στη διαχείριση διακομιστών και δεδομένων. Ο χρήστης απολαμβάνει συγκεκριμένο επίπεδο ελέγχου μόνο στα VMs. Η έλλειψη ελέγχου των δεδομένων οδηγεί σε περισσότερους κινδύνους για τα δεδομένα και την ασφάλεια από το συμβατικό υπολογιστικό μοντέλο. Επιπλέον, τα χαρακτηριστικά του υπολογιστικού νέφους, όπως η πολλαπλή μίσθωση και η εικονοποίηση, παρουσιάζουν επίσης δυνατότητες επιθέσεων διαφορετικές από το συμβατικό υπολογιστικό μοντέλο.

3.5 Data privacy και ακεραιότητα δεδομένων

Αν και το υπολογιστικό νέφος διασφαλίζει την οικονομία χρημάτων και επίσης απαλλάσσει τους χρήστες από δραστηριότητες διαχείρισης υποδομής, συνεπάγεται επίσης ζητήματα ασφάλειας. Τα δεδομένα στο νέφος είναι πολύ πιο ευάλωτα σε κινδύνους όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα σε σύγκριση με το συμβατικό υπολογιστικό μοντέλο [25]. Ο συνεχώς αυξανόμενος αριθμός χρηστών και εφαρμογών οδηγεί σε αυξημένους κινδύνους ασφαλείας.

Σε ένα κοινόχρηστο περιβάλλον, το επίπεδο ασφαλείας του νέφους ισούται με το επίπεδο ασφαλείας της πιο αδύναμης οντότητάς του [26]. Όχι μόνο η κακόβουλη οντότητα που συνεργάζεται με τα δεδομένα του θύματος, αλλά και οποιαδήποτε μη κακόβουλη αλλά μη ασφαλής οντότητα μπορεί να οδηγήσει σε παραβίαση δεδομένων. Μια επιτυχημένη επίθεση σε μία μόνο οντότητα θα έχει ως αποτέλεσμα μη εξουσιοδοτημένη πρόσβαση στα δεδομένα όλων των χρηστών. Παραβίαση της ακεραιότητας μπορεί επίσης να προκύψει από τη φύση πολλαπλών ενοικιαστών του νέφους. Υπάλληλος παρόχων SaaS, με πρόσβαση σε πληροφορίες μπορεί επίσης να λειτουργήσει ως πιθανός κίνδυνος [27].

Εκτός από τα «ακίνητα» δεδομένα (data at rest[12]), τα δεδομένα που υποβάλλονται σε επεξεργασία ενέχουν επίσης κινδύνους ασφαλείας [28]. Λόγω της εικονικοποίησης, οι φυσικοί πόροι μοιράζονται μεταξύ πολλών ενοικιαστών (clients). Αυτό τελικά μπορεί να επιτρέψει σε κακόβουλους χρήστες (που μοιράζονται τους ίδιους υπολογιστικούς πόρους) να εξαπολύσουν επιθέσεις στα δεδομένα άλλων χρηστών κατά τη φάση επεξεργασίας. Επιπλέον, εάν η διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων ανατεθεί σε τρίτο μέρος από τον CSP (Cloud Service Provider), το όριο κινδύνου διευρύνεται.

Η απουσία ασφαλών και τυπικών τεχνικών διαχείρισης κλειδιών για το νέφος δεν επιτρέπει στους τυπικούς κρυπτογραφικούς μηχανισμούς να κλιμακωθούν καλά στο μοντέλο υπολογιστικού νέφους [29]. Επομένως, ο τομέας κρυπτογραφίας ενισχύει επίσης τους πιθανούς κινδύνους για τα δεδομένα.

[12] Είναι τα δεδομένα που έχουν φτάσει σε έναν προορισμό και δεν χρησιμοποιούνται. Ο όρος συνήθως αναφέρεται σε αποθηκευμένα δεδομένα και εξαιρεί δεδομένα που κινούνται σε ένα δίκτυο ή βρίσκονται προσωρινά στη μνήμη του υπολογιστή και περιμένουν να διαβαστούν ή να ενημερωθούν.

3.6 Ασφάλεια web εφαρμογών και API

Οι υπηρεσίες και οι εφαρμογές στους χρήστες του νέφους παρέχονται μέσω του διαδικτύου. Στην πραγματικότητα, είναι μια από τις βασικές απαιτήσεις για μια εφαρμογή νέφους να χρησιμοποιείται και να μπορεί να διαχειριστεί μέσω του διαδικτύου. Η εφαρμογή που παρέχεται από τον CSP βρίσκεται πάντα στο νέφος με τους χρήστες να έχουν πρόσβαση παντού σε αυτήν. Ένα από τα σημαντικά χαρακτηριστικά των εφαρμογών νέφους είναι ότι δεν συνδέονται με συγκεκριμένους χρήστες. Διαφορετικοί χρήστες ενδέχεται να έχουν πρόσβαση στην ίδια εφαρμογή την ίδια στιγμή. Οι εφαρμογές νέφους κληρονομούν τα ίδια τρωτά σημεία με τις παραδοσιακές εφαρμογές και τεχνολογία Web. Ωστόσο, οι παραδοσιακές λύσεις ασφαλείας δεν είναι επαρκείς για το περιβάλλον υπολογιστικού νέφους, επειδή τα τρωτά σημεία στην διαδικτυακή εφαρμογή στο νέφος μπορεί να αποδειχθούν πολύ πιο καταστροφικά από τις παραδοσιακές διαδικτυακές εφαρμογές. Η παράλληλη φιλοξενία πολλών χρηστών, των δεδομένων τους και άλλων πόρων καθιστά πολύ μεγαλύτερο πρόβλημα. Οι δέκα κορυφαίοι κίνδυνοι στις εφαρμογές Web έχουν προσδιοριστεί από το Open Web Application Security Project (OWASP) ως εξής [30].

1. Broken Access Control
2. Cryptographic Failures
3. Injection (SQL, OS, and LDAP)
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and outdated components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-side request forgery

Η ανάπτυξη, διαχείριση και χρήση διαδικτυακών εφαρμογών πρέπει να λαμβάνει υπόψιν τους παραπάνω κινδύνους για την προστασία των εφαρμογών Ιστού και των πόρων των χρηστών. Ο χρήστης και οι υπηρεσίες στο νέφος γεφυρώνονται από τα API. Η ασφάλεια των API επηρεάζει σε μεγάλο βαθμό την ασφάλεια και τη διαθεσιμότητα

των υπηρεσιών νέφους. Τα ασφαλή API διασφαλίζουν την προστατευμένη και μη κακόβουλη χρήση των υπηρεσιών νέφους. Ένα API μπορεί να θεωρηθεί ως ένας οδηγός χρήστη που περιγράφει τις λεπτομέρειες σχετικά με την αρχιτεκτονική και τις δυνατότητες του CSP. Οι χρήστες δημιουργούν ή επεκτείνουν τις υπηρεσίες χρησιμοποιώντας τα API. Οι CSP συνήθως δημοσιεύουν τα API τους για να προωθήσουν τα χαρακτηριστικά του νέφους τους. Από τη μία πλευρά, η δημοσίευση των API βοηθά τους χρήστες να γνωρίζουν τις λεπτομέρειες σχετικά με τα στοιχεία και τις λειτουργίες του νέφους. Από την άλλη πλευρά, η αρχιτεκτονική του νέφους σε κάποιο βαθμό εκτίθεται στους εισβολείς. Επομένως, τα μη ασφαλή API μπορεί να είναι ενοχλητικά τόσο για το νέφος όσο και για τους χρήστες. Τα τρωτά σημεία των API περιλαμβάνουν αδύναμα διαπιστευτήρια, ανεπαρκή εξουσιοδότηση και επικύρωση δεδομένων εισόδου. Επιπλέον, οι συχνές ενημερώσεις των API ενδέχεται να εισάγουν κενά ασφαλείας στις εφαρμογές.

3.7 Ευαίσθητα δεδομένα στο νέφος

Με την πάροδο του χρόνου, οι οργανισμοί έχουν συλλέξει πολύτιμες πληροφορίες για τα άτομα στις κοινωνίες μας που περιέχουν ευαίσθητες πληροφορίες, π.χ. ιατρικά δεδομένα. Οι ερευνητές πρέπει να έχουν πρόσβαση και να αναλύουν τέτοια δεδομένα χρησιμοποιώντας τεχνολογίες «μεγάλων» δεδομένων (big data) [31], [32], [33] στο υπολογιστικό νέφος, ενώ οι οργανισμοί απαιτείται να επιβάλλουν τη συμμόρφωση με την προστασία δεδομένων με το αντίστοιχο νομοθετικό κανονιστικό πλαίσιο ανάλογα την γεωγραφική περιοχή, πχ GDPR, HIPAA κ.α..

Έχει σημειωθεί σημαντική πρόοδος στη διατήρηση της ιδιωτικής ζωής για ευαίσθητα δεδομένα τόσο στη βιομηχανία όσο και στον ακαδημαϊκό χώρο, π.χ. λύσεις που αναπτύσσουν πρωτόκολλα και εργαλεία για την ανωνυμοποίηση ή την κρυπτογράφηση δεδομένων για λόγους εμπιστευτικότητας. Αυτή η ενότητα κατηγοριοποιεί τις εργασίες που σχετίζονται με αυτόν τον τομέα σύμφωνα με διαφορετικές απαιτήσεις προστασίας της ιδιωτικής ζωής. Ωστόσο, αυτές οι λύσεις δεν έχουν ακόμη υιοθετηθεί ευρέως από παρόχους υπηρεσιών νέφους ή οργανισμούς.

Ο Pearson [34] συζητά μια σειρά από προκλήσεις ασφάλειας και απορρήτου που δημιουργούνται από το υπολογιστικό νέφος. Η έλλειψη ελέγχου των χρηστών, η έλλειψη εκπαίδευσης και τεχνογνωσίας, η μη εξουσιοδοτημένη χρήση, η πολυπλοκότητα της συμμόρφωσης με τους κανονισμούς, οι διασυνοριακοί περιορισμοί ροής δεδομένων και οι δικαστικές διαφορές είναι μεταξύ των προκλήσεων που αντιμετωπίζουν τα περιβάλλοντα υπολογιστικού νέφους. Στο [35], οι συγγραφείς περιγράφουν τις προκλήσεις απορρήτου των γονιδιωματικών δεδομένων στο νέφος, συμπεριλαμβανομένων των όρων παροχής υπηρεσιών των παρόχων νέφους που δεν έχουν αναπτυχθεί με νοοτροπία υγειονομικής περίθαλψης, την περίπτωση όπου δεδομένα ασθενών να ανεβαίνουν στο νέφος χωρίς τη συγκατάθεσή τους, την παρακολούθηση δεδομένων, την ασφάλεια δεδομένων και τη λογοδοσία (accountability). Οι συγγραφείς παρέχουν επίσης συστάσεις για τους κατόχους δεδομένων όταν στοχεύουν να χρησιμοποιήσουν υπηρεσίες νέφους.

Στο [35] οι συγγραφείς συζήτησαν διάφορα ζητήματα απορρήτου που σχετίζονται με τη γονιδιωματική αλληλουχία. Αυτή η μελέτη περιέγραψε επίσης αρκετά ανοιχτά ερευνητικά προβλήματα (όπως η εξωτερική ανάθεση σε παρόχους νέφους, η κρυπτογράφηση γονιδιωματικών δεδομένων, η αναπαραγωγή, η ακεραιότητα και η αφαίρεση των γονιδιωματικών δεδομένων) μαζί με την παροχή προτάσεων για τη βελτίωση του απορρήτου μέσω της συνεργασίας μεταξύ διαφορετικών οντοτήτων και οργανισμών.

Η ομομορφική κρυπτογράφηση είναι μια άλλη λύση διατήρησης της ιδιωτικής ζωής που βασίζεται στην ιδέα του υπολογισμού πάνω από κρυπτογραφημένα δεδομένα χωρίς να γνωρίζουμε τα κλειδιά. Για να διασφαλιστεί η εμπιστευτικότητα, ο κάτοχος δεδομένων μπορεί να κρυπτογραφήσει δεδομένα με ένα δημόσιο κλειδί και να αποθηκεύσει δεδομένα στο νέφος. Όταν η μηχανή διεργασίας διαβάζει τα δεδομένα, δεν χρειάζεται το ιδιωτικό κλειδί του DP (data processor) για την αποκρυπτογράφηση των δεδομένων. Ουσιαστικά η ομομορφική κρυπτογράφηση επιτρέπει την εκτέλεση υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα χωρίς να χρειάζεται ποτέ η πρόσβαση στα αρχικά δεδομένα. Σε ιδιωτικούς υπολογισμούς σε κρυπτογραφημένα γονιδιωματικά δεδομένα [38], οι συγγραφείς πρότειναν ένα μοντέλο διατήρησης της ιδιωτικής ζωής για την επεξεργασία γονιδιωματικών δεδομένων χρησιμοποιώντας ομομορφική κρυπτογράφηση σε μελέτες συσχέτισης σε όλο το γονιδίωμα.

Η ανωνυμοποίηση είναι μια άλλη προσέγγιση για τη διασφάλιση του απορρήτου των ευαίσθητων δεδομένων. Το SAIL [39] παρέχει πληροφορίες σε

ατομικό επίπεδο σχετικά με τη διαθεσιμότητα τύπων δεδομένων σε μια συλλογή. Οι ερευνητές δεν είναι σε θέση να διασυνδέσουν (πράγμα που είναι παρόμοιο με μια ένωση ισότητας στην SQL) δεδομένα από διαφορετικές εξωτερικές μελέτες, καθώς οι ταυτότητες των δειγμάτων είναι ανώνυμες.

Σε μια άλλη προσπάθεια [40] οι συγγραφείς προτείνουν μια αρχιτεκτονική για να καταστεί δυνατή η εκτέλεση συγκεντρωτικών ερωτημάτων σε ανώνυμα σύνολα ιατρικών δεδομένων από διαφορετικούς παρόχους δεδομένων. Σε αυτήν τη λύση, οι πάροχοι δεδομένων αφαιρούν τα αναγνωριστικά των υποκειμένων των δεδομένων και εφαρμόζουν κρυπτογράφηση δύο επιπέδων χρησιμοποιώντας πιστοποιητικά κατακερματισμού (hash certificates) και PKI[13]. Στη συνέχεια, οι ευαίσθητες πληροφορίες θα ανωνυμοποιηθούν χρησιμοποιώντας μια εργαλειοθήκη ανοιχτού κώδικα και θα κρυπτογραφηθούν αναλυτικά χρησιμοποιώντας το δημόσιο κλειδί του παρόχου. Το ScaBIA [41] είναι μια άλλη λύση για την επεξεργασία και την αποθήκευση ανώνυμων δεδομένων απεικόνισης εγκεφάλου στο νέφος. Αυτή η προσέγγιση παρέχει έλεγχο ταυτότητας PKI για τον ρόλο του διαχειριστή για την ανάπτυξη ενός ενδιάμεσου λογισμικού PaaS και ορίζει τους ερευνητές ως χρήστες στο Microsoft Azure. Οι ερευνητές μπορούν να συνδέονται με όνομα χρήστη/κωδικό

[13] PKI (Public Key Encryption) είναι το σύνολο των τεχνολογιών και των διαδικασιών που συνθέτουν ένα πλαίσιο κρυπτογράφησης για την προστασία και τον έλεγχο ταυτότητας των ψηφιακών επικοινωνιών. Το PKI χρησιμοποιεί κρυπτογραφικά δημόσια κλειδιά που συνδέονται με ένα ψηφιακό πιστοποιητικό, το οποίο επαληθεύει τη συσκευή ή τον χρήστη που μετέχει στην ψηφιακή επικοινωνία. Τα ψηφιακά πιστοποιητικά εκδίδονται από μια αξιόπιστη πηγή, μια αρχή έκδοσης πιστοποιητικών (CA) και λειτουργούν ως τύπος ψηφιακού διαβατηρίου για να διασφαλιστεί ότι ο αποστολέας είναι αυτός που λέει ότι είναι. Η υποδομή δημόσιου κλειδιού προστατεύει και επαληθεύει τις επικοινωνίες μεταξύ διακομιστών και χρηστών, όπως μεταξύ ενός ιστοτόπου (που φιλοξενείται σε έναν διακομιστή) και των πελατών (ο χρήστης που προσπαθεί να συνδεθεί μέσω του προγράμματος περιήγησής του). Μπορεί επίσης να χρησιμοποιηθεί για ασφαλείς επικοινωνίες εντός ενός οργανισμού για να διασφαλιστεί ότι τα μηνύματα είναι ορατά μόνο στον αποστολέα και τον παραλήπτη και ότι δεν έχουν παραβιαστεί κατά τη μεταφορά.
Τα κύρια στοιχεία της υποδομής δημόσιου κλειδιού περιλαμβάνουν τα ακόλουθα:
Αρχή έκδοσης πιστοποιητικών (CA): Η CA είναι μια αξιόπιστη οντότητα που εκδίδει, αποθηκεύει και υπογράφει το ψηφιακό πιστοποιητικό. Η CA υπογράφει το ψηφιακό πιστοποιητικό με το δικό της ιδιωτικό κλειδί και στη συνέχεια δημοσιεύει το δημόσιο κλειδί το οποίο μπορεί να προσπελαστεί κατόπιν αιτήματος.
Αρχή καταχώρισης (RA): Η RA επαληθεύει την ταυτότητα του χρήστη ή της συσκευής που ζητά το ψηφιακό πιστοποιητικό. Αυτό μπορεί να είναι τρίτο μέρος ή η CA μπορεί επίσης να ενεργεί ως RA.
Βάση δεδομένων πιστοποιητικών: Αυτή η βάση δεδομένων αποθηκεύει το ψηφιακό πιστοποιητικό και τα μεταδεδομένα (metadata) του, τα οποία περιλαμβάνουν τη διάρκεια ισχύος του πιστοποιητικού.
Κεντρικός κατάλογος (Central directory): Αυτή είναι η ασφαλής τοποθεσία όπου καταχωρούνται και αποθηκεύονται τα κρυπτογραφικά κλειδιά.
Σύστημα διαχείρισης πιστοποιητικών: Αυτό είναι το σύστημα διαχείρισης της παράδοσης των πιστοποιητικών καθώς και της πρόσβασης σε αυτά.
Πολιτική πιστοποιητικών: Αυτή η πολιτική περιγράφει τις διαδικασίες του PKI. Μπορεί να χρησιμοποιηθεί από ξένους για τον προσδιορισμό της αξιοπιστίας του PKI.

πρόσβασης για να εκτελούν εργασίες στατιστικής παραμετρικής χαρτογράφησης[14] (statistical parametric mapping) εντός απομονωμένων containers[15]. Τα σύνολα δεδομένων απεικόνισης εγκεφάλου και τα σχετικά αποτελέσματα μπορούν να κοινοποιηθούν από τους ερευνητές χρησιμοποιώντας ένα μοντέλο RBAC[16] μέσω ασφαλών συνδέσεων HTTPS.

[14] Η στατιστική παραμετρική χαρτογράφηση (SPM) είναι μια στατιστική τεχνική για την εξέταση διαφορών στην εγκεφαλική δραστηριότητα που καταγράφονται κατά τη διάρκεια πειραμάτων νευροαπεικόνισης

[15] Η τεχνολογία container είναι μια ελαφριά, εκτελέσιμη μονάδα λογισμικού που «συσκευάζει» κώδικα και dependencies, όπως βιβλιοθήκες και αρχεία διαμόρφωσης για εύκολη ανάπτυξη σε διαφορετικά περιβάλλοντα υπολογιστών.

[16] Ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) περιορίζει την πρόσβαση σε ένα δίκτυο με βάση τον ρόλο ενός ατόμου σε έναν οργανισμό και έχει γίνει μια από τις κύριες μεθόδους για προηγμένο έλεγχο πρόσβασης

4

Θέματα ασφαλείας υποδομής

4.1 Εισαγωγή στην ασφάλεια υποδομής

Το λογισμικό, η πλατφόρμα και η υποδομή ως υπηρεσία είναι τα τρία κύρια μοντέλα παροχής υπηρεσιών για το υπολογιστικό νέφος. Αυτά τα μοντέλα είναι προσβάσιμα ως υπηρεσία μέσω διαδικτύου. Οι υπηρεσίες νέφους διατίθενται ως pay-as-you-go, όπου οι χρήστες πληρώνουν μόνο για τους πόρους που χρησιμοποιούν πραγματικά για μια συγκεκριμένη χρονική στιγμή, σε αντίθεση με τις παραδοσιακές υπηρεσίες, π.χ. web Hosting. Επιπλέον, η τιμολόγηση για τις υπηρεσίες νέφους ποικίλλει γενικά ανάλογα με τις απαιτήσεις QoS[17] (Quality of Service) του εκάστοτε πελάτη [45]. Τα μοντέλα ανάπτυξης υπολογιστικού νέφους, με βάση τη σχέση τους με την επιχείρηση, ταξινομούνται σε ιδιωτικά, δημόσια και υβριδικά. Οι υπηρεσίες public cloud πωλούνται ως Utility Computing, ενώ το private cloud αναφέρεται σε εσωτερικά κέντρα δεδομένων μιας επιχείρησης που δεν είναι διαθέσιμα στο ευρύ κοινό.

Η σύγχυση μεταξύ υπολογιστικού νέφους και Service Oriented Architecture (SOA) προσφέρεται για μια σύντομη σύγκριση μεταξύ τους. Το SOA και το υπολογιστικό νέφος μπορούν να θεωρηθούν συμπληρωματικές υπηρεσίες με κοινά

[17] Ποιότητα υπηρεσίας (QoS) είναι η περιγραφή ή η μέτρηση της συνολικής απόδοσης μιας υπηρεσίας, όπως ένα δίκτυο τηλεφωνίας ή υπολογιστών, ή μια υπηρεσία υπολογιστικού νέφους, ιδιαίτερα η απόδοση που βλέπουν οι χρήστες του δικτύου. Για να μετρηθεί ποσοτικά η ποιότητα της υπηρεσίας, συχνά λαμβάνονται υπόψη πολλές σχετικές πτυχές της υπηρεσίας δικτύου, όπως η απώλεια πακέτων, ο ρυθμός μετάδοσης (bitrate), η απόδοση, η καθυστέρηση μετάδοσης (latency), η διαθεσιμότητα, το jitter κ.λπ.

χαρακτηριστικά. Ως εκ τούτου, εάν το SOA είναι ένα σύνολο αρχών και μεθοδολογιών που έχει σχεδιαστεί για να διευκολύνει την ολοκλήρωση και την επικοινωνία συστημάτων ανεξάρτητα από τις γλώσσες και τις πλατφόρμες ανάπτυξης, το υπολογιστικό νέφος, από την άλλη πλευρά, έχει σχεδιαστεί για να επιτρέπει στις εταιρείες να χρησιμοποιούν τεράστιες δυνατότητες άμεσα χωρίς να χρειάζεται να επενδύσουν σε νέα υποδομή, να εκπαιδεύσουν νέο προσωπικό ή αγοράσουν νέο λογισμικό.

Το υπολογιστικό νέφος επιτρέπει τόσο στις μικρές και μεσαίες επιχειρήσεις να αναθέτουν πλήρως την υποδομή των κέντρων δεδομένων τους σε έναν πάροχο, όσο και σε μεγάλες εταιρείες που έχουν ανάγκη αποθήκευσης τεράστιων όγκων δεδομένων, να μην χρειάζεται να δημιουργούν εσωτερικά μεγαλύτερα και ακριβότερα κέντρα δεδομένων. Όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, το υπολογιστικό νέφος χρησιμοποιεί την τεχνολογία εικονικοποίησης (virtualization) για να προσφέρει ένα ασφαλές, επεκτάσιμο, κοινόχρηστο και διαχειρίσιμο περιβάλλον. Εν ολίγοις, ανεξάρτητα από τη διαφορά στους σχεδιαστικούς σκοπούς και την εξάρτηση του νέφους από την τεχνολογία εικονικοποίησης, το υπολογιστικό νέφος μπορεί να διασταυρωθεί με το SOA στα Components as a Service, π.χ., SOA μέσω πρότυπων υπηρεσιών web. Επομένως, το υπολογιστικό νέφος και το SOA μπορούν να υλοποιηθούν ανεξάρτητα ή ταυτόχρονα ως συμπληρωματικές δραστηριότητες για την παροχή ενός μοναδικού αποτελέσματος.

Το υπολογιστικό νέφος εξαρτάται κατά κύριο λόγο από το επίπεδο IaaS για να παρέχει φθηνή επεξεργαστική ισχύ, αποθήκευση δεδομένων και άλλους κοινόχρηστους πόρους. Σε αυτή την εργασία, παρουσιάζεται μια λεπτομερής και ακριβής μελέτη των ανησυχιών για την ασφάλεια και το απόρρητο του IaaS. Ερευνήθηκε η ασφάλεια για κάθε στοιχείο IaaS: Service Level Agreement (SLA), Utility Computing (UC), Virtualization πλατφόρμας, Δίκτυα και Συνδεσιμότητα στο Διαδίκτυο και υπολογιστικό Hardware. Επιπλέον, παρουσιάζεται η ασφάλεια του λογισμικού στο νέφος που επηρεάζει το IaaS και ολόκληρο το υπολογιστικό νέφος. Η εργασία εστιάζει στο μοντέλο παράδοσης IaaS επειδή είναι το θεμέλιο όλων των άλλων μοντέλων και η έλλειψη ασφάλειας σε αυτό το επίπεδο επηρεάζει τα άλλα επίπεδα του νέφους που είναι χτισμένα πάνω στο IaaS.

4.2 Συνιστώσες του IaaS

Το μοντέλο παράδοσης IaaS αποτελείται από πολλά στοιχεία που έχουν αναπτυχθεί τα τελευταία χρόνια, ωστόσο, η χρήση αυτών των στοιχείων μαζί σε ένα κοινόχρηστο και εξωτερικό περιβάλλον φέρει πολλαπλές προκλήσεις. Η ασφάλεια και το απόρρητο είναι οι πιο σημαντικές προκλήσεις που μπορεί να εμποδίσουν την υιοθέτηση του Cloud Computing. Η παραβίαση της ασφάλειας οποιουδήποτε στοιχείου επηρεάζει την ασφάλεια των άλλων στοιχείων, κατά συνέπεια, η ασφάλεια ολόκληρου του συστήματος θα καταρρεύσει. Ακολούθως θα αναλυθεί το ζήτημα ασφάλειας κάθε στοιχείου και θα προταθούν λύσεις και συστάσεις.

4.2.1 Service Level Agreement (SLA)

Το υπολογιστικό νέφος αναδύει ένα σύνολο πολυπλοκοτήτων διαχείρισης IT και η χρήση του SLA είναι η λύση για την εξασφάλιση αποδεκτού επιπέδου QoS. Ένα SLA περιλαμβάνει τον ορισμό σύμβασης SLA, διαπραγμάτευση SLA, παρακολούθηση SLA και επιβολή SLA. Το στάδιο του καθορισμού και της διαπραγμάτευσης της σύμβασης SLA είναι σημαντικό για τον προσδιορισμό των οφελών και των ευθυνών κάθε μέρους, οποιαδήποτε παρεξήγηση θα επηρεάσει την ασφάλεια του συστήματος και θα αφήσει τον πελάτη εκτεθειμένο σε τρωτά σημεία. Από την άλλη πλευρά, η παρακολούθηση και η επιβολή SLA είναι ζωτικής σημασίας για την οικοδόμηση της εμπιστοσύνης μεταξύ του παρόχου και του πελάτη. Για την επιβολή SLA σε ένα δυναμικό περιβάλλον όπως το νέφος, είναι απαραίτητο να παρακολουθούνται συνεχώς τα χαρακτηριστικά QoS. Επί του παρόντος, οι πελάτες νέφους πρέπει να εμπιστεύονται την παρακολούθηση SLA των παρόχων μέχρι την τυποποίηση των συστημάτων υπολογιστικού νέφους και την ανάθεση τρίτων για τη μεσολάβηση της παρακολούθησης και επιβολής της SLA.

4.2.2 Utility Computing

Το Utility Computing δεν είναι νέα έννοια. έπαιξε ουσιαστικό ρόλο στην ανάπτυξη του Grid Computing[18]. Ομαδοποιεί τους πόρους (π.χ. επεξεργαστές, εύρος ζώνης, αποθήκευση κ.λπ.) ως υπηρεσίες και τις παραδίδει στον πελάτη. Η δύναμη αυτού του μοντέλου έγκειται σε δύο βασικά σημεία: Πρώτον, μειώνει το συνολικό κόστος, δηλαδή, αντί να κατέχει τους πόρους, ο πελάτης μπορεί να πληρώσει μόνο για την ώρα χρήσης (pay-as-you-go). Δεύτερον, έχει αναπτυχθεί για να υποστηρίζει κλιμακούμενα συστήματα, δηλαδή, ο ιδιοκτήτης ενός ταχέως αναπτυσσόμενου συστήματος, δεν χρειάζεται να ανησυχεί για τις δυνατότητες εξυπηρέτησης της υποδομής του καθώς αυτή μπορεί να αυξηθεί ή να μειωθεί αυτόματα αναλόγως τη ζήτηση. Προφανώς, το Utility Computing διαμορφώνει δύο από τα κύρια χαρακτηριστικά του υπολογιστικού νέφους (π.χ. επεκτασιμότητα και pay-as-you-go).

Η πρώτη πρόκληση για το Utility Computing είναι η πολυπλοκότητα του υπολογιστικού νέφους, για παράδειγμα, ένας πάροχος πρώτου επιπέδου όπως η Amazon πρέπει να προσφέρει τις υπηρεσίες του ως μετρήσιμες υπηρεσίες. Αυτές οι υπηρεσίες μπορούν να χρησιμοποιηθούν από παρόχους δεύτερου επιπέδου που παρέχουν επίσης μετρήσιμες υπηρεσίες. Σε τέτοια πολλαπλά επίπεδα, τα συστήματα γίνονται πιο πολύπλοκα και απαιτούν μεγαλύτερη προσπάθεια διαχείρισης τόσο από τους παρόχους ανώτερου όσο και από τους παρόχους δεύτερου επιπέδου. Το Amazon DevPay, ένα παράδειγμα τέτοιων συστημάτων, καθώς επιτρέπει στον πάροχο δεύτερου επιπέδου να μετράει τη χρήση των υπηρεσιών AWS και να χρεώνει τους χρήστες του σύμφωνα με τις τιμές που καθορίζει ο πάροχος δεύτερου επιπέδου. Η δεύτερη πρόκληση είναι ότι τα συστήματα Utility Computing μπορούν να είναι ελκυστικοί στόχοι για τους εισβολείς, επομένως ένας εισβολέας μπορεί να στοχεύει στην πρόσβαση σε υπηρεσίες χωρίς να πληρώσει ή μπορεί να προχωρήσει περαιτέρω για να οδηγήσει συγκεκριμένους εταιρικούς

[18] Το Grid Computing είναι μια υπολογιστική υποδομή που συνδυάζει πόρους υπολογιστών κατανεμημένους σε διαφορετικές γεωγραφικές τοποθεσίες για την επίτευξη ενός κοινού στόχου. Όλοι οι αχρησιμοποίητοι πόροι σε πολλούς υπολογιστές συγκεντρώνονται και διατίθενται για μία μόνο εργασία.

λογαριασμούς σε μη διαχειρίσιμα επίπεδα. Ο πάροχος είναι ο κύριος υπεύθυνος για τη διατήρηση της υγείας και της καλής λειτουργίας του συστήματος.

4.2.3 Λογισμικό του υπολογιστικού νέφους

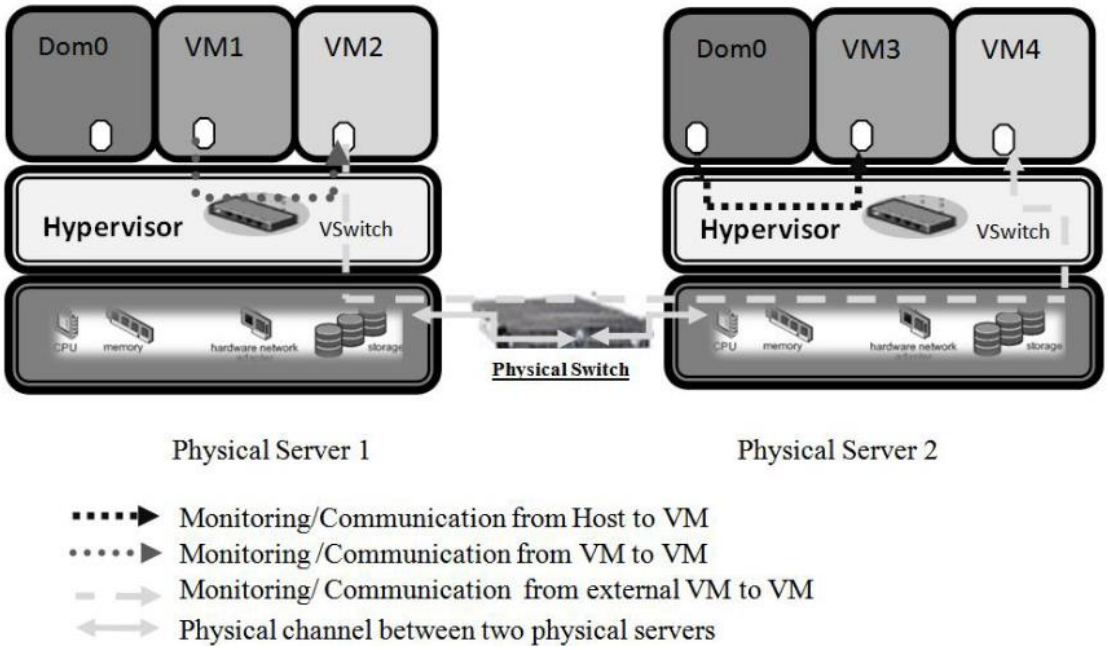
Υπάρχουν πολλές εφαρμογές λογισμικού ανοιχτού κώδικα για το νέφος όπως το Eucalyptus [46] και το Nimbus [47]. Το λογισμικό του υπολογιστικού νέφους ενώνει τα στοιχεία του νέφους μαζί. Το λογισμικό νέφους μπορεί να είναι ανοιχτού κώδικα είτε εμπορικό κλειστού κώδικα. Οι πάροχοι υπηρεσιών cloud παρέχουν APIs (REST, SOAP ή HTTP με XML/JSON) για την εκτέλεση των περισσότερων λειτουργιών διαχείρισης, όπως ο έλεγχος πρόσβασης από απομακρυσμένη τοποθεσία. Για παράδειγμα, ο πελάτης μπορεί να χρησιμοποιήσει τα κιτ εργαλείων Amazon EC2, μια ευρέως υποστηριζόμενη διεπαφή, για να καταναλώσει τις υπηρεσίες εφαρμόζοντας δικές του εφαρμογές ή χρησιμοποιώντας απλώς τις web διεπαφές που προσφέρονται από τον πάροχο. Και στις δύο περιπτώσεις, ο χρήστης χρησιμοποιεί πρωτόκολλα υπηρεσιών web. Το SOAP είναι το πιο δημοφιλές υποστηριζόμενο πρωτόκολλο στις υπηρεσίες web.

Το WS-Security, μια τυπική επέκταση για την ασφάλεια στο SOAP, ασχολείται με την ασφάλεια για υπηρεσίες web. Ορίζει μια κεφαλίδα SOAP (Security) που φέρει τις επεκτάσεις WS-Security και καθορίζει τον τρόπο με τον οποίο εφαρμόζονται τα υπάρχοντα πρότυπα ασφαλείας XML, όπως η υπογραφή XML και η κρυπτογράφηση XML, στα μηνύματα SOAP. Γνωστές επιθέσεις σε πρωτόκολλα που χρησιμοποιούν την υπογραφή XML για έλεγχο ταυτότητας ή προστασία ακεραιότητας [48] θα μπορούσαν να εφαρμοστούν σε υπηρεσίες ιστού επηρεάζοντας κατά συνέπεια τις υπηρεσίες νέφους.

Τέλος, ένα ακραίο σενάριο στο [49] έδειξε τη δυνατότητα να σπάσει η ασφάλεια μεταξύ του προγράμματος περιήγησης και του νέφους, πράγμα το οποίο οδήγησε σε πρόταση για ενίσχυση της τρέχουσας ασφάλειας των προγραμμάτων περιήγησης. Είναι αλήθεια πως αυτές οι επιθέσεις ανήκουν περισσότερο στον κόσμο των υπηρεσιών web, αλλά ως τεχνολογία που χρησιμοποιείται στο υπολογιστικό νέφος, η ασφάλεια των υπηρεσιών web επηρεάζει έντονα την ασφάλεια των υπηρεσιών νέφους.

4.2.4 Εικονικοποίηση πλατφόρμας

Το Virtualization (Εικονικοποίηση), μια θεμελιώδης τεχνολογική πλατφόρμα για υπηρεσίες νέφους, διευκολύνει τη συγκέντρωση πολλαπλών αυτόνομων συστημάτων σε μια ενιαία πλατφόρμα υλικού εικονικοποιώντας τους υπολογιστικούς πόρους (π.χ. δίκτυο, CPU, μνήμη και αποθήκευση). Η εικονικοποίηση κρύβει την πολυπλοκότητα της διαχείρισης της φυσικής υπολογιστικής πλατφόρμας και απλοποιεί την επεκτασιμότητα των υπολογιστικών πόρων. Ως εκ τούτου, η εικονικοποίηση παρέχει πολλαπλή μίσθωση και επεκτασιμότητα, και αυτά είναι δύο σημαντικά χαρακτηριστικά του νέφους.



Εικόνα 3: Διαφορετικά είδη αλληλεπίδρασης Εικονικών Μηχανών και Host

Καθώς ο hypervisor είναι υπεύθυνος για την απομόνωση των VM, τα VM δεν θα μπορούσαν να έχουν άμεση πρόσβαση σε εικονικούς δίσκους, μνήμη ή εφαρμογές άλλων στον ίδιο κεντρικό υπολογιστή. Το IaaS, ένα κοινόχρηστο περιβάλλον, απαιτεί ακριβή διαμόρφωση για τη διατήρηση ισχυρής απομόνωσης. Οι πάροχοι υπηρεσιών νέφους καταβάλουν σημαντική προσπάθεια για την ασφάλεια των συστημάτων τους, προκειμένου να ελαχιστοποιήσουν τις απειλές που προκύπτουν από την επικοινωνία,

την παρακολούθηση, το migration[19] και το DoS. Ακολούθως αναλύονται τα ρίσκα και τα τρωτά σημεία της εικονικοποίησης που επηρεάζουν ιδιαίτερα το μοντέλο IaaS, επιπλέον των προτεινόμενων λύσεων για την εγγύηση της ασφάλειας, του απορρήτου και της ακεραιότητας των δεδομένων για το IaaS.

1) ***Απειλές ασφαλείας που προέρχονται από τον κεντρικό υπολογιστή (Host):***

Οι απειλές που προέρχονται από τον κεντρικό υπολογιστή προέρχονται από διαδικασίες παρακολούθησης, επικοινωνίας ή τροποποίησης των VM. Αυτές οι απειλές και οι προτεινόμενες λύσεις χωρίζονται ως εξής:

Παρακολούθηση VM από κεντρικό υπολογιστή:

Η παρακολούθηση θεωρείται μια σημαντική απειλή που περιλαμβάνει ενέργειες ελέγχου (π.χ. εκκίνηση, τερματισμός λειτουργίας, παύση, επανεκκίνηση των VM) και τροποποίηση πόρων των VM. Δυστυχώς, ο διαχειριστής (sysadmin) ή οποιοσδήποτε εξουσιοδοτημένος χρήστης που έχει προνομιακό έλεγχο στο backend μπορεί να κάνει κακή χρήση αυτής της διαδικασίας.

Επικοινωνίες μεταξύ VM και κεντρικού υπολογιστή:

Οι επικοινωνίες μεταξύ VM και κεντρικού υπολογιστή γίνονται μέσω κοινόχρηστων εικονικών πόρων (π.χ. εικονικό δίκτυο). Η Εικόνα 3 δείχνει ότι όλα τα πακέτα δικτύου που προέρχονται από ή πηγαίνουν σε ένα VM περνούν μέσα από τον κεντρικό υπολογιστή, έτσι ο κεντρικός υπολογιστής είναι γενικά σε θέση να παρακολουθεί την

[19] Το migration στο νέφος είναι η διαδικασία μεταφοράς των ψηφιακών περιουσιακών στοιχείων, των υπηρεσιών, των βάσεων δεδομένων, των πόρων πληροφορικής και των εφαρμογών μιας εταιρείας είτε εν μέρει είτε εξ ολοκλήρου στο νέφος.

κίνηση δικτύου των VM που φιλοξενεί. Κακόβουλοι χρήστες ενδέχεται να εκμεταλλευτούν ορισμένες χρήσιμες λειτουργίες σε μια εικονική μηχανή, όπως το κοινόχρηστο πρόχειρο που επιτρέπει τη μεταφορά δεδομένων μεταξύ VM και του κεντρικού υπολογιστή για την ανταλλαγή δεδομένων μεταξύ συνεργαζόμενων κακόβουλων προγραμμάτων. Ωστόσο, η χειρότερη περίπτωση συμβαίνει όταν ένας κεντρικός υπολογιστής παραβιάζεται, αυτό θέτει σε κίνδυνο όλα τα VM. Αφού αναλυθούν οι απειλές που προέρχονται από έναν host, παρουσιάζονται και οι προτεινόμενες λύσεις που αποτρέπουν ή μετριάζουν αυτές τις απειλές και τρωτά σημεία.

Το Terra [50] είναι μια αρχιτεκτονική που παρουσιάζει ένα έμπιστο περιβάλλον εκτέλεσης για VM που θα τα προστατεύει από έναν χρήστη με πλήρη δικαιώματα (π.χ. sysadmin), έτσι ώστε τα VM να μην επιθεωρούνται ή να τροποποιούνται από άλλο VM που εκτελείται στην ίδια πλατφόρμα, ακόμη και από χρήστη με πλήρη προνόμια. Δυστυχώς, το Terra δεν είναι κατάλληλο για να αναπτυχθεί σε ένα πολύπλοκο δυναμικό περιβάλλον όπως το IaaS που περιλαμβάνει πολλές εκατοντάδες μηχανές δικτυωμένες μεταξύ τους. Στο περιβάλλον IaaS, τα VM δημιουργούνται και προγραμματίζονται να εκτελούνται δυναμικά. Επιπλέον, η εξυπηρέτηση ενός τεράστιου αριθμού καταναλωτών καθιστά το IaaS πιο ευάλωτο και λιγότερο αξιόπιστο.

Για να ξεπεραστούν τα μειονεκτήματα σε παραδοσιακές αξιόπιστες πλατφόρμες όπως η Terra, προτείνεται η τεχνική Trusted Virtual Datacenter (TVDc) [51], [52] για την αντιμετώπιση ζητημάτων ασφάλειας τόσο της υποδομής όσο και της διαχείρισης. Το TVDc διαχειρίζεται την ασφάλεια στην εικονικοποίηση κέντρων δεδομένων επιβάλλοντας συστήματα ελέγχου πρόσβασης που βασίζονται σε ετικέτες ασφαλείας και εφαρμόζοντας πρότυπα διαχείρισης που προτείνουν την επιβολή κανόνων απομόνωσης (isolation protocols) και τον έλεγχο ακεραιότητας (integrity check).

Η χρήση VLAN [53] για την ενίσχυση της απομόνωσης δικτύου και τη βελτίωση των δυνατοτήτων διαχείρισης συστημάτων εφαρμόστηκε από τα TVDc [51], [52]. Τα TPMs (Trusted Processing Modules) προτάθηκαν από την Trusted Computing Group (TCG) για την παροχή

κρυπτογραφικών διαπιστευτηρίων, απομακρυσμένης βεβαίωσης (remote verification) και προστασίας ακεραιότητας. Θα μπορούσαν επίσης να χρησιμοποιηθούν στο υπολογιστικό νέφος για την ενεργοποίηση της απομακρυσμένης βεβαίωσης όπως στις Αξιόπιστες Πλατφόρμες (Trusted Platforms) [54] και [55].

2) ***Απειλές ασφαλείας που προέρχονται από άλλα VM:***

Σε αυτήν την ενότητα, αναλύονται απειλές που προκύπτουν από την επικοινωνία, παρακολούθηση και τροποποίηση της εικονικής μηχανής από άλλο VM ή από εξωτερικό μηχάνημα.

Παρακολούθηση VM από άλλα VM:

Η παρακολούθηση VM θα μπορούσε να παραβιάσει την ασφάλεια και το απόρρητο σε ένα φυσικό μηχάνημα που φιλοξενεί πολλές εικονικές μηχανές, αλλά η νέα αρχιτεκτονική των CPU, ενσωματώνει μια δυνατότητα προστασίας μνήμης, η οποία θα μπορούσε να αποτρέψει την παραβίαση του απορρήτου. Ο hypervisor χρησιμοποιεί αυτή την τεχνολογία για να εμποδίσει ένα VM να παρακολουθεί τους πόρους μνήμης άλλων VM και να έχει πρόσβαση σε εικονικούς δίσκους άλλων VM που έχουν εκχωρηθεί στον κεντρικό υπολογιστή. Από την άλλη πλευρά, οι μηχανές φυσικής δικτύωσης συνδέονται με φυσικό αποκλειστικό κανάλι. Ωστόσο, στην εικονική δικτύωση, τα VM συνδέονται με τον κεντρικό υπολογιστή μέσω ενός εικονικού μεταγωγέα (switch). Δυστυχώς, και στις δύο περιπτώσεις, θα μπορούσαν να προκληθούν επιθέσεις όπως packet sniffing και ARP poisoning[20] μεταξύ μηχανών.

[20] Το ARP Poisoning (γνωστό και ως ARP Spoofing) είναι ένας τύπος κυβερνοεπίθεσης που πραγματοποιείται μέσω ενός τοπικού δικτύου (LAN) που περιλαμβάνει την αποστολή κακόβουλων πακέτων ARP σε μια προεπιλεγμένη πύλη (gateway) σε ένα LAN προκειμένου να αλλάξουν οι αντιστοιχίες IP και MAC διευθύνσεων στο routing table.

Ένα σχήμα κρυπτογράφησης, όπως το TLS ή το IPSec μπορεί να χρησιμοποιηθεί για την προστασία του απορρήτου, καθώς για να τροποποιηθούν τα δεδομένα πακέτων, θα ήταν απαραίτητο να τροποποιηθεί και ο κώδικας του πυρήνα (kernel) Dom0[21] που ελέγχει δικτυακή γέφυρα (bridge).

Η κρυπτογράφηση παρέχει μια πρόσθετη άμυνα έναντι επιθέσεων στην ακεραιότητα του δικτύου και η χρήση του λογισμικού Virtual Private Networking (VPN) στο Guest VM θα ήταν αρκετή για την προστασία του απορρήτου και της ακεραιότητας του δικτύου από έναν κακόβουλο Dom0-admin.

Από αυτά τα σενάρια, παρατηρούμε ότι η προστασία που παρέχεται στις συνδέσεις εικονικού δικτύου είναι ισοδύναμη με το φυσικό δίκτυο όταν συνδέεται σε ένα μη αξιόπιστο δίκτυο. Ωστόσο, η χρήση παραδοσιακών εργαλείων IDS (Intrusion Detection System) [56], [57] σε συμβατικά δίκτυα θα έλυνε τέτοια προβλήματα, αλλά η χρήση τους σε περιβάλλον υπολογιστικού νέφους δεν θα ήταν η κατάλληλη λύση για τον εντοπισμό ύποπτων δραστηριοτήτων λόγω των ιδιαίτερων χαρακτηριστικών του νέφους.

Επικοινωνία μεταξύ εικονικών μηχανών:

Οι απειλές κατά της επικοινωνίας μεταξύ εικονικών μηχανών εξαρτώνται από τον τρόπο ανάπτυξης αυτών των μηχανημάτων (π.χ. κοινή χρήση φυσικού υπολογιστή μεταξύ πολλών οργανισμών). Η κοινή χρήση πόρων μεταξύ εικονικών μηχανών μπορεί να εκθέσει την ασφάλεια κάθε εικονικής μηχανής, για παράδειγμα, η συνεργασία μεταξύ ορισμένων εφαρμογών, όπως ένα κοινόχρηστο πρόχειρο, επιτρέπει τη μεταφορά δεδομένων μεταξύ των εικονικών μηχανών και του κεντρικού υπολογιστή, βοηθώντας κακόβουλα προγράμματα σε εικονικά μηχανήματα να ανταλλάσσουν δεδομένα μέσω των οποίων παραβιάζουν την ασφάλεια και το απόρρητο. Ένα κακόβουλο VM

[21] Το Dom0 είναι μια συντομογραφία για τον Domain 0, τον τομέα διαχείρισης ή ελέγχου με προνομιακή πρόσβαση στο υλικό και τα προγράμματα οδήγησης συσκευών.

μπορεί ενδεχομένως να έχει πρόσβαση σε άλλα VM μέσω κοινόχρηστης μνήμης, συνδέσεων δικτύου και οποιονδήποτε άλλο κοινόχρηστο πόρο χωρίς να θέτει όμως σε κίνδυνο το επίπεδο του hypervisor. Οι κρίσιμοι κίνδυνοι τέτοιων δικτυακών περιβαλλόντων παρακίνησαν τους ερευνητές να παρέχουν προστατευτικές λύσεις και τεχνικές για την διασφάλιση της επικοινωνίας μεταξύ των VM.

Πρώτον, η τεχνική TVDc (που αναφέρθηκε και προηγουμένως) στο [51] αναπτύχθηκε για να παρέχει απομόνωση του φόρτου εργασίας των πελατών μεταξύ τους για να αποτρέψει τη διαρροή δεδομένων, επομένως αποτρέπει τα VM από τη διάδοση ιών και άλλων κακόβουλων προγραμμάτων.

Δεύτερον, στο [58] προτείνεται ένα IDS για περιβάλλον υπολογιστών πλέγματος και υπολογιστικού νέφους. Η προτεινόμενη προσέγγιση εφαρμόζει δύο τεχνικές ανίχνευσης εισβολής στα δεδομένα που συλλέγονται από το νέφος:

I- Μέθοδος που βασίζεται στη συμπεριφορά για την επαλήθευση των ενεργειών του χρήστη που αντιστοιχούν σε γνωστά προφίλ συμπεριφοράς.

II- Μέθοδος που βασίζεται στην πρότερη γνώση για την επαλήθευση παραβιάσεων της πολιτικής ασφαλείας και γνωστών επιθέσεων προτύπων.

Ωστόσο, σύμφωνα με τα αποτελέσματα των πρωτοτύπων που εφαρμόστηκαν, η εφαρμογή και των δύο τεχνικών μαζί επέτυχε υψηλότερο επίπεδο ασφάλειας και χαμηλότερο ποσοστό ψευδώς θετικών και αρνητικών. Δυστυχώς, αυτή η προσέγγιση λειτουργεί μόνο για εισβολή στο επίπεδο του ενδιάμεσου λογισμικού (δηλαδή, PaaS) και αξίζει μια πιο λεπτομερής έρευνα για να επεκταθεί στο IaaS.

Τρίτον, μια εικονική μηχανή ασφαλείας (SVM) παρέχει ανάλυση όλης της κίνησης του εικονικού δικτύου χρησιμοποιώντας ένα σύστημα πρόληψης εισβολής (Intrusion Prevention System). Το IPS, μια προηγμένη έκδοση του Intrusion Detection Systems, είναι ικανό να ανιχνεύει και να αποτρέπει τόσο γνωστές όσο και άγνωστες επιθέσεις.

Τέταρτον, τα Rootkits [59] είχαν αρχικά δημιουργηθεί ως εφαρμογές για να βοηθήσουν στην απόκτηση ελέγχου ενός συστήματος που αποτυγχάνει ή δεν ανταποκρίνεται, αλλά τελευταία, χρησιμοποιούνται ως κακόβουλο λογισμικό για να βοηθήσουν τους εισβολείς να έχουν πρόσβαση σε συστήματα αποφεύγοντας τον εντοπισμό. Μια προσέγγιση anti-rootkit προτάθηκε στο [60] για αυτοματοποιημένο εντοπισμό και περιορισμό των δικαιωμάτων χρήστη, καθώς και για επιθέσεις rootkit σε επίπεδο πυρήνα και άλλα κακόβουλα προγράμματα που χρησιμοποιούν rootkit για κάλυψη.

Τέλος, έχει προταθεί το Anti-DDoS Virtualized Operating System (ADVOS) [61] για την ασφάλεια των δικτυωμένων υπολογιστών από επιθέσεις DDoS. Το ADVOS ενσωματώνει δυνατότητες anti-DDoS σε λειτουργικά συστήματα φιλτράροντας πακέτα που έρχονται από τον ίδιο υπολογιστή προέλευσης για την ταξινόμηση της κακόβουλης κυκλοφορίας. Επιπλέον, το anti-DDoS μετακινήθηκε εκτός του κεντρικού υπολογιστή σε ανεξάρτητο τομέα για την προστασία του anti-DDoS host από κακόβουλο κώδικα. Το ADVOS δεν προτείνεται να χρησιμοποιηθεί στο νέφος, αλλά ενδεχομένως θα ήταν μια εφικτή και αποτελεσματική λύση για άμυνα απέναντι στο DDoS σε οποιοδήποτε περιβάλλον εικονικοποίησης, ειδικά για το IaaS.

Κινητικότητα εικονικών μηχανών (VM Mobility):

Η κινητικότητα είναι ένα χαρακτηριστικό που επιτρέπει στα εικονικά μηχανήματα να μεταφέρονται σε άλλα φυσικά μηχανήματα όπου τα περιεχόμενα του εικονικού δίσκου για κάθε εικονική μηχανή αποθηκεύονται ως αρχείο. Η κινητικότητα είναι απαραίτητη για τη συντήρηση συστημάτων και την εξισορρόπηση φορτίου, αλλά θα αποτελούσε πηγή κινδύνου για την ασφάλεια (π.χ., το αρχείο VM μπορεί να κλαπεί χωρίς φυσική κλοπή του κεντρικού υπολογιστή). Η ακεραιότητα μιας εικονικής μηχανής εκτός σύνδεσης μπορεί να τεθεί σε κίνδυνο εάν ο κεντρικός υπολογιστής δεν είναι ασφαλής και προστατευμένος. Για παράδειγμα, οι επιθέσεις εκτός σύνδεσης μπορεί

να προκύψουν με την αντιγραφή ενός VM εκτός σύνδεσης μέσω του δικτύου σε ένα φορητό μέσο αποθήκευσης και την πρόσβαση ή την καταστροφή δεδομένων στο host μηχάνημα χωρίς να κλαπεί φυσικά κανένας σκληρός δίσκος. Από την άλλη πλευρά, η μετεγκατάσταση ζωντανής (live migration), δηλαδή εν λειτουργία, εικονικής μηχανής μπορεί να είναι μια σοβαρή απειλή για την εικονική μηχανή. Οι τεχνικές ζωντανής μετεγκατάστασης συνήθως υλοποιούνται αντιγράφοντας τις σελίδες μνήμης του VM προέλευσης στο VM προορισμού.

Στο [62], τρεις κατηγορίες επιθέσεων «live migration» κατά ζωντανών VM διερευνήθηκαν για να δείξουν τη σημασία της διασφάλισης της διαδικασίας migration. Επιπλέον, στο [38] αποδεικνύεται πώς ένα κακόβουλο μέρος μπορεί να εκμεταλλευτεί κάποιες εκδόσεις των Xen[22] και VMware και προτείνεται ένα μοντέλο αμοιβαίου ελέγχου ταυτότητας μεταξύ των VM προέλευσης και προορισμού για την προστασία της διαδικασίας μετεγκατάστασης μέσω του δικτύου, όπως αναφέρθηκε προηγουμένως.

Denial of Service (DoS):

Οι επιθέσεις Denial of Service (DoS) σε εικονικό περιβάλλον αποτελούν κρίσιμη απειλή για τα VM. Αυτές οι επιθέσεις μπορεί να είναι αποτέλεσμα λανθασμένης διαμόρφωσης ενός hypervisor που επιτρέπει σε ένα μόνο VM να καταναλώνει όλους τους διαθέσιμους πόρους, με αποτέλεσμα να εξαφανίζεται οποιοδήποτε άλλο VM που εκτελείται στον ίδιο φυσικό υπολογιστή και να αλλοιώνεται η σωστή λειτουργία των κεντρικών υπολογιστών δικτύου λόγω της έλλειψης πόρων. Ωστόσο, οι hypervisors εμποδίζουν οποιαδήποτε εικονική μηχανή να αποκτήσει 100% χρήση οποιωνδήποτε κοινόχρηστων πόρων υλικού, συμπεριλαμβανομένης της CPU, της RAM, του εύρους ζώνης δικτύου και της μνήμης γραφικών. Επιπλέον, μια κατάλληλη διαμόρφωση του hypervisor επιτρέπει την ανίχνευση ακραίας

[22] Είναι ένας hypervisor, που παρέχει υπηρεσίες που επιτρέπουν σε πολλά VMs να εκτελούνται ταυτόχρονα στο ίδιο υλικό υπολογιστή

κατανάλωσης πόρων και την λήψη κατάλληλων αποφάσεων, π.χ. αυτόματη επανεκκίνηση του VM, ωστόσο, η επανεκκίνηση του VM έχει μικρότερο αποτέλεσμα από την επανεκκίνηση ενός φυσικού μηχανήματος, καθώς τα VM μπορούν συνήθως να αρχικοποιηθούν πολύ πιο γρήγορα από τα φυσικά μηχανήματα επειδή δεν υπάρχει ανάγκη προετοιμασίας και επαλήθευσης υλικού.

5

Κριτήρια καταλληλόλητας παρόχου

5.1 Τρόπος προσέγγισης

Τα τελευταία χρόνια, έχει παρατηρηθεί αυξανόμενη ανάπτυξη και χρήση υπηρεσιών υπολογιστικού νέφους. Παρά τα αρχικά θετικά αποτελέσματα, είναι δύσκολο στην πράξη να βρεθεί ο κατάλληλος πάροχος που να ταιριάζει με τις απαιτήσεις κάθε φορέα. Επιπλέον, η διαδικασία σύγκρισης περιπλέκεται από πολλούς νεοεισερχόμενους παρόχους καθώς και από προσφορές μη διαφανών υπηρεσιών, οι οποίες μερικές φορές διαφέρουν σημαντικά. Για το σκοπό αυτό, καθορίστηκαν οι στοχευόμενες μετρικές για το ‘Cloud Computing from a customer’s perspective’, βασισμένες σε συνεντεύξεις ειδικών [63], μια διεθνής βιβλιογραφική ανασκόπηση και μια ανάλυση της αγοράς παρόχων νέφους (IaaS και hosting).

5.2 Ποιότητα Υπηρεσίας και SLA

Οι υπηρεσίες νέφους σχετίζονται με μια σειρά από χαρακτηριστικά QoS, όπως απόδοση, αξιοπιστία, ασφάλεια, τιμές, απόρρητο, χρηστικότητα κ.λπ. Αυτά τα διαφορετικά χαρακτηριστικά QoS καθιστούν τη διαδικασία επιλογής υπηρεσίας

σημαντικά δύσκολη. Για παράδειγμα, οι πάροχοι υπηρεσιών και οι καταναλωτές μπορεί να έχουν διαφορετικές προσδοκίες (ή μέτρηση) των χαρακτηριστικών QoS [64], [65]. Υπάρχει όμως έλλειψη τυπικού σημείου αναφοράς για τη μέτρηση του QoS στο νέφος. Αν και το SMI[23] (Service Measurement Index) είναι ένα βήμα προς τα εμπρός για την τυποποίηση του QoS στο νέφος, εξακολουθεί να μην παρέχει όλες τις απαραίτητες μετρήσεις που ανταποκρίνονται στις προσδοκίες τόσο των καταναλωτών όσο και των παρόχων.

Η SLA διασφαλίζει ότι οι πάροχοι υπηρεσιών και οι καταναλωτές συμμορφώνονται με τους όρους και τις προϋποθέσεις της σύμβασης. Για παράδειγμα, οι υπηρεσίες νέφους παρέχονται με τρόπο που να πληροί τις απαιτήσεις QoS. Παράλληλα όμως, η SLA κάνει επίσης δύσκολη την επιλογή υπηρεσιών. Διαφορετικοί πάροχοι υπηρεσιών ακολουθούν ιδιόκτητες SLA και υπάρχει έλλειψη τυποποίησης της SLA για υπηρεσίες νέφους.

5.3 Παροχή υπηρεσιών κατ' απαίτηση

Οι υπηρεσίες νέφους θα πρέπει να παρέχονται αυτόματα σε στυλ αυτοεξυπηρέτησης κατ' απαίτηση (on-demand) που σημαίνει ότι απαιτούν ελάχιστη ή καθόλου ανθρώπινη παρέμβαση. Ωστόσο, προτού διασφαλιστεί αυτή η αυτόματη παροχή υπηρεσιών, οι καταναλωτές πρέπει να προσδιορίσουν και να κατανοήσουν σωστά τις τεχνικές πολυπλοκότητες των υπηρεσιών νέφους. Για παράδειγμα, η υπηρεσία αναζήτησης και επιλογής από το Intel Cloud Finder δεν μπορεί να χρησιμοποιηθεί ή να γίνει κατανοητή από τους καταναλωτές υπηρεσιών, εκτός εάν έχουν καλή γνώση των τεχνολογιών υπολογιστικού νέφους.

[23] Το SMI λειτουργεί αφήνοντας τους καταναλωτές υπηρεσιών cloud να τις αξιολογήσουν, μέσω τυποποιημένων ερευνών, με βάση έξι βασικές μετρήσεις: ποιότητα, ευελιξία, κίνδυνος, κόστος, δυνατότητες και ασφάλεια. Υπάρχει μια μεγάλη και αυξανόμενη βάση δεδομένων με ολοκληρωμένες έρευνες και επί του παρόντος έχουν αξιολογηθεί περισσότερες από 120 υπηρεσίες.

5.4 Elasticity

Η ελαστικότητα είναι ένα από τα βασικά χαρακτηριστικά του υπολογιστικού νέφους όπου οι υπηρεσίες μπορούν να παρέχονται και να απελευθερώνονται ελαστικά. Από τη μία πλευρά, αυτό επιτρέπει στους καταναλωτές να αποκτούν ή να απελευθερώνουν πόρους με βάση τις ανάγκες τους. Από την άλλη πλευρά, αυτό επιτρέπει στους παρόχους να κατανέμουν και να ελευθερώνουν πόρους ανάλογα με τη διαθεσιμότητα και τη ζήτηση της υπηρεσίας. Ωστόσο, η ενσωμάτωση της ελαστικότητας στην επιλογή υπηρεσιών απαιτεί τη γνώση των δυναμικών αλλαγών στην κατανάλωση και την παροχή υπηρεσιών και ένα εργαλείο που μπορεί να παρακολουθεί τέτοιες αλλαγές.

5.5 Συγκέντρωση και διανομή πόρων

Οι πόροι του νέφους, όπως η ο αποθηκευτικός χώρος, η CPU, η μνήμη και το εύρος ζώνης δικτύου συγκεντρώνονται από τους παρόχους υπηρεσιών με τέτοιο τρόπο ώστε πολλοί καταναλωτές να μπορούν να χρησιμοποιούν τους ίδιους πόρους χρησιμοποιώντας μια ποικιλία μοντέλων, όπως μοντέλα πολλαπλής μίσθωσης και εικονικοποίησης. Οι καταναλωτές μπορούν να έχουν πρόσβαση σε πόρους του παρόχου με διαφάνεια χωρίς να γνωρίζουν την γεωγραφική θέση των (παρεχόμενων) υπηρεσιών. Αν και αυτή η διαφάνεια είναι χρήσιμη, μπορεί να προκαλέσει ζητήματα όπως η ασφάλεια, το απόρρητο και η αξιοπιστία των υπηρεσιών ή οποιεσδήποτε άλλες πτυχές QoS (όπως περιγράφεται παραπάνω). Για παράδειγμα, οι καταναλωτές υπηρεσιών μπορεί να εκφράσουν ανησυχίες σχετικά με τις τοποθεσίες των υπηρεσιών, εάν δεν είναι αξιόπιστες και ασφαλείς.

5.6 Μοντέλα παροχής υπηρεσιών

Οι υπηρεσίες νέφους υπάγονται γενικά σε ένα από τα τρία μοντέλα: SaaS (λογισμικό ως υπηρεσία), PaaS (πλατφόρμα ως υπηρεσία) και IaaS (υποδομή ως υπηρεσία). Αυτά τα μοντέλα απαιτούν εργαλεία επιλογής υπηρεσιών για να μπορούν οι χρήστες να μπορούν να προσδιορίζουν τις ανάγκες τους σύμφωνα με τα μοντέλα παροχής υπηρεσιών που θέλουν να χρησιμοποιήσουν για τη λήψη/χρήση υπηρεσιών νέφους. Για παράδειγμα, το μοντέλο IaaS μπορεί να απαιτεί περισσότερες λεπτομέρειες χαμηλού επιπέδου (όπως μνήμη, CPU, κ.λπ.) από το SaaS που απαιτεί περισσότερες λεπτομέρειες υψηλού επιπέδου για υπηρεσίες (όπως ταχύτητα, χρηστικότητα κ.λπ.).

5.7 Μοντέλα ανάπτυξης υπηρεσιών

Τα πιο κοινά μοντέλα ανάπτυξης νέφους είναι: δημόσιο νέφος, κοινοτικό νέφος, ιδιωτικό νέφος και υβριδικό νέφος. Το δημόσιο νέφος προσφέρει μεγαλύτερη ευελιξία όσον αφορά την παροχή υπηρεσιών, αλλά απαιτεί επίσης μεγαλύτερο επίπεδο ασφάλειας και ιδιωτικότητας. Το ιδιωτικό νέφος θεωρείται πιο ασφαλές αλλά περιορίζεται στην παροχή υπηρεσιών μέσω ενός ιδιωτικού δικτύου και μιας ιδιωτικής φιλοξενίας. Επομένως, τα εργαλεία επιλογής υπηρεσιών νέφους θα πρέπει να σχεδιάζονται με τρόπο που να καλύπτει το απαιτούμενο επίπεδο QoS και SLA των διαφορετικών μοντέλων ανάπτυξης.

5.8 Συμπεράσματα

Η ωριμότητα των λύσεων επιλογής υπηρεσιών όχι μόνο θα πρέπει να βελτιώσει και να απλοποιήσει τη διαδικασία επιλογής υπηρεσιών, αλλά θα πρέπει επίσης να ανοίξει νέες κατευθύνσεις στην έρευνα του cloud computing. Παραπάνω αναλύονται

οι παράμετροι οι οποίες θα πρέπει να ληφθούν υπ' όψιν πριν την επιλογή ενός παρόχου υπολογιστικού νέφους όμως πέραν αυτών, θα πρέπει να συνυπολογιστούν και ορισμένοι κίνδυνοι οι οποίοι μπορεί να προκύψουν μετά την επιλογή παρόχου. Ορισμένοι από αυτούς περιγράφονται ως εξής.

- *Εναλλαγή υπηρεσιών ή μετεγκατάσταση*: Τα εργαλεία και οι τεχνικές επιλογής υπηρεσιών μπορούν να επιτρέψουν τη διαφανή και απρόσκοπτη μετεγκατάσταση υπηρεσιών από έναν πάροχο νέφους σε έναν άλλο. Για παράδειγμα, το uSwitch παρέχει μια διαδικτυακή υπηρεσία σύγκρισης και εναλλαγής προκειμένου να βοηθήσει τους χρήστες να συγκρίνουν τις τιμές υπηρεσιών κοινής ωφέλειας και προϊόντα όπως φυσικό αέριο, ηλεκτρισμός, τηλέφωνο κ.λπ., από διαφορετικούς προμηθευτές. Με βάση τη σύσταση της uSwitch, οι πελάτες μπορούν στη συνέχεια να αλλάξουν τις υπηρεσίες τους από τον έναν προμηθευτή στον άλλο. Στο μέλλον, θα πρέπει να αναπτυχθούν εργαλεία και τεχνικές στο νέφος, ώστε οι χρήστες του να μπορούν εύκολα να αλλάξουν τις υπηρεσίες τους από τον έναν πάροχο στον άλλο. Ωστόσο, οι τρέχουσες λύσεις δεν παρέχουν εύκολη εναλλαγή ή μετεγκατάσταση υπηρεσιών. Η απουσία εγκαταστάσεων για εναλλαγή υπηρεσιών είναι επίσης ένας από τους κύριους λόγους για το πρόβλημα κλειδώματος.
- *Κλείδωμα προμηθευτή νέφους*: Το πρόβλημα του κλειδώματος προμηθευτή είναι ένα από τα σημαντικότερα εμπόδια στην υιοθέτηση τεχνολογιών νέφους. Λόγω της πολυπλοκότητας των υπηρεσιών νέφους, πολλοί χρήστες μένουν με τους υπάρχοντες παρόχους, παρόλο που μπορεί να μην ικανοποιούν τις ανάγκες τους. Παρόμοια με τις υπηρεσίες κοινής ωφέλειας (όπως φυσικό αέριο, ηλεκτρισμός, τηλέφωνο), οι χρήστες νέφους δεν πρέπει να μένουν κλειδωμένοι με έναν προμηθευτή. Αντίθετα, θα πρέπει να υπάρχουν εργαλεία, τεχνικές και μέθοδοι που να βοηθούν στην επίλυση του προβλήματος κλειδώματος.
- *Cloud brokers*: Ο σχεδιασμός και η ανάπτυξη υπηρεσιών cloud broker μπορεί να βοηθήσει και να συμβουλεύσει τους χρήστες και τους παρόχους cloud σχετικά με την επιλογή και την παροχή υπηρεσιών

νέφους. Οι μεσίτες νέφους θα λειτουργούν ως μεσάζοντες μεταξύ παρόχων και χρηστών νέφους. Οι υπηρεσίες μεσιτών μπορούν να επωφεληθούν από τα εργαλεία επιλογής υπηρεσιών νέφους, καθώς μπορούν να προτείνουν κατάλληλες υπηρεσίες στους χρήστες.

6

Βιβλιογραφία

[1] "What is the cloud? | Cloud definition," *Cloudflare*. https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (accessed Oct. 11, 2022).

[2] "A Comprehensive Study on Cloud Computing," *IJCSMC*.

[3] T. Y. Chernysheva, "Preliminary Risk Assessment in it Projects," *Applied Mechanics and Materials*, vol. 379, pp. 220–223, 2013, doi: 10.4028/www.scientific.net/AMM.379.220.

[4] S. V. Razumnikov, "Assessing Efficiency of Cloud-Based Services by the Method of Linear Programming," *Applied Mechanics and Materials*, vol. 379, pp. 235–239, 2013, doi: 10.4028/www.scientific.net/AMM.379.235.

[5] M. G. Avram, "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective," *Procedia Technology*, vol. 12, pp. 529–534, 2014, doi: 10.1016/j.protcy.2013.12.525.

[6] L. B. A. Rabai, M. Jouini, A. B. Aissa, and A. Mili, "A cybersecurity model in cloud computing environments," *Journal of King Saud University - Computer and Information Sciences*, vol. 25, no. 1, Art. no. 1, 2012, Accessed: Oct. 13, 2022. [Online]. Available: https://cyberleninka.org/article/n/974626

[7] S. Rajan and A. Jairath, "Cloud Computing: The Fifth Generation of Computing," in *2011 International Conference on Communication Systems and Network Technologies*, Jun. 2011, pp. 665–667. doi: 10.1109/CSNT.2011.143.

[8] J. Brodkin, "5 problems with SaaS security," *Network World*, Sep. 27, 2010. https://www.networkworld.com/article/2219462/5-problems-with-saas-security.html (accessed Oct. 13, 2022).

[9] W. Petruska, "How University Data Backup Is Moving Online," presented at the Educause Conference Anaheim, California, 2010.

[10] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, Sao Carlos, Brazil, Nov. 2012, pp. 198–205. doi: 10.1109/CASoN.2012.6412402.

[11] "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing." https://ieeexplore.ieee.org/document/5719003 (accessed Oct. 14, 2022).

[12] "Which is less expensive: Amazon or self-hosted? | Open Spectrum." https://openspectruminc.com/which-is-less-expensive-amazon-or-self-hosted/ (accessed Oct. 14, 2022).

[13] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," Apr. 2010, pp. 1–8.

[14] E. Toews, B. Satchwill, R. Rankin, J. Shillington, and T. King, “An internationally distributed cloud for science: the cloud-enabled space weather platform,” in *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing*, New York, NY, USA, Feb. 2011, pp. 1–7. doi: 10.1145/1985500.1985502.

[15] Songjie, J. Yao, and C. Wu, “Cloud computing and its key techniques,” Aug. 2011, pp. 320–324. doi: 10.1109/EMEIT.2011.6022935.

[16] J. Martins, J. Pereira, S. Fernandes, and J. Cachopo, “Towards a Simple Programming Model in Cloud Computing Platforms,” Nov. 2011, pp. 83–90. doi: 10.1109/NCCA.2011.21.

[17] Z. Mahmood, “Cloud Computing: Characteristics and Deployment Approaches,” in *2011 IEEE 11th International Conference on Computer and Information Technology*, Dec. 2011, pp. 121–126. doi: 10.1109/CIT.2011.75.

[18] “Cloud Foundry – Open-Source Cloud Native Application Delivery,” *Cloud Foundry*. https://www.cloudfoundry.org/ (accessed Oct. 17, 2022).

[19] P. Hu and F. Hu, “An optimized strategy for cloud computing architecture,” in *2010 3rd International Conference on Computer Science and Information Technology*, Jul. 2010, vol. 9, pp. 374–378. doi: 10.1109/ICCSIT.2010.5564912.

[20] J. C. Mudge, P. Chandrasekhar, G. S. Heinson, and S. Thiel, “Evolving Inversion Methods in Geophysics with Cloud Computing - A Case Study of an eScience Collaboration,” in *2011 IEEE Seventh International Conference on eScience*, Sep. 2011, pp. 119–125. doi: 10.1109/eScience.2011.25.

[21] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, “Security issues in cloud environments: a survey,” *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, Apr. 2014, doi: 10.1007/s10207-013-0208-7.

[22] R. Chandramouli, M. Iorga, and S. Chokhani, “Cryptographic Key Management Issues and Challenges in Cloud Services,” in *Secure Cloud Computing*, S. Jajodia, K. Kant, P. Samarati, A. Singhal, V. Swarup, and C. Wang, Eds. New York, NY: Springer, 2014, pp. 1–30. doi: 10.1007/978-1-4614-9278-8_1.

[23] “A survey of mobile cloud computing: architecture, applications, and approaches”, doi: 10.1002/wcm.1203.

[24] W. Lloyd, S. Pallickara, O. David, J. Lyon, M. Arabi, and K. Rojas, “Performance implications of multi-tier application deployments on Infrastructure-as-a-Service clouds: Towards performance modeling,” *Future Generation Computer Systems*, vol. 29, no. 5, pp. 1254–1264, Jul. 2013, doi: 10.1016/j.future.2012.12.007.

[25] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, Apr. 2012, doi: 10.1109/TSC.2011.24.

[26] K. Salah, J. M. Alcaraz Calero, S. Zeadally, S. Al-Mulla, and M. Alzaabi, “Using Cloud Computing to Implement a Security Overlay Network,” *IEEE Security & Privacy*, vol. 11, no. 1, pp. 44–53, Jan. 2013, doi: 10.1109/MSP.2012.88.

[27] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 5, Feb. 2013, doi: 10.1186/1869-0238-4-5.

[28] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, “A review on remote data auditing in single cloud server: Taxonomy and open issues,” *Journal*

of Network and Computer Applications, vol. 43, pp. 121–141, Aug. 2014, doi: 10.1016/j.jnca.2014.04.011.

[29] Y. Hu, T. Li, P. Yang, and K. Gopalan, "An Application-Level Approach for Privacy-Preserving Virtual Machine Checkpointing," in *2013 IEEE Sixth International Conference on Cloud Computing*, Jun. 2013, pp. 59–66. doi: 10.1109/CLOUD.2013.28.

[30] "OWASP Top 10 Vulnerabilities," *Check Point Software*. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/ (accessed Jan. 02, 2023).

[31] S. Sharma, U. Tim, J. Wong, S. Gadia, and S. Sharma, "A Brief Review on Leading Big Data Models," *Data Science Journal*, Dec. 2014, doi: 10.2481/dsj.14-041.

[32] S. Sharma, "An Extended Classification and Comparison of NoSQL Big Data Models." arXiv, Oct. 06, 2015. doi: 10.48550/arXiv.1509.08035.

[33] "International Journal of Business Information Systems (IJBIS) Inderscience Publishers - linking academia, business and industry through research." https://www.inderscience.com/jhome.php?jcode=ijbis (accessed Jan. 02, 2023).

[34] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee, Eds. London: Springer London, 2013, pp. 3–42. doi: 10.1007/978-1-4471-4189-1_1.

[35] E. S. Dove, Y. Joly, A.-M. Tassé, Public Population Project in Genomics and Society (P3G) International Steering Committee, International Cancer Genome Consortium (ICGC) Ethics and Policy Committee, and B. M. Knoppers, "Genomic cloud computing: legal and ethical points to consider," *Eur J Hum Genet*, vol. 23, no. 10, pp. 1271–1278, Oct. 2015, doi: 10.1038/ejhg.2014.196.

[36] E. Ayday, E. De Cristofaro, J.-P. Hubaux, and G. Tsudik, "The Chills and Thrills of Whole Genome Sequencing." arXiv, Feb. 16, 2015. doi: 10.48550/arXiv.1306.1264.

[37] Y. Huang and I. Goldberg, "Outsourced private information retrieval," in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, Berlin Germany, Nov. 2013, pp. 119–130. doi: 10.1145/2517840.2517854.

[38] K. Lauter, A. Lopez-Alt, and M. Naehrig, "Private Computation on Encrypted Genomic Data." 2015. Accessed: Jan. 02, 2023. [Online]. Available: https://eprint.iacr.org/2015/133

[39] M. Gostev *et al.*, "SAIL—a software system for sample and phenotype availability across biobanks and cohorts," *Bioinformatics*, vol. 27, no. 4, pp. 589–591, Feb. 2011, doi: 10.1093/bioinformatics/btq693.

[40] A. Gholami, E. Laure, P. Somogyi, O. Spjuth, S. Niazi, and J. Dowling, "Privacy-Preservation for Publishing Sample Availability Data with Personal Identifiers," *JOMB*, vol. 4, no. 2, pp. 117–125, 2015, doi: 10.12720/jomb.4.2.117-125.

[41] "ScaBIA: Scalable Brain Image Analysis in the Cloud:," in *Proceedings of the 3rd International Conference on Cloud Computing and Services Science*, Aachen, Germany, 2013, pp. 329–336. doi: 10.5220/0004358003290336.

[42] A. Gholami and E. Laure, "Advanced Cloud Privacy Threat Modeling," in *Computer Science & Information Technology (CS & IT)*, Jan. 2016, pp. 229–239. doi: 10.5121/csit.2016.60120.

[43] A. Gholami, J. Dowling, and E. Laure, "A security framework for population-scale genomics analysis," in *2015 International Conference on High Performance*

Computing & Simulation (HPCS), Jul. 2015, pp. 106–114. doi: 10.1109/HPCSim.2015.7237028.
[44] A. Gholami, A.-S. Lind, J. Reichel, J.-E. Litton, A. Edlund, and E. Laure, "Privacy Threat Modeling for Emerging BiobankClouds," *Procedia Computer Science*, vol. 37, pp. 489–496, 2014, doi: 10.1016/j.procs.2014.08.073.
[45] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," in *2008 10th IEEE International Conference on High Performance Computing and Communications*, Sep. 2008, pp. 5–13. doi: 10.1109/HPCC.2008.172.
[46] D. Nurmi *et al.*, "The Eucalyptus Open-Source Cloud-Computing System," in *2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, Shanghai, China, 2009, pp. 124–131. doi: 10.1109/CCGRID.2009.93.
[47] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc., 2009.
[48] "XML signature element wrapping attacks and countermeasures | Proceedings of the 2005 workshop on Secure web services." https://dl.acm.org/doi/10.1145/1103022.1103026 (accessed Nov. 15, 2022).
[49] "On Technical Security Issues in Cloud Computing | IEEE Conference Publication | IEEE Xplore." https://ieeexplore.ieee.org/document/5284165 (accessed Nov. 15, 2022).
[50] "Terra: a virtual machine-based platform for trusted computing: ACM SIGOPS Operating Systems Review: Vol 37, No 5." https://dl.acm.org/doi/10.1145/1165389.945464 (accessed Nov. 27, 2022).
[51] S. Berger *et al.*, "TVDc: Managing Security in the Trusted Virtual Datacenter," *Operating Systems Review*, vol. 42, pp. 40–47, Aug. 2008.
[52] S. Berger *et al.*, "Security for the cloud infrastructure: Trusted virtual data center implementation," *IBM J. Res. & Dev.*, vol. 53, no. 4, p. 6:1-6:12, Jul. 2009, doi: 10.1147/JRD.2009.5429060.
[53] V. Rajaravivarma, "Virtual local area network technology and applications," in *Proceedings The Twenty-Ninth Southeastern Symposium on System Theory*, Mar. 1997, pp. 49–52. doi: 10.1109/SSST.1997.581577.
[54] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "vTPM: Virtualizing the Trusted Platform Module," p. 16.
[55] D. G. Murray, G. Milos, and S. Hand, "Improving Xen security through disaggregation," in *Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments - VEE '08*, Seattle, WA, USA, 2008, p. 151. doi: 10.1145/1346256.1346278.
[56] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," p. 27.
[57] K. A. Jackson, "INTRUSION DETECTION SYSTEM (IDS) PRODUCT SURVEY," p. 106.
[58] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing," *IT Prof.*, vol. 12, no. 4, pp. 38–43, Jul. 2010, doi: 10.1109/MITP.2009.89.
[59] S. T. King and P. M. Chen, "SubVirt: implementing malware with virtual machines," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley/Oakland, CA, 2006, p. 14 pp. – 327. doi: 10.1109/SP.2006.38.
[60] A. Baliga, L. Iftode, and X. Chen, "Automated containment of rootkits attacks," *Computers & Security*, vol. 27, no. 7, pp. 323–334, Dec. 2008, doi: 10.1016/j.cose.2008.06.003.

[61] “Anti-DDoS Virtualized Operating System | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/document/4529407 (accessed Nov. 29, 2022).
[62] J. Oberheide, E. Cooke, and F. Jahanian, “Empirical Exploitation of Live Virtual Machine Migration,” p. 6.
[63] J. Repschläger, S. Wind, R. Zarnekow, and K. Turowski, “Developing a Cloud Provider Selection Model”.
[64] M. Eisa, M. Younas, K. Basu, and H. Zhu, “Trends and Directions in Cloud Service Selection,” in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, Oxford, United Kingdom, Mar. 2016, pp. 423–432. doi: 10.1109/SOSE.2016.59.
[65] “A cloud service selection model using improved ranked voting method | Request PDF.” https://www.researchgate.net/publication/290074938_A_cloud_service_selection_model_using_improved_ranked_voting_method (accessed Jan. 03, 2023).
+