ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών: Κυβερνοασφάλεια

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

# ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

**Θεοδωράκος Ιωάννης**

AM: cscyb21007

Επιβλέπων Καθηγητής Δρ. Παναγιώτης Γιαννακόπουλος

Αθήνα, Δεκέμβριος 2023

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

| ΠΑΝΑΓΙΩΤΗΣ ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ | ΕΜΜΑΝΟΥΗΛ ΜΙΧΑΗΛΙΔΗΣ | ΔΗΜΗΤΡΙΟΣ ΚΟΓΙΑΣ |
|---|---|---|
| Panagiotis Giannakopoulos<br>Digitally signed by Panagiotis Giannakopoulos<br>Date: 2024.06.19 17:45:03 +03'00' | EMMANOUIL MICHAILIDIS<br>Digitally signed by EMMANOUIL MICHAILIDIS<br>Date: 2024.06.19 20:40:54 +03'00' | Dimitrios Kogias<br>Digitally signed by Dimitrios Kogias<br>Date: 2024.06.19 18:21:24 +03'00' |

**ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ**

Ο κάτωθι υπογεγραμμένος Θεοδωράκος Ιωάννης του Ευριπίδη, με αριθμό μητρώου cscyb21007 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφάλειας του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

# Περιεχόμενα

## Κατάλογος Εικόνων

## ΚατάλογοςΠινάκων

## Ακρωνύμια και συντμήσεις

ΜΔΥ: **Μ**ηχανές **Δ**ιανυσμάτων **Υ**ποστήριξης

ΤΠΕ: **Τ**εχνολογίες **Π**ληροφορικής και **Ε**πικοινωνιών

ΥΝ: **Υ**πολογιστικό **Ν**έφος

## Abbreviations

2FA: **T**wo-**F**actor-**A**uthentication

APIs: **A**pplication **P**rogramming **I**nterfaces

B2C: **B**usiness-**To**-**C**onsumer

BAU: **B**usiness-**a**s-**U**sual

BYOD: **B**ring **Y**our **O**wn **D**evice

CC: **C**loud **C**omputing

CFI: **C**ontrol-**F**low **I**ntegrity

CIA triad: **C**onfidentiality, **I**ntegrity, and **A**vailability

CSA: **C**loud **S**ecurity **A**lliance

CSP: **C**ontent **S**ecurity **P**olicy

CSP: **C**loud **S**ervice **P**rovider

CPU: **C**entral **P**rocessing **U**nit

DDoS: **D**istributed **D**enial of **S**ervice

DKSM **D**irect **K**ernel **S**tructure **M**anipulation

DNS: **D**omain **N**ame **S**ystem

DOM: **D**ocument **O**bject **M**odel

DoS: **D**enial **o**f **S**ervice

E-Commerce: **E**lectronic-**Commerce**

FTP: **F**ile **T**ransfer **P**rotocol

GRC: **G**overnance, **R**isk and **C**ompliance

HIPAA: **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

HTML: **H**yper**t**ext **M**ark-up **L**anguage

HTTP: **H**ypertext **T**ransfer **P**rotocol

HTTPS: **H**ypertext **T**ransfer **P**rotocol **S**ecure

IaaS: **I**nfrastructure **a**s **a** **S**ervice

IBA: **I**dentity-**B**ased **A**uthentication

ICLEEDS: **I**ntelligent **C**loud **B**ased **E**mail **E**ncryption and **D**ecryption **S**ystem

ICMP: **I**nternet **C**ontrol **M**essage **P**rotocol

IDS: **I**ntrusion **D**etection **S**ystem

IPS: **I**ntrusion **P**revention **S**ystem

IP: **I**nternet **P**rotocol

ISP: **I**ndependent **S**oftware **P**rovider

MiLAMoB: **Mi**ddleware **La**yer for **Mob**ile (Devices)

MLP: **M**ulti**l**ayer **P**erceptron

NAS: **N**etwork-**A**ttached **S**torage

NIST: **N**ational **I**nstitute of **S**tandards and **T**echnology

OAuth: **O**pen **Auth**orization

OS: **O**perating **S**ystem

OTP: **O**ne **T**ime **P**assword

P2P: **P**eer-**T**o-**P**eer

PaaS: **P**latform **a**s **a** **S**ervice

PII: **P**ersonally **I**dentifiable **I**nformation

PKI: **P**ublic **K**ey **I**nfrastructure

RFID: **R**adio **F**requency **I**dentification

ROP: **R**eturn-**O**riented **P**rogramming

RPC: **R**emote **P**rocedure **C**all

RSA: **R**ivest-**S**hamir-**A**dleman (encryption algorithm)

SaaS: **S**oftware **a**s **a** **S**ervice

SADI: **S**teganography **A**udio **D**ynamical **I**nterference

SAML: **S**ecurity **A**ssertion **M**arkup **L**anguage

SAN: **S**torage **A**rea **N**etwork

SCRIPT: **S**cale of **C**hildren's **R**eadiness **i**n **P**rinting

SLA: **S**ervice **L**evel **A**greement

SMC: **S**elf-**M**odifying **C**ode

SNMP: **S**imple **N**etwork **M**anagement **P**rotocol

SOA: **S**ervice-**O**riented **A**rchitecture

SOAP: **S**imple **O**bject **A**ccess **P**rotocol

SPI: **S**oftware, **P**latform, **I**nfrastructure

SPML: **S**ervices **P**rovisioning **M**arkup **L**anguage

SQL: **S**tructural **Q**uery **L**anguage

SQLi: **SQL**-**i**njection

SSO: **S**ingle **s**ign-**o**n

SSL: **S**ecure **S**ockets **L**ayer

SVM: **S**upport **V**ector **M**achine

URL: **U**niform **R**esource **L**ocator

vCPU: **v**irtual **CPU**

VM: **V**irtual **M**achine

vMemory: **v**irtual **Memory**

VPN: **V**irtual **P**rivate **N**etwork

W3C: **W**orld **W**ide **W**eb **C**onsortium

WAF: **W**eb **A**pplication **F**irewall

XACML: E**x**tensible **A**ccess **C**ontrol **M**arkup **L**anguage

XML: **E**xtensible **M**arkup **L**anguage

XSS: **C**ross-**S**ite **S**cripting

# Λεξικό όρων

Application Programming Interfaces: Διεπαφές προγραμματισμού εφαρμογών

Authentication server: Εξυπηρετητής αυθεντικοποίησης

Bring Your Own Device: Φέρε τη δική σου συσκευή

Broad Network Access: Ευρεία πρόσβαση στο δίκτυο

Browser: Φυλλομετρητής

Brute-force attack: Επίθεση ωμής βίας

Business-as-Usual: Καθημερινή λειτουργία μιας επιχείρησης

Central Processing Unit: Κεντρική Μονάδα Επεξεργασίας

CIA triad: Εμπιστευτικότητα, Ακεραιότητα και της Διαθεσιμότητα

Client-to-Client attacks: Επιθέσεις μεταξύ πελατών

Cloud Computing: Υπολογιστικό νέφος

Community Cloud: Κοινοτικό υπολογιστικό νέφος

Content-Security-Policy: Πολιτική Ασφάλειας Περιεχομένου

Cross VM Side-Channel Attacks: Επιθέσεις Πλευρικών Καναλιών

Customer fraud: Απάτη καταναλωτή

Decision Tree Induction: Επαγωγή με δέντρα απόφασης

Denial of Service(attack): Επίθεση άρνησης υπηρεσίας

Distributed Denial of Service (attacks): Κατανεμημένες επιθέσεις άρνησης υπηρεσίας

Deployment Models: Μοντέλα διάθεσης υπολογιστικού νέφους

DOM-based XSS attacks: Επιθέσεις XSS που βασίζονται σε DOM

Ensemble Machine Learning: Συλλογική μάθηση ή μηχανική εκμάθηση συνόλων

Escape characters: Χαρακτήρες διαφυγής

Governance, Risk and Compliance: Εταιρική Διακυβέρνηση, Διαχείριση Ρίσκου και Κανονιστική Συμμόρφωση

Guest-to-guest attacks: Επιθέσεις μεταξύ επισκεπτών / φιλοξενούμενων

Health Insurance Portability and Accountability Act: Νόμος περί φορητότητας και λογοδοσίας της ασφάλισης υγείας

Hybrid Cloud: Υβριδικό υπολογιστικό νέφος

Incident response: Απόκριση περιστατικού

Infrastructure as a Service: Η υποδομή ως υπηρεσία

K-Nearest Neighbor: Αλγόριθμος πλησιέστερης γειτνίασης

Keylogger attacks: Επιθέσεις καταγραφέα πλήκτρων

Maintenance: Τακτική προγραμματισμένη συντήρηση

Man-in-the-middle attack: Επιθέσεις τύπου «άνθρωπος στη μέση»

Massive scalability: Επεκτασιμότητα

Measured Services: Μετρήσιμη εξυπηρέτηση

Multi-Cloud: Πολυ-σύννεφο ή μοντέλο πολλαπλών σύννεφων

Multilayer Perceptron: Πολυεπίπεδοι αισθητήρες

Multitenancy: Πολυμίσθωση ή πολυμετοχικότητα

Naïve Bayes: Ταξινομητής Bayes

National Academy of Sciences: Εθνική Ακαδημία Επιστημών

Non-persistent or reflected XSS attacks: Μη επίμονες ή αντανακλαστικές XSS επιθέσεις

On-demand self-service: Διαθεσιμότητα κατ' απαίτηση

Operating System: Λειτουργικό σύστημα

Password discovery attacks: Επιθέσεις ανακάλυψης κωδικού πρόσβασης

Pay-as-you-go: Πληρωμή ανάλογα με τη χρήση.

Peer-To-Peer: Ομότιμα δίκτυα

Persistent or stored attacks: Επίμονες ή αποθηκευμένες επιθέσεις τύπου XSS

Personally Identifiable Information: Προσωπικά στοιχεία ταυτοποίησης

Phishing: Ηλεκτρονικό ψάρεμα

Platform as a Service: Η πλατφόρμα ως υπηρεσία

Private Cloud: Ιδιωτικό υπολογιστικό νέφος

Prepared Statements: Έτοιμες δηλώσεις

Public Cloud: Δημόσιο υπολογιστικό νέφος

Ransomware: Λυτρισμικό

Rapid Elasticity: Ταχεία ελαστικότητα

Resource Pooling: Συγκέντρωση πόρων

Reverse Engineering: Αντίστροφη ή ανάστροφη μηχανική

Scalability: Επεκτασιμότητα

Self-provisioning of resources: Αυτοπρομήθεια πόρων

Service Delivery Models: Μοντέλα υπηρεσιών υπολογιστικού νέφους

Service Level Agreement: Συμφωνίες επιπέδων εξυπηρέτησης / Συμφωνίες επιπέδου υπηρεσιών

Session hijacking attacks: Επιθέσεις κλοπής συνεδριών ή πειρατείες συνεδρίας

Software as a Service: Το λογισμικό ως υπηρεσία

Spoofing attacks: Επιθέσεις πλαστοπροσωπίας

Stakeholders: Βασικά ενδιαφερόμενα μέρη

Support Vector Machine: Μηχανές Διανυσμάτων Υποστήριξης

Two-factor-authentication: Έλεγχος ταυτότητας δύο παραγόντων

Virtual Machine: Εικονική μηχανή

Vendor lock-in: Κλείδωμα πωλητή

VM-to-VM attacks: Επιθέσεις μεταξύ εικονικών μηχανημάτων

Web Application Firewall: Τείχος προστασίας εφαρμογών

Web Services: Υπηρεσίες Ιστού

# Περίληψη

Στο **1ο Κεφάλαιο** της παρούσας διπλωματικής εργασίας παρουσιάζεται η έννοια του υπολογιστικού νέφους και περιγράφονται τόσο τα μοντέλα διάθεσής του όσο και τα διαφορετικά μοντέλα των προσφερόμενων υπηρεσιών. Επίσης, γίνεται λόγος για τη διακυβέρνηση στο υπολογιστικό νέφος και το πως διαμορφώνεται ο βαθμός ελέγχου ενός οργανισμού που έχει υιοθετήσει το *cloud* έναντι του παρόχου ανάλογα και με το επιλεγμένο μοντέλο διάθεσης. Τέλος, αναφέρονται οι έννοιες της εικονοποίησης των μηχανών που συνιστούν βασικό δομικό λίθο του τρόπου δημιουργίας των υπολογιστικών πόρων στο νέφος. Πολλοί είναι οι σκεπτικιστές της υιοθέτησης του υπολογιστικού νέφους. **Στο 2ο Κεφάλαιο** γίνεται ειδική μνεία στα πλεονεκτήματα και στα μειονεκτήματα της χρήσης του.

Στο **3ο Κεφάλαιο** αναλύονται διεξοδικά οι έννοιες που συνιστούν την ασφάλεια και την ιδιωτικότητα, ξεκινώντας από την CIA τριάδα. Όπως αναφέρεται χαρακτηριστικά όλες αυτές οι παράμετροι δεν είναι αποκλειστικό προνόμιο του υπολογιστικού νέφους, αλλά ξεκίνησαν από τα συμβατικά – παραδοσιακά υπολογιστικά συστήματα και βρίσκουν εφαρμογή σε όλες τις μηχανές που αποθηκεύουν, επεξεργάζονται και διαχειρίζονται δεδομένα και πληροφορίες.

Στο **4ο Κεφάλαιο** γίνεται μια ταξινόμηση των απειλών και των κινδύνων κάτω από πολλά και διαφορετικά πρίσματα και οπτικές. Αρχικά δίνεται μια γενική κατηγοριοποίηση, έπειτα επιχειρείται μια κατάταξη ανάλογα με το αν οι απειλές σχετίζονται με τον ανθρώπινο ή τον τεχνολογικό παράγοντα και στη συνέχεια γίνεται μια προσπάθεια συσχέτισης των κινδύνων ανά περιοχή του νέφους. Αναφέρονται επίσης τα τρία γενικά επίπεδα επιθέσεων καθώς και οι επιφάνειες των επιθέσεων ανά μοντέλο διάθεσης.

Στο **5ο Κεφάλαιο** γίνεται μια αναλυτική περιγραφή του κάθε τύπου επίθεσης ανάλογα με το μοντέλο διάθεσης στο οποίο εμπίπτει.

Στο **6ο Κεφάλαιο** παρουσιάζονται οι μηχανισμοί εκείνοι που θα πρέπει να λάβει υπόψιν ένας επαγγελματίας της ασφάλειας των πληροφοριών για κάθε ζήτημα ασφαλείας που μπορεί να προκύψει.

Τέλος, στο **7ο Κεφάλαιο** παρουσιάζονται τα συμπεράσματα που εξήχθησαν μετά την ολοκλήρωση της εκπόνησης της παρούσας διπλωματικής εργασίας.



**Λέξεις κλειδιά:** υπολογιστικό νέφος, ασφάλεια και ιδιωτικότητα στο σύννεφο, απειλές στο σύννεφο, ζητήματα ασφάλειας, CIA τριάδα, εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, λογοδοσία, απόρρητο

Abstract

In the **1st Chapter** of this thesis, the concept of cloud computing is presented and both its deployment models and the different offered models of the services are described. Also, there is an analysis about the governance and the setup of the degree of the organization's control versus the provider's control in relation to the chosen deployment model. Finally, the concepts of machine virtualization are mentioned, which constitute a basic building block of creating and managing computing resources in the cloud.

There are many sceptics of cloud computing adoption. **In Chapter 2**a comprehensive citation of the advantages and disadvantages of its use are quoted.

**In Chapter 3**, the concepts that make up security and privacy are thoroughly analysed, starting with the CIA triad. As mentioned, all these parameters are not an exclusive privilege of the cloud computingarea; they started from the conventional / traditional computing systems and they can be applied to all the machines that store, process and manage data or handle with bits of information.

In the **4th Chapter** a classification of threats and risks under many and different prisms and perspectives is attempted. Firstly, a general categorization is being given, then a classification according to whether the threats are related to the human or technology factor is cited, and then an endeavor to correlate the risks by cloud area is made. Also, the three general cloud attack layers are listed and the attack surfaces per deployment model are mentioned.

In the **5th Chapter**, a detailed description of each type of the attacks according to the deployment model in which they fall are given.

**Chapter 6** presents the mechanisms that an information security professional should consider for any security issue that may arise in cloud area.

Finally, the **7th Chapter** presents the conclusions drawn after completing the preparation of this thesis.

**Key Words:** cloud computing, cloud security and privacy, cloud threats, security issues, CIA triad, confidentiality, integrity, availability, accountability, privacy

# ΕΙΣΑΓΩΓΗ

Ένα ευρύ φάσμα νέων τεχνολογιών, συμπεριλαμβανομένων της τεχνητής νοημοσύνης, των έξυπνων μηχανών (τηλέφωνα, αυτοκίνητα, οικιακές συσκευές), σε συνδυασμό με τις τεχνολογίες υπολογιστικού νέφους και τις νέες δυνατότητες δικτύωσης των δικτύων 5ης γενιάς, έχουν εφαρμογές στους τομείς της υγείας, των μεταφορών, των κατασκευών και των αγροδιατροφικών προϊόντων, καθώς και σε άλλους τομείς όπως η εθνική άμυνα. Το έδαφος για κακόβουλες και παράνομες συμπεριφορές μεγαλώνει καθώς ο ψηφιακός κόσμος διεισδύει σε όλο και περισσότερες πτυχές της καθημερινής οικονομικής και κοινωνικής ζωής.

Όλες οι παραπάνω ταχύτατες εξελίξεις, σε συνδυασμό με την αυξανόμενη ζήτηση για ψηφιακές εφαρμογές και υπηρεσίες, ενέχουν σημαντικές προκλήσεις. Οι κίνδυνοι για την εκμετάλλευση ή την παραβίαση των προσωπικών δεδομένων αυξάνονται καθώς οι νέες υπηρεσίες επιτρέπουν στον σύγχρονο άνθρωπο μεγαλύτερη προσαρμογή και εστίαση στις προσωπικές του ανάγκες και απαιτήσεις (ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, 2020).

Τα τελευταία χρόνια, οι φράσεις «ψηφιακός μετασχηματισμός» και «μετανάστευση στο σύννεφο» έχουν γίνει συνηθισμένες σε πολλά και διάφορα επιχειρηματικά πλαίσια. Και οι δύο εκφράσεις παρακινούνται από την επιθυμία για αλλαγή, ακόμα κι αν η σημασία τους μπορεί να διαφέρει ανάλογα με τον οργανισμό. Όταν οι επιχειρήσεις υιοθετούν αυτές τις πρακτικές και εργάζονται για τη βελτίωση της επιχειρησιακής τους στρατηγικής, νέες δυσκολίες ανακύπτουν στην εξισορρόπηση των επιπέδων παραγωγικότητας και των επιπέδων ασφάλειας.

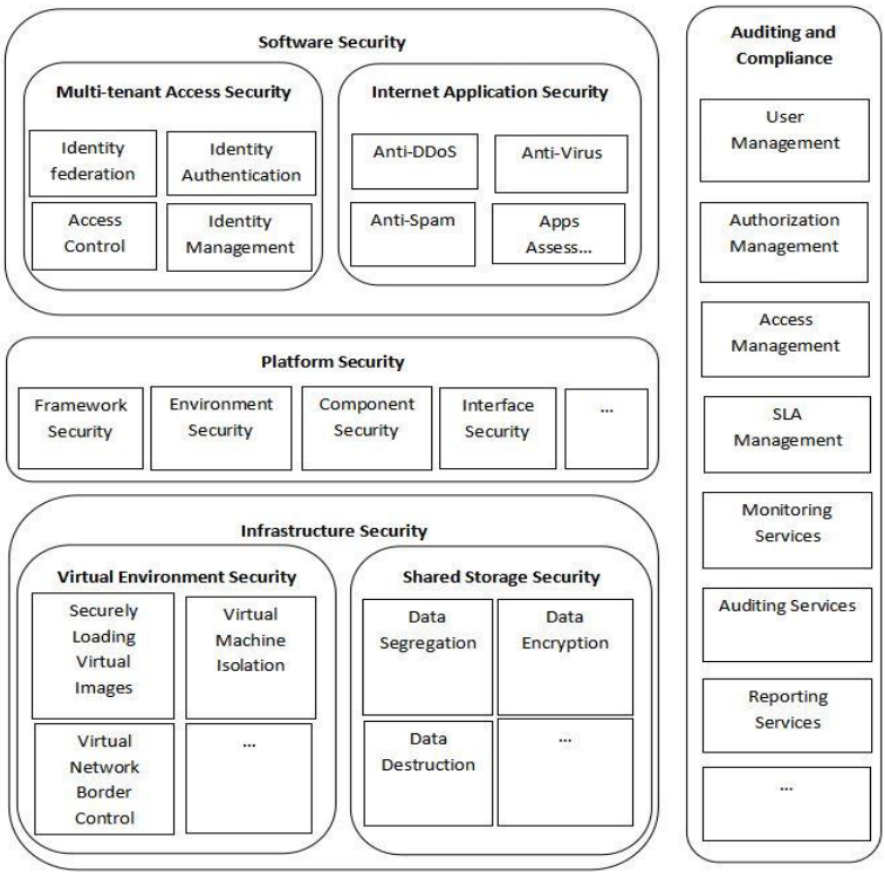
Ενώ η μετακίνηση στο σύννεφο, εάν γίνει με σωστό σχεδιασμό, μπορεί να έχει θετικές προεκτάσεις, από την άλλη αν η μετάβαση δεν γίνει βάσει σχεδίου όπου θα λαμβάνονται υπόψιν, πρωτίστως, όλες οι παράμετροι που επιτάσσει η ασφάλεια των πληροφοριακών συστημάτων, η ενέργεια αυτή ενέχει κινδύνους. Η κατανόηση του τρόπου με τον οποίο οι σύγχρονες επιχειρήσεις μπορούν να επωφεληθούν από τη χρήση της τεχνολογίας του υπολογιστικού νέφους εφαρμόζοντας τις καλύτερες πολιτικές ασφάλειας είναι απαραίτητη για την επίτευξη των θετικών αποτελεσμάτων της εν λόγω τεχνολογίας.

Η ασφάλεια στο υπολογιστικό νέφος αποτελείται από ένα σύνολο πρακτικών και εργαλείων που δημιουργήθηκαν για τη διαχείριση τόσο των εσωτερικών όσο και των εξωτερικών κινδύνων από τις επιχειρήσεις. Καθώς οι οργανισμοί εφαρμόζουν το σχέδιο ψηφιακού μετασχηματισμού και ενσωματώνουν εργαλεία και υπηρεσίες στην υποδομή τους που βασίζονται στο σύννεφο, απαιτείται η υιοθέτηση αυτών των προτύπων ασφαλείας (IBM, 2023).

Για την προστασία της εικονικής διεύθυνσης *IP*(*Internet Protocol*), των δεδομένων, των εφαρμογών, των υπηρεσιών και της σχετικής υποδομής του υπολογιστικού νέφους,

χρησιμοποιείται ένα ευρύ φάσμα κανόνων, τεχνολογιών, εφαρμογών και ελέγχων, που μαζί αναφέρονται ως ασφάλεια *cloud* ή ασφάλεια υπολογιστικού νέφους. Πρόκειται για έναν υποτομέα της ασφάλειας των υπολογιστικών συστημάτων που εμπίπτει στην ομπρέλα της ασφάλειας των πληροφοριών, των δικτύων και των υπολογιστών (Hassaan, 2022).

Στο παρακάτω σχήμα απεικονίζεται η αρχιτεκτονική ασφάλειας του υπολογιστικού νέφους. Η ορολογία αυτή αναφέρεται σε όλο το υλικό και το λογισμικό που χρησιμοποιούν οι πλατφόρμες νέφους για την προστασία των δεδομένων, του φόρτου εργασίας και των συστημάτων τους. Ένα σχέδιο για την αρχιτεκτονική ασφάλειας του υπολογιστικού νέφους θα πρέπει να καταρτιστεί και να ενσωματωθεί από την αρχή μιας λύσης που φιλοξενείται στο*cloud*. Πολύ συχνά, λανθασμένα, οι αρχιτέκτονες του υπολογιστικού νέφους δίνουν προτεραιότητα στην απόδοση των συστημάτων, ενώ προσπαθούν να προσθέσουν τα διάφορα επίπεδα ασφάλειας αργότερα. Από την παρακάτω εικόνα είναι σαφές ότι κάθε επίπεδο παρέχει μέτρα ασφαλείας με διαφορετικό τρόπο (Hassaan, 2022).

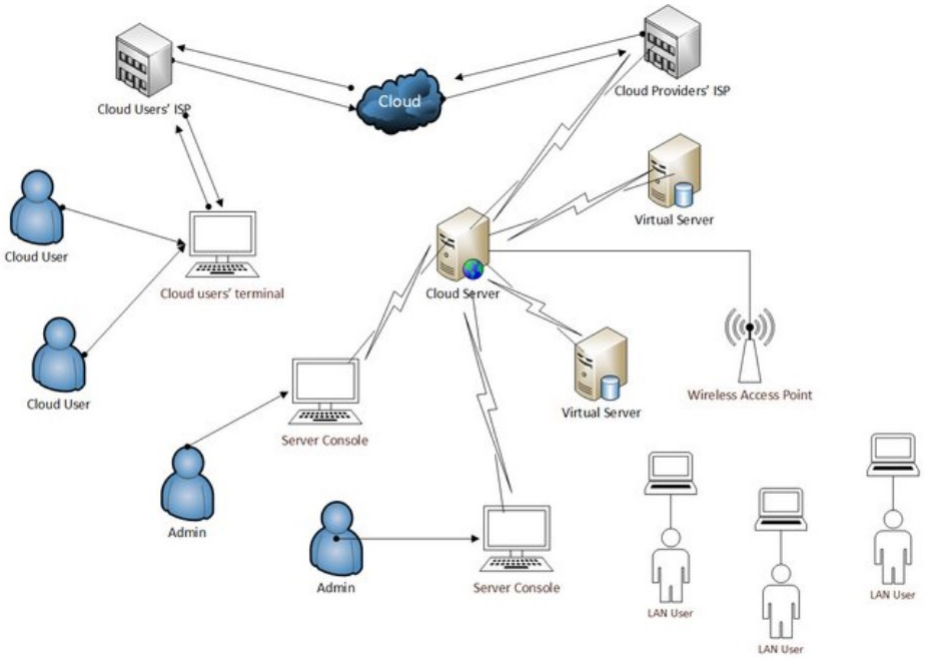



***Εικόνα 1**: Αρχιτεκτονική ασφάλειας στο υπολογιστικό νέφος*
**Πηγή**: Hassaan, M., 2022

# 1. ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

## 1.1 Ορισμός

Το υπολογιστικό νέφος (*CC: Cloud Computing*)ορίζεται ως μια κοινόχρηστη δεξαμενή αναδιαμορφώσιμων υπολογιστικών πόρων, όπως δίκτυα, διακομιστές, αποθηκευτικός χώρος, εφαρμογές και υπηρεσίες, που μπορεί να αναπτυχθεί γρήγορα και να παρασχεθεί σε όσους το επιθυμούν, με λίγη διοικητική εργασία ή εμπλοκή του παρόχου των υπηρεσιών. Τρία μοντέλα υπηρεσιών, τέσσερις μέθοδοι ανάπτυξης και πέντε βασικά κριτήρια συνθέτουν το υπολογιστικό νέφος (Mell&Grance, 2011). Στην παρακάτω τοπολογία απεικονίζεται ένα τυπικό διάγραμμα της αρχιτεκτονικής του:




***Εικόνα 2**: Τυπικό διάγραμμα τοπολογίας της αρχιτεκτονικής του υπολογιστικού νέφους*
**Πηγή**: Ahmed&Hossain, 2014

## 1.2 Χαρακτηριστικά

Ο ορισμός του *NIST* (*National Institute of Standards and Technology*) απαριθμεί πέντε βασικά χαρακτηριστικά του *cloud computing* (Alleweldt., 2012; Mell&Grance, 2011):

- **Διαθεσιμότητα κατ' απαίτηση (*On-demand self-service*):** Ένας πελάτης μπορεί να αποκτήσει αυτόματα υπολογιστικούς πόρους, όπως υπολογιστική ισχύ, αποθηκευτικό χώρο, μνήμη, εύρος ζώνης δικτύου, όποτε τους χρειαστεί και αυτόματα χωρίς, δηλαδή να απαιτείται καμία απευθείας επικοινωνία με τον πάροχο των υπηρεσιών. Το τελευταίο αυτό χαρακτηριστικό γνώρισμα του *cloud* ονομάζεται αυτοπρομήθεια πόρων (*Self-provisioning of resources*).

- **Ευρεία πρόσβαση στο δίκτυο (*Broad Network Access*):**Οι χρήστες μπορούν να έχουν πρόσβαση στη λειτουργικότητα που προσφέρεται μέσω του διαδικτύου χρησιμοποιώντας τυποποιημένες μεθόδους που θα πρέπει να λειτουργούν σε διάφορες συσκευές, όπως κινητά τηλέφωνα, ταμπλέτες, φορητούς υπολογιστές αλλά και σταθερούς σταθμούς εργασίας.
- **Συγκέντρωση πόρων (*Resource Pooling*):**Χρησιμοποιώντας ένα μοντέλο πολλαπλών μισθώσεων, οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται για την εξυπηρέτηση πολλών πελατών, με διακριτούς φυσικούς και εικονικούς πόρους να διανέμονται δυναμικά ανάλογα με τη ζήτηση των πελατών. Καθώς ο καταναλωτής δεν έχει κανέναν έλεγχο ή γνώση της ακριβούς τοποθεσίας των προσφερόμενων πόρων, υπάρχει συνήθως μια αίσθηση γεωγραφικής ανεξαρτησίας. Ωστόσο, μπορεί κάποιος, σε ορισμένες περιπτώσεις, να επιλέξει την περιοχή στην οποία θα αποθηκεύονται οι πόροι στους οποίους έχει πρόσβαση, σε υψηλότερο πάντοτε επίπεδο αφαίρεσης, όπως η επιλογή της χώρας, της πολιτείας ή ενός κέντρου δεδομένων.
- **Ταχεία ελαστικότητα (*Rapid Elasticity*):**Οι δυνατότητες μπορούν να παρέχονται και να απελευθερώνονται ελαστικά και σε ορισμένες περιπτώσεις αυτόματα, επιτρέποντας την γρήγορη προς τα πάνω ή προς τα κάτω κλιμάκωση ανάλογα πάντοτε με τη ζήτηση. Για τον τελικό χρήστη, οι λειτουργίες που προσφέρονται μοιάζουν να είναι πάντοτε διαθέσιμες και ανεξάντλητες.
- **Μετρήσιμη εξυπηρέτηση (*Measured Services*):**Τα συστήματα υπολογιστικού νέφους χρησιμοποιούν μετρήσεις, κατάλληλες για κάθε τύπο υπηρεσίας, προκειμένου να πετυχαίνουν αυτόματες ρυθμίσεις, αλλά και βελτιστοποίηση της χρήσης των διαθέσιμων πόρων, όπως είναι για παράδειγμα η αποθήκευση, η επεξεργασία, το εύρος ζώνης οι ενεργοί λογαριασμοί χρηστών κ.λπ.. Η παρακολούθηση, η ρύθμιση και η αναφορά της χρήσης πόρων επιτρέπει τη διαφάνεια, παρέχοντας μια αναλυτική εικόνα της κατανάλωσης και της διαθεσιμότητας των πόρων τόσο για τον πάροχο των υπηρεσιών όσο και για τους τελικούς χρήστες.

Στην βιβλιογραφία αναφέρονται πληθώρα άλλων γνωρισμάτων που χαρακτηρίζουν το υπολογιστικό νέφος. Μερικά από αυτά είναι τα εξής (Mather et al., 2009):

- **Πολυμίσθωση πολυμετοχικότητα (Multitenancy):** Όπως έγινε σαφές μέχρι τώρα, το *cloud computing* βασίζεται σε ένα επιχειρηματικό μοντέλο όπου οι πόροι διαμοιράζονται, πολλοί χρήστες, δηλαδή, χρησιμοποιούν τους ίδιους πόρους (κοινόχρηστοι πόροι) σε επίπεδο δικτύου, σε επίπεδο κεντρικού υπολογιστή (φυσικά

μηχανήματα) και σε επίπεδο εφαρμογών. Αυτό έρχεται σε αντίθεση με προηγούμενα υπολογιστικά μοντέλα όπου απαιτούνταν αποκλειστικοί πόροι, υπολογιστικές, δηλαδή, εγκαταστάσεις αφιερωμένες σε έναν μόνο χρήστη ή ιδιοκτήτη.

- **Επεκτασιμότητα (Massive scalability):** Παρά το γεγονός ότι οι επιχειρήσεις μπορεί να διαθέτουν εκατοντάδες ή χιλιάδες συστήματα και εφαρμογές, το νέφος τις επιτρέπει να αναπτυχθούν σε δεκάδες χιλιάδες συστήματα καθώς και να αυξήσουν δραματικά το εύρος ζώνης και τον αποθηκευτικό χώρο των δεδομένων τους.
- **Πληρωμή ανάλογα με τη χρήση (Pay-as-you-go):** Μόνο οι πόροι που χρησιμοποιούνται πραγματικά από τον χρήστη καθώς και ο χρόνος που απαιτείται για να εκτελεστούν οι εργασίες που απαιτούνται καλύπτονται από τα τέλη σύνδεσης στα διάφορα μοντέλα πληρωμών.

## 1.3 Τύποι υπολογιστικού νέφους

Σε σχέση με τους τύπους των υπολογιστικών νεφών εξετάζονται συνήθως δύο διακριτά σύνολα μοντέλων:

- **Μοντέλα διάθεσης(*Deployment Models*):** Τα μοντέλα αυτά αναφέρονται στη θέση και στη διαχείριση της υποδομής του νέφους.
- **Μοντέλα υπηρεσιών (*Service Delivery Models):*** Τα μοντέλα αυτά αναφέρονται στους ιδιαίτερους τύπους υπηρεσιών που μπορεί κάποιος να έχει πρόσβαση σε μια πλατφόρμα υπολογιστικού νέφους.

### *1.3.1 Μοντέλα διάθεσης*

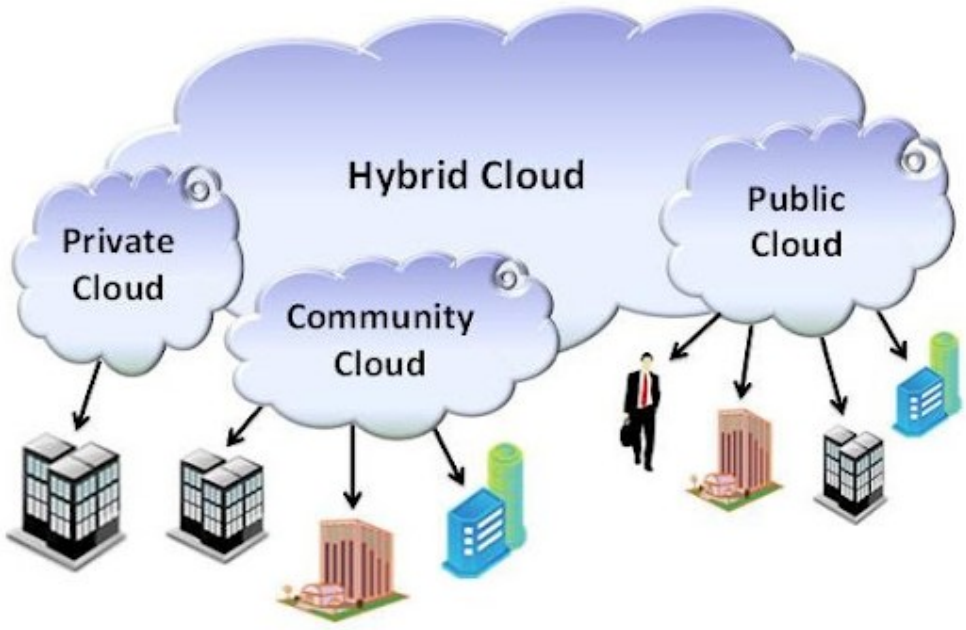
Υπάρχουν τέσσερις τύποι παροχής των πόρων του ΥΝ (Υπολογιστικού Νέφους) (Alleweldt., 2012; El-Sofany&El-Seoud, 2019; Hwangetal., 2010;Issa, 2021;Mather et al., 2009; Mell&Grance, 2011;Pandaetal, 2021;Sen, 2015):

- **Ιδιωτικό σύννεφο (*Private Cloud*):**Αυτή η υποδομή παρέχεται για την αποκλειστική χρήση και διάθεση των πόρων από έναν μόνο οργανισμό και περιλαμβάνει πολλούς καταναλωτές· για παράδειγμα, τις επιχειρηματικές μονάδες και τους μεμονωμένους χρήστες / υπαλλήλους εντός του οργανισμού. Η υποδομή του ιδιωτικού υπολογιστικού νέφους μπορεί να ανήκει στον οργανισμό και να τη διαχειρίζεται ο ίδιος, ή να ανήκει σε κάποιον τρίτο που είναι υπεύθυνος και για τη διαχείρισή του, ή τέλος το μοντέλο να περιλαμβάνει κάποιους συνδυασμούς των παραπάνω. Σε κάθε περίπτωση, το ιδιωτικό σύννεφο μπορεί να υπάρχει εντός ή εκτός των εγκαταστάσεων του οργανισμού.
- **Κοινοτικό σύννεφο (*Community Cloud*):**Η υποδομή αυτού του τύπου παρέχεται για την αποκλειστική χρήση μιας συγκεκριμένης κοινότητας καταναλωτών, συνήθως από

οργανισμούς που μοιράζονται κοινές ανησυχίες, όπως για παράδειγμα θέματα ασφάλειας, πολιτικής και συμμόρφωσης. Αυτή η υποδομή μπορεί να ανήκει, να διαχειρίζεται και να λειτουργεί από έναν ή περισσότερους κοινοτικούς οργανισμούς, από κάποιο τρίτο μέρος ή από κάποιο συνδυασμό των παραπάνω και μπορεί να υπάρχει εντός ή εκτός των εγκαταστάσεων ενός από τους οργανισμούς της κοινότητας.

- **Δημόσιο σύννεφο (*Public Cloud*):**Αυτή η υποδομή υπολογιστικού νέφους παρέχεται για ανοιχτή χρήση από το ευρύ κοινό. Μπορεί να ανήκει και να λειτουργεί από μια επιχείρηση, έναν ακαδημαϊκό ή κυβερνητικό οργανισμό ή από κάποιον συνδυασμό των προαναφερθέντων οντοτήτων. Υπάρχει στις εγκαταστάσεις του παρόχου του υπολογιστικού νέφους.
- **Υβριδικό σύννεφο (*Hybrid Cloud*)**. Η υβριδική υποδομή cloud είναι μια σύνθεση δύο ή περισσότερων διακριτών υποδομών υπολογιστικού νέφους (ιδιωτική, κοινοτική ή δημόσια), οι οποίες ενώ παραμένουν μοναδικές οντότητες, συνδέονται μεταξύ τους με τυποποιημένη ή αποκλειστική τεχνολογία που επιτρέπει τη φορητότητα των δεδομένων και των εφαρμογών.

Στην παρακάτω εικόνα απεικονίζονται τα τέσσερα διαφορετικά μοντέλα διάθεσης και οι διαφορετικοί χρήστες του κάθε μοντέλου:




***Εικόνα 3**: Τα 4 μοντέλα διάθεσης του υπολογιστικού νέφους*
**Πηγή**:WebBazarIndia, 2021

Στην βιβλιογραφία αναφέρεται πολλές φορές και ένα τέταρτο μοντέλο διάθεσης πόρων υπολογιστικού νέφους:

- **Πολυ-σύννεφο ή μοντέλο πολλαπλών σύννεφων (*Multi-Cloud*):** Ένα ακόμη όλο και πιο πιθανό σενάριο επιλογής ενός μοντέλου διάθεσης είναι ένα σενάριο πολλαπλών σύννεφων. Σε ένα τέτοιο μοντέλο, γίνεται χρήση πολλών διαφορετικών παρόχων δημόσιου νέφους. Το πολυ-σύννεφο είναι τόσο ευέλικτο όσο και η ίδια η ανάπτυξη του *cloud* (Microsoft, 2023). Αυτό το μοντέλο δίνει την ευελιξία σε μια επιχείρηση ή σε έναν οργανισμό να χρησιμοποιεί τις διαφορετικές δυνατότητες που παρέχεται από καθέναν από τους διαφορετικούς παρόχους. Πέραν όμως του προφανούς αυτού κριτηρίου, ορισμένες επιχειρήσεις ενδέχεται να χρησιμοποιήσουν μια στρατηγική πολλαπλών *cloud* για να επωφεληθούν από τις διαφορετικές υπηρεσίες με βάση τις ανησυχίες τους για την ασφάλεια, καθώς και τις διαφορετικές τιμολογιακές πολιτικές. Υπάρχουν επίσης και άλλοι λόγοι όπως για παράδειγμα η αποφυγή ορίων τιμών ή η ανάγκη μέτρησης των αναγκών των υπηρεσιών νέφους σε πολλούς παρόχους ταυτόχρονα (Theastrologypage, 2023).

### *1.3.2 Μοντέλα υπηρεσιών*

Κατά κανόνα, το υπολογιστικό νέφος παρέχεται ως υπηρεσία σε διάφορα επιχειρηματικά μοντέλα (ή και με κάποιους συνδυασμούς αυτών), τα οποία κλιμακώνονται από τη μερική έως την πλήρη χρήση του και απευθύνονται σε διαφορετικούς τύπους πελατών (Mell&Grance, 2011).

Ανάλογα με τις υπηρεσίες που προσφέρονται, τα τρία επιχειρηματικά μοντέλα που διατίθενται είναι τα εξής(Alleweldt, 2012; Hwang et al., 2010; Issa, 2021; Khanetal., 2022; Mather et al., 2009; Mell&Grance, 2011; Sosinsky, 2011;Pandaetal, 2021; Sen, 2015):

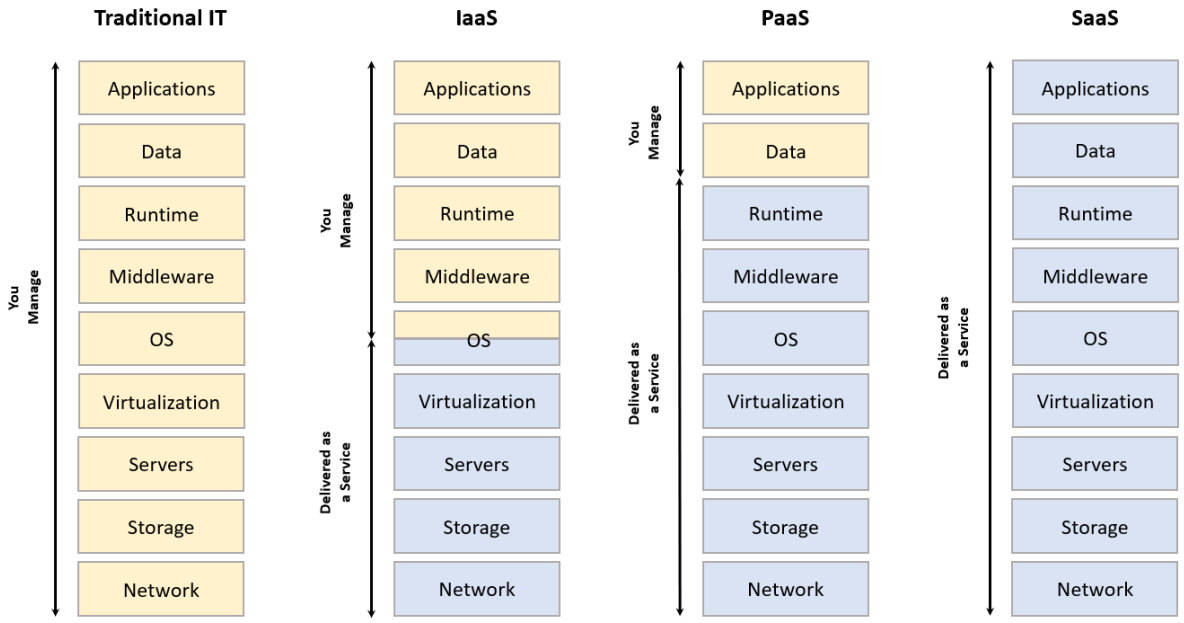
- **Το λογισμικό ως υπηρεσία (*SaaS: Software as a Service):***Σε αυτό το επιχειρηματικό μοντέλο η δυνατότητα που παρέχεται στον τελικό χρήστη είναι η χρήση των εφαρμογών του παρόχου που φιλοξενούνται σε μια υποδομή cloud. Οι εφαρμογές αυτές είναι προσβάσιμες από διάφορες συσκευές του πελάτη είτε μέσω μιας λεπτής διεπαφής Ιστού, όπως ένα πρόγραμμα περιήγησης Ιστού (*web browser*), είτε μέσω μιας διεπαφής προγράμματος (*program interface*). Ο καταναλωτής δεν μπορεί να διαχειριστεί ούτε να ελέγξει την υποκείμενη υποδομή του υπολογιστικού νέφους, συμπεριλαμβανομένων των δικτύων, των διακομιστών, των λειτουργικών συστημάτων, της αποθήκευσης ή ακόμη και των δυνατοτήτων μεμονωμένων εφαρμογών, με πιθανή εξαίρεση τη διαμόρφωση περιορισμένων ρυθμίσεων των εφαρμογών για συγκεκριμένους χρήστες (*application configuration settings*).

- **Ηπλατφόρμα ως υπηρεσία (*PaaS: Platform as a Service*):**Σε αυτό το μοντέλο παροχής υπηρεσιών ο τελικός χρήστης μπορεί να διαθέσει μέσω της υποδομής του υπολογιστικού νέφους εφαρμογές που δημιουργεί ο ίδιος χρησιμοποιώντας γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες και εργαλεία που υποστηρίζονται από τον πάροχο. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει την υποκείμενη υποδομή, συμπεριλαμβανομένων του δικτύου, των διακομιστών, των λειτουργικών συστημάτων ή του χώρου αποθήκευσης, αλλά έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί καθώς και τις ρυθμίσεις διαμόρφωσης για το περιβάλλον φιλοξενίας τους.
- **Η υποδομή ως υπηρεσία (*IaaS:Infrastructure as a Service*):**Οι λειτουργίες που παρέχονται στον τελικό χρήστη είναι η επεξεργασία, η αποθήκευση, η παροχή δικτύων και άλλων βασικών υπολογιστικών πόρων για την ανάπτυξη και την εκτέλεση του λογισμικού, συμπεριλαμβανομένων των λειτουργικών συστημάτων και των εφαρμογών. Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποκείμενη υποδομή του υπολογιστικού νέφους, αλλά έχει τον έλεγχο του λειτουργικού συστήματος, των εφαρμογών του και των επιλογών της αποθήκευσης και σε ορισμένες περιπτώσεις περιορισμένο έλεγχο κάποιων στοιχείων του δικτύου, όπως των τειχών προστασίας.

  Οι πάροχοι *IaaS*, οι οποίοι διαχειρίζονται μόνο την υποδομή του νέφους, χρεώνουν τους χρήστες για ένα σταθερό χρονικό διάστημα με βάση τη χωρητικότητα και τη δυνατότητα της υποδομής που ζητείται. Στην περίπτωση του περιβάλλοντος *IaaS* της *Amazon*, οι χρήστες μπορούν να δημιουργούν, να εκτελούν και να τερματίζουν διακομιστές ανάλογα με τις ανάγκες τους, πληρώνοντας με την ώρα για όσους από αυτούς παραμένουν ενεργοί.

## 1.4Διακυβέρνηση στο υπολογιστικό νέφος

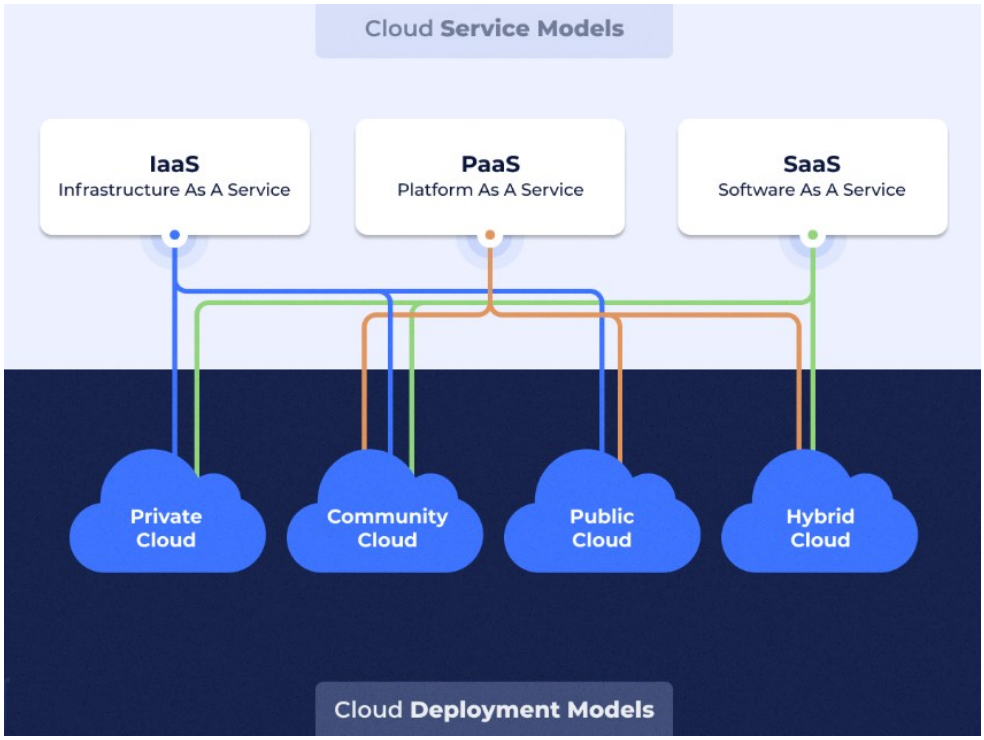
Η επίδραση του *cloud computing* στη δομή διακυβέρνησης των εταιρειών πληροφορικής φαίνεται στο παρακάτω σχήμα:




***Εικόνα 4**: Διαθέσιμα μοντέλα υπηρεσιών υπολογιστικού νέφους συγκρινόμενα με την παραδοσιακή παροχή IT υπηρεσιών*

Τα διάφορα τεχνολογικά επίπεδα που απεικονίζονται στο διάγραμμα διέπονται παραδοσιακά από την πλειοψηφία των εταιρειών πληροφορικής. Το παράδειγμα επιτόπιας εγκατάστασης δείχνει ότι όλα τα τεχνολογικά επίπεδα υπόκεινται στον πλήρη έλεγχο και την εποπτεία της πληροφορικής της εκάστοτε εταιρίας. Ο βαθμός ελέγχου που κατέχει ο οργανισμός πληροφορικής μειώνεται καθώς προχωράμε από το *IaaS* στο *PaaS*και έπειτα στο *SaaS*, ενώ το επίπεδο ελέγχου που κατέχει ο πάροχος υπολογιστικού νέφους αυξάνεται. Αν και ο πάροχος έχει μεγαλύτερη ισχύ, το τμήμα *IT* εξακολουθεί να έχει την ευθύνη. Για να βεβαιωθεί ένας οργανισμός ότι πληρούνται τα πρότυπα υπηρεσιών και οι συμβατικές ευθύνες που απορρέουν από αυτή την επιλογή, είναι ζωτικής σημασίας για τις εταιρείες πληροφορικής να δημιουργήσουν ισχυρούς μηχανισμούς παρακολούθησης ανάλογα με το μοντέλο της υπηρεσίας που θα επιλέξουν (*SPI: Software, Platform, Infrastructure*) (Mather et al., 2009).

Στην παρακάτω εικόνα απεικονίζεται η δυνατότητα επιλογής μοντέλου διάθεσης σε σχέση με τα μοντέλα των υπηρεσιών και το αντίστροφο:




***Εικόνα 5**:Διαθέσιμα μοντέλα υπηρεσιών ανάλογα με το μοντέλο διάθεσης και το αντίστροφο*
**Πηγή**: Koshkin, 2022

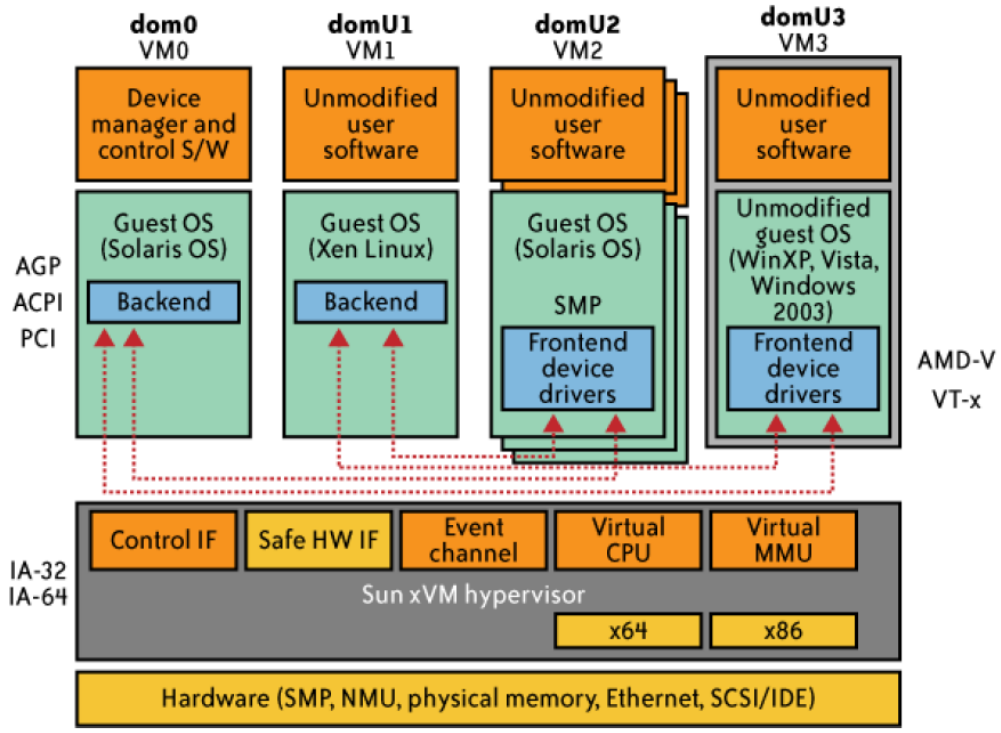
## 1.5 Αφαίρεση και εικονοποίηση

Η εικονικοποίηση είναι μια βασική τεχνολογία που υποστηρίζει το *cloud computing* και αλλάζει την εμφάνιση του σύγχρονου κέντρου δεδομένων. Η λέξη «*virtualization*» περιγράφει τον διαχωρισμό των υπολογιστικών πόρων, συμπεριλαμβανομένης της *CPU*, της αποθήκευσης, του δικτύου, της μνήμης, της στοίβας εφαρμογών και της βάσης δεδομένων, από τις εφαρμογές και τους τελικούς χρήστες που χρησιμοποιούν την υπηρεσία. Η αφαίρεση της υποδομής γεννά την ιδέα του εκδημοκρατισμού των πόρων, είτε πρόκειται για υποδομή, είτε για εφαρμογές είτε για πληροφορίες, και δημιουργεί τη δυνατότητα να καταστούν οι συγκεντρωμένοι πόροι διαθέσιμοι και προσβάσιμοι σε οποιονδήποτε ή οτιδήποτε επιτρέπεται να τους χρησιμοποιήσει μέσω τυποποιημένων μεθόδων.

Οι τεχνολογίες εικονικοποίησης καθιστούν δυνατές τις πολλαπλές μισθώσεις, παρέχοντας σε κάθε ενοικιαστή πρόσβαση σε μια επεκτάσιμη, κοινόχρηστη πλατφόρμα πόρων. Το πιο σημαντικό είναι ότι δίνουν στους χρήστες της πλατφόρμας μια εξειδικευμένη προβολή των πόρων. Από επιχειρηματική άποψη, η ενοποίηση του κέντρου δεδομένων και η αυξημένη λειτουργική αποτελεσματικότητα των υπηρεσιών της πληροφορικής είναι δύο βασικά πλεονεκτήματα της εικονικοποίησης. Οι επιχειρήσεις χρησιμοποιούν πλέον μια ποικιλία τεχνολογιών εικονικοποίησης στα κέντρα δεδομένων τους, όπως εικονικοποίηση λειτουργικού συστήματος (*VMware, Xen*), εικονικοποίηση αποθήκευσης (*NAS:Network-*

*Attached Storage, SAN: SAN: Storage Area Network*), εικονικοποίηση βάσεων δεδομένων και εικονικοποίηση εφαρμογών ή λογισμικού (*ApacheTomcat, JBoss, Oracle App Server, WebSphere*).Από την άποψη του δημόσιου νέφους, ανάλογα και με το μοντέλο υπηρεσιών και την αρχιτεκτονική, η εικονικοποίηση εμφανίζεται ως κοινόχρηστος πόρος σε διαφορετικά επίπεδα της εικονικοποιημένης υπηρεσίας, όπως για παράδειγμα στο λειτουργικό σύστημα, στην αποθήκευση, στη βάση δεδομένων, στις εφαρμογές κ.λπ.

Ο ορισμός της *Sun Microsystems* για τα επίπεδα του περιβάλλοντος εικονικοποίησης ανάλογα με το επιλεγμένο λειτουργικό σύστημα φαίνεται στο παρακάτω σχήμα:




***Εικόνα 6**: Περιβάλλον hypervisorSunxVM*
**Πηγή**: Matheretal, 2019

Αυτού του είδος η εικονικοποίηση χρησιμοποιείται από παρόχους *IaaS* όπως το *Amazon* (*EC2*), το *ServePath* (*GoGrid*) και το *Sun Cloud*, επιτρέποντας στους χρήστες να λειτουργούν στιγμιότυπα διαφορετικών εκδόσεων του λειτουργικού συστήματος σε ένα δημόσιο σύννεφο. Το περιβάλλον υπερεπόπτη *SunxVM* (το οποίο είναι η πλατφόρμα εικονικοποίησης) εικονικοποιεί κοινόχρηστους πόρους υλικού για εικονικούς διακομιστές που

τρέχουν λειτουργικά τόσο σε *Linux*, όσο και σε *Solaris* αλλά και σε *Microsoft Windows* τα οποία φιλοξενούνται στον υπερπιστωτή (*hypervisor*[1]).

Ο υπερπιστωτής (*hypervisor*) είναι ένα μικρό πρόγραμμα που λειτουργεί πάνω από το επίπεδο υλικού ενός φυσικού συστήματος. Εφαρμόζει και ελέγχει την κοινή μνήμη, τα κανάλια συμβάντων, την εικονική κεντρική μονάδα επεξεργασίας (*vCPU: virtual CPU -Central Processing Unit*) και την εικονική μνήμη (*vMemory: virtual Memory*) των εγκατεστημένων εικονικών μηχανών(*VMs: Virtual Machines*). Διαχειρίζεται επίσης τον τρόπο με τον οποίο οι συσκευές έχουν πρόσβαση στη μνήμη και στις διάφορες εισόδους/εξόδους τους. Μία εικονική μηχανή αναφέρεται ως τομέας στους *Xen* και *SunxVM* υπερόπτες, αλλά ως επισκέπτης λειτουργικού συστήματος στο λογισμικό εικονικοποίησης της *VMware*. Οι εικονικές μηχανές στο παραπάνω σχήμα προσδιορίζονται ως dom0, domU1, domU2 και domU3.

Οι πάροχοι υπηρεσιών *SaaS* και *PaaS* είναι γνωστό ότι έχουν εισαγάγει εικονικοποίηση λογισμικού και βάσεων δεδομένων, η οποία επιτρέπει στους πελάτες να διαμοιράζονται τόσο τη στοίβα των εφαρμογών λογισμικού όσο και τους πόρους της βάσης δεδομένων, εκτός από την εικονικοποίηση του λειτουργικού συστήματος και της αποθήκευσης. Με αυτήν την αρχιτεκτονική, κάθε επίπεδο της υποδομής που παραδίδεται μπορεί να διαμοιραστεί σε κάθε πελάτη.

Το *cloud computing* είναι ένα επαναστατικό υπολογιστικό παράδειγμα που επιτρέπει την ευέλικτη, κατ' απαίτηση και οικονομικά προσιτή χρήση διαμοιρασμένων υπολογιστικών πόρων. Κατά ειρωνικό τρόπο, αυτά τα οφέλη είναι που οδηγούν σε ζητήματα ασφάλειας και απορρήτου, επειδή τα δεδομένα διαφορετικών χρηστών διατηρούνται σε κοινά φυσικά μηχανήματα στους *cloud* διακομιστές αντί να βρίσκονται υπό τον δικό τους έλεγχο (Mather et al., 2009).

## 2. ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Οι διάφοροι οργανισμοί θα πρέπει να εξετάσουν το *cloud computing* ως εναλλακτική στην παραδοσιακή χρήση της τεχνολογίας των πληροφοριών για διάφορους λόγους. Μια τέτοια επιλογή, αλλάζει, σαφώς, τη λειτουργία του *IT* τμήματος ενός οργανισμού και ορισμένα από τα παλιά μοντέλα οργάνωσης και παροχής υπηρεσιών θα χρειαστεί να τροποποιηθούν ώστε να ληφθεί υπόψη η ικανότητα επεξεργασίας που μπορεί να παρασχεθεί γρήγορα και άμεσα μέσω του υπολογιστικού νέφους (Mather et al., 2009).

[1]Ένας *hypervisor* (επίσης γνωστός ως οθόνη *εικονικής* μηχανής, *VMM* ή *virtualizer*) είναι ένας τύπος λογισμικού (*software*), υλικολογισμικού (*firmware*) ή υλικού (hardware) που δημιουργεί και εκτελεί εικονικές μηχανές (Πηγή: https://en.wikipedia.org/wiki/Hypervisor).

Όπως κάθε τεχνολογία έτσι και το υπολογιστικό νέφος κρύβει κινδύνους και βρίθει μειονεκτημάτων. Εναπόκειται στο βαθμό ωρίμανσης του κάθε οργανισμού και στη σωστή αξιολόγηση των πλεονεκτημάτων και των μειονεκτημάτων που απορρέουν από τη χρήση του ώστε να αξιολογηθεί το αν και το πότε θα πρέπει να επιχειρηθεί μια τέτοια μετάβαση.

## 2.1 Πλεονεκτήματα

Τα πλεονεκτήματα του *cloud computing* περιλαμβάνουν: οικονομική αποδοτικότητα, άμεση ανταπόκριση, ευελιξία, αντιστοίχιση του κόστους πληροφορικής με τον όγκο των συναλλαγών, άμεσο έλεγχο των τεχνολογικών επιλογών από τους χρήστες των επιχειρήσεων (Mather et al., 2009), γρήγορη εγκατάσταση, άφθονο χώρο αποθήκευσης και τέλος απρόσκοπτη πρόσβαση στο σύστημα από οποιαδήποτε τοποθεσία και ανά πάσα στιγμή(Khanetal., 2022).Στην παρακάτω λίστα εξετάζεται καθένα από αυτά ξεχωριστά:

- **Εναλλακτική λύση χαμηλού κόστους**

Πρωτίστως οι τεχνολογίες του υπολογιστικού νέφους είναι οικονομικά αποδοτικές και βελτιώνουν την αναλογία μεταξύ του κόστους συντήρησης και των διακριτικών δαπανών μιας εταιρείας, κυρίως σε έργα προστιθέμενης αξίας. Η μεγάλη πλειονότητα των τμημάτων πληροφορικής ξοδεύουν, στις μέρες μας, το μεγαλύτερο μέρος των ετήσιων προϋπολογισμών τους για συντήρηση και αναβάθμιση, ενέργειες που προσθέτουν ελάχιστη προστιθέμενη αξία. Στην πραγματικότητα δεν υπάρχει κανένα απτό όφελος, στην περίπτωση που μια εταιρία εναλλακτικά προβεί στη μείωση των εξόδων υποδομής, χρησιμοποιώντας υφιστάμενο λογισμικό και λειτουργικό, ενώ τελικά θα χρειαστεί να πληρώσει μεγαλύτερο κόστος για την ολοκλήρωση (*integration*)των νέων εφαρμογών που δημιουργεί και θα χρειαστεί να φιλοξενηθούν στις παλιές υποδομές.

Η ισορροπία μεταξύ συντήρησης των υφιστάμενων συστημάτων και απόσβεσης της νέας προστιθέμενης αξίας είναι ζωτικής σημασίας για την επιβίωση κάθε οργανισμού. Έχοντας την παραπάνω αρχή κατά νου, κάθε οργανισμός θα πρέπει να έχει ακριβή εικόνα τόσο για τη σημασία της υιοθέτησης μιας συνολικής προοπτικής όσο και για τις πραγματικές δαπάνες της πληροφορικής στο σύνολό της, οι οποίες περιλαμβάνουν τις δαπάνες του προσωπικού του τμήματος *IT*, το κόστος ολοκλήρωσης, το κόστος αναφοράς, το κόστος σχεδιασμού και αποκατάστασης καταστροφών και τέλος την τιμή μετάβασης από τον έναν πάροχο υπηρεσιών νέφους σε έναν άλλον στην περίπτωση που το επίπεδο υπηρεσιών δεν αποδειχθεί το αναμενόμενο. Η υιοθέτηση του υπολογιστικού νέφους επιβαρύνεται από τα άτομα και τις επιχειρήσεις που επηρεάζονται από κακούς συμβατικούς δεσμούς και όχι από τις επιτακτικές αναλύσεις κόστους / οφέλους. Ένας σημαντικός παράγοντας απόδειξης του κόστους /οφέλους

είναι η ευκαιρία για οικονομίες κλίμακας και καινοτομίας που προσφέρει το νέφος. Τα επιχειρηματικά τμήματα των οργανισμών στρέφονται στους παρόχους αντί για τα συμβατικά τμήματα πληροφορικής λόγω και του χαμηλού κόστους της τεχνολογίας που προσφέρουν οι πάροχοι.

Ο ρόλος του *IT* τμήματος μιας εταιρίας αλλάζει από προμηθευτή υλοποίησης σε σύμβουλο κινδύνου και σύμβουλο παρόχου. Προκειμένου η μετάβαση αυτή να βοηθήσει ουσιαστικά τα διάφορα επιχειρηματικά τμήματα του οργανισμού, απαιτούνται νέα σύνολα δεξιοτήτων πληροφορικής και μια νέα οργάνωση γύρω από τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) της εταιρίας. Η πληροφορική θα πρέπει να είναι ουσιαστικά ενοποιημένη με τις εκάστοτε επιχειρηματικές μονάδες και να γίνεται αντιληπτή ως στοιχείο όλων των επιμέρους μονάδων του οργανισμού παρά ως σιλό ομάδων ή ατόμων σε θέσεις συνδέσμου ή ακόμη χειρότερα ως ένα πλήρως ανεξάρτητο τμήμα. Όταν οι πόροι της πληροφορικής αγκαλιάσουν τη νέα τεχνολογία, θα πρέπει να εκπαιδευτούν, να καθοδηγηθούν και να ενημερωθούν σχετικά με τις νέες αυτές ανάγκες συμμόρφωσης.

- **Απόκριση/Ευελιξία**

Παρόλο που οι στόχοι της διαθεσιμότητας και της αξιοπιστίας ενδέχεται να επιτυγχάνονται από μια παραδοσιακή αρχιτεκτονική που παρέχεται από το τμήμα πληροφορική ενός οργανισμού, διατηρώντας παράλληλα λογικά τα έξοδα, η ανταπόκριση και η ευελιξία σε πολλές περιπτώσεις τείνουν να είναι τελικά πιο σημαντικοί παράγοντες από το κόστος. Στις περιπτώσεις όπου το δυναμικό πωλήσεων αναδιαρθρώνεται, ένα νέο προϊόν εισάγεται ή μια νέα εταιρεία εξαγοράζεται, όπου είναι πιθανόν ακόμη και το ενδεχόμενο των απολύσεων, απαιτούνται επιπρόσθετοι υπολογιστικοί και άλλου τύπου πόροι και μάλιστα, αυτοί είναι συνήθως απαιτητοί σε σύντομο χρονικό διάστημα. Οι πόροι αυτοί σε τέτοιες περιπτώσεις έχει αποδειχθεί ότι συνήθως τείνουν να εξαντλούν ολόκληρο τον προϋπολογισμό του *IT* τμήματος σε πολύ σύντομο χρονικό διάστημα. Ως εκ τούτου, σε αυτές τις περιπτώσεις καθίσταται περισσότερο σημαντικό να διατηρείται ο οργανισμός σε λειτουργία παρά να γίνεται χρήση της τεχνολογίας για τη βελτίωση των διαδικασιών.

Σε μια περίπτωση εξαγοράς, είναι πιθανό ο πάροχος να έχει περισσότερη τεχνογνωσία στη συγχώνευση των μισθολογίων των δύο εταιρειών από ό,τι τα εσωτερικά τμήματα της πληροφορικής καθεμιάς από τις δυο συγχωνευμένες εταιρίες. Η τεχνογνωσία του παρόχων μπορεί να οδηγήσει σε μια πιο ευέλικτη και οικονομικά προσιτή λύση από τις παραδοσιακές ομάδες πληροφορικής. Η ανάθεση τέτοιων καθηκόντων σε έναν πάροχο απελευθερώνει χρόνο από την εσωτερική ομάδα του *IT* τμήματος για να χειριστεί άλλα δύσκολα ζητήματα, όπως

είναι η διαχείριση των ατόμων, η ενοποίηση των διαδικασιών και των γραμμών παραγωγής και η μεγιστοποίηση της αξίας της εξαγοράς.

Η λειτουργία της πληροφορικής σε καθημερινή βάση (*BAU: Business-as-Usual*) θα πρέπει επίσης να ακολουθεί την λογική της επένδυσης σε κρίσιμες επιχειρηματικές λειτουργίες. Εάν η πλειονότητα του προϋπολογισμού *IT* χρησιμοποιείται για εργασίες ρουτίνας ή συντήρησης, η ποιότητα των υπηρεσιών που προσφέρουν αξία, θα μειωθεί. Οι χρήστες είναι λιγότερο ικανοποιημένοι εάν δεν μπορούν να επωφεληθούν από τις αλλαγές της τεχνολογίας. Η ευελιξία επιτρέπει σε έναν τμήμα μιας εταιρείας να προσαρμόζεται στους μεταβαλλόμενους νόμους, να ανταποκρίνεται στις νέες απαιτήσεις και να δημιουργεί πιο αποτελεσματικούς τρόπους για να εκτελεί λειτουργίες. Ο μεγαλύτερος κίνδυνος για μια εξελισσόμενη εταιρία είναι η απώλεια της ανταπόκρισης, της ευελιξίας και της προσαρμοστικότητας, σταθερές τις οποίες μπορεί να εγγυηθεί ένας πάροχος υπολογιστικού νέφους.

- **Το κόστος πληροφορικής είναι σύμφωνο με τον όγκο των συναλλαγών**

Ένα γλαφυρό παράδειγμα του πλεονεκτήματος της αποτίμησης του κόστους ανάλογα με τον όγκο των συναλλαγών περιγράφεται στη συνέχεια. Μια επιχείρηση χρειάζεται να συγκεντρώσει άμεσα νέο προσωπικό πωλήσεων σε μια διαφορετική περιοχή από εκείνη που κλασικά δραστηριοποιείται. Για την παρακολούθηση της εκτέλεσης των πωλήσεων και του διαμετρήματος της ζήτησης, υπάρχουν κριτήρια που περιλαμβάνουν υψηλό επίπεδο γνώσης και κατάρτισης στη διαχείριση των πωλήσεων. Με βάση τα αρχικά αποτελέσματα, θα κριθεί αν θα μπορούσαν να γίνουν περισσότερες επενδύσεις. Ο αντίκτυπος στις ταμειακές ροές, ένας από τους πιο κρίσιμους δείκτες της εταιρείας, προστίθεται στους παράγοντες της ανταπόκρισης. Μια επιχείρηση μπορεί να αγοράσει όσες εφαρμογές υπολογιστικού νέφους χρειάζεται για να υποστηρίξει μια δυναμική ανάγκη που μπορεί να έχουν οι πωλήσεις μιας και αυτές ενδέχεται είτε να συρρικνωθούν είτε να αυξηθούν. Έτσι δεν απαιτείται να γίνει από την αρχή μια τεράστια επένδυση σε υλικό και λογισμικό για την ικανοποίηση μιας κατά τα άλλα αμφίβολης και αμφιλεγόμενης απαίτησης.

Ένα άλλο παράδειγμα είναι η ενοικίαση ενός προγράμματος *IT* για την αξιολόγηση της Εταιρικής Διακυβέρνησης, της Διαχείρισης Ρίσκου και της Κανονιστικής Συμμόρφωσης (*GRC: Governance, Risk and Compliance*) για δοκιμές ελέγχου που μια επιχείρηση μπορεί να απαιτείται να διεξάγει μία φορά το χρόνο. Η ενοικίαση μιας τέτοιας υποδομής κατά το απαιτούμενο χρονικό πλαίσιο μπορεί να οδηγήσει σε εξοικονόμηση κόστους. Επιπροσθέτως, η επιχείρηση μπορεί να επωφεληθεί από την αυτοματοποίηση και την ταχύτερη συμμόρφωση με τους νέους νόμους που μπορεί να προσφέρει ένας *SaaS* προμηθευτής.

- **Οι τεχνολογικές επιλογές ελέγχονται άμεσα από τους επαγγελματίες χρήστες**

Στο μέλλον, οι επαγγελματίες χρήστες θα μπορούν να επιλέγουν τις υπηρεσίες που θέλουν να χρησιμοποιήσουν απευθείας από έναν κατάλογο υπηρεσιών. Σε αυτήν την περίπτωση, το τμήμα *IT* ενδέχεται να έχει ελάχιστη έως καθόλου ανάμειξη στη διαδικασία συναλλαγής υπηρεσιών και οι πάροχοι ενδέχεται να αποδίδουν τις χρεώσεις για τις συναλλαγές και τις υπηρεσίες που ένας επιχειρηματικός χρήστης χρησιμοποιεί, απευθείας σε αυτόν. Σε αυτή την περίπτωση, οι επιχειρησιακοί χρήστες θα έχουν ένα κίνητρο να σταματήσουν να χρησιμοποιούν ξεπερασμένες λειτουργικότητες και υποδομές, γεγονός που θα αύξανε την αξιολόγηση του κόστους / οφέλους των ΤΠΕ του οργανισμού.

- **Διάκριση μεταξύ εφαρμογών για ιδιώτες καταναλωτές και επιχειρήσεις**

Τα εργαλεία που προσφέρονται μέσω του Διαδικτύου χρησιμοποιούνται συχνά πιο αποτελεσματικά στο σπίτι παρά από τους εργαζόμενους στο χώρο εργασίας τους. Οι άνθρωποι τείνουν να συνεργάζονται καλύτερα με τους φίλους τους στο σπίτι, από ότι στο εργασιακό περιβάλλον, με τους συναδέλφους τους. Αυτό εν μέρει συμβαίνει, γιατί στην καθημερινή ζωή οι άνθρωποι αξιολογούν την αξία των εφαρμογών που χρησιμοποιούν και καταβάλλουν την απαραίτητη προσπάθεια για να τις ενσωματώσουν στη μέθοδο λειτουργίας των ίδιων και της οικογένειάς τους δεν χρησιμοποιούν κάτι που δεν λειτουργεί ή δεν τους ταιριάζει. Στην αντίθετη περίπτωση βρίσκουν ένα υποκατάστατο, το οποίο ανταποκρίνεται καλύτερα στις ανάγκες τους. Θα πρέπει να σημειωθεί ότι η παραγωγικότητα των εργαζομένων τόσο στην επαγγελματική όσο και στην οικιακή τους ζωή επηρεάζει η μια την άλλη και προωθεί την τάση για υιοθέτηση αποτελεσματικών εργαλείων. Είναι αναπόφευκτο λοιπόν, κάποια στιγμή στο σύντομο μέλλον, οι επαγγελματίες να έχουν τις ίδιες απαιτήσεις από τις προσφερόμενες υπηρεσίες του*IT* τμήματος του οργανισμού τους. Όσο σύγχρονο και ενημερωμένο, μπορεί τελικά να φροντίσει να είναι, ένα τέτοιο τμήμα σε έναν οργανισμό, σε καμία περίπτωση δεν μπορεί να συναγωνιστεί τους παρόχους στο σύννεφο.

## 2.2 Μειονεκτήματα

Αρκετές επιχειρήσεις έχουν διαπιστώσει ότι η εξοικονόμηση κόστους από το *cloud computing* είναι επωφελής. Από τα όσα προαναφέρθηκαν, γίνεται φανερό ότι δίνεται η δυνατότητα στις εταιρείες να επικεντρωθούν στην άσκηση των βασικών τους καθηκόντων παρά τις δυσκολίες των υποδομών και της πληροφορικής. Παρ 'όλα αυτά, εξακολουθούν να υπάρχουν σαφή μειονεκτήματα που εμπεριέχονται στο υπολογιστικό νέφος τα οποία και θα πρέπει σε κάθε περίπτωση να ληφθούν υπόψη.

- **Χρόνος διακοπής λειτουργίας**

Κανένας προμηθευτής *cloud* δεν μπορεί να επιβεβαιώσει την ανοσία σε διακοπές της προσφερόμενης υπηρεσίας. Τα συστήματα του νέφους βασίζονται στο διαδίκτυο. Ως αποτέλεσμα, η πρόσβαση σε αυτές βασίζεται εξ ολοκλήρου από τη σύνδεση των καταναλωτών στο διαδίκτυο. Τα συστήματα νέφους μπορεί να δυσλειτουργούν όπως κάθε άλλο τεχνολογικό εργαλείο, και αυτό πρακτικά σημαίνει ότι ο κάθε οργανισμός θα αναγκαστεί να βιώσει σημαντικές απώλειες στην περίπτωση που υπάρξουν μεγάλες ή συχνές διακοπές στη λειτουργία του.

- **Απόρρητο και ασφάλεια**

Θέματα ασφάλειας και απορρήτου θα πρέπει να περιλαμβάνονται σε κάθε συζήτηση σχετικά με τα δεδομένα. Τα δεδομένα του διαδικτύου είναι ευάλωτα σε τροποποιήσεις, υποκλοπές, παραβιάσεις και παρεμβάσεις. Τόσο οι πληροφορίες που έχουν να κάνουν με τα διαπιστευτήρια του χρήστη (*credentials*) όσο και η εμπιστευτικότητα των δεδομένων που βασίζονται στο *cloud* είναι ευαίσθητα δεδομένα. Η χρήση μιας απομακρυσμένης υποδομής που βασίζεται σε σύννεφο ισοδυναμεί ουσιαστικά με εξωτερική ανάθεση όλων των πόρων μιας εταιρείας σε τρίτα μέρη. Η υποκείμενη υποδομή του υλικού μιας ανάπτυξης στο νέφος υποτίθεται ότι διαχειρίζεται και προστατεύεται από τον πάροχο, ωστόσο η έλλειψη εμπιστοσύνης ανάθεσης των ευαίσθητων πληροφοριών σε τρίτους είναι ένα λεπτό ζήτημα, ανεξάρτητα από το πόσο προσπαθούν να πείσουν οι πάροχοι για το αντίθετο.

- **Ευπάθεια σε επίθεση**

Οποιοδήποτε μέρος μιας υπηρεσίας υπολογιστικού νέφους μπορεί να είναι προσβάσιμο μέσω του παγκόσμιου Ιστού. Είναι φανερό ότι όσες οντότητες διασυνδέονται με το διαδίκτυο δεν μπορεί να είναι 100% ασφαλείς έναντι κακόβουλων ή τυχαίων βλαβών, καθώς οι κυβερνοεπιθέσεις και τα κενά ασφαλείας επηρεάζουν ακόμη και τις καλύτερες ομάδες. Επιπροσθέτως, καθώς το υπολογιστικό νέφος είναι ένας κοινόχρηστος πόρος, η προστασία των δεδομένων τείνει να αξιολογείται ως ακόμη πιο δύσκολη.

- **Περιορισμένος έλεγχος και ευελιξία**

Δεδομένου ότι η υποδομή ανήκει εξ ολοκλήρου σε ένα τρίτο μέρος, υφίσταται τις πολιτικές διαχείρισης και τα πρωτόκολλα συντήρησης του παρόχου των υπηρεσιών. Ως εκ τούτου, υπάρχει ελάχιστος έλεγχος σε αυτήν. Οι χρήστες του νέφους έχουν ποικίλους βαθμούς περιορισμένου, ωστόσο, ελέγχου σχετικά με τον τρόπο λειτουργίας της υποδομής φιλοξενίας τους. Επίσης, υπάρχουν πολιτικές που καθορίζουν τον έλεγχο που μπορούν να ασκούν οι καταναλωτές στα δεδομένα, στις υπηρεσίες και στις εφαρμογές.

- **Εξαρτήσεις πλατφόρμας υπολογιστικού νέφους**

Μια επιλογή παρόχου είναι μια σιωπηρή εξάρτηση και ισοδυναμεί συνήθως με «κλείδωμα πωλητή» (*vendor lock-in*).Η εναλλαγή από μια πλατφόρμα *cloud* σε μια άλλη, ενδέχεται να μην είναι δυνατή, λόγω κάποιας θεμελιώδους διαφοράς μεταξύ των προμηθευτών. Πέραν τούτου, η αλλαγή των εφαρμογών μιας εταιρίας προκειμένου να ταιριάζει στις ανάγκες ενός νέου κεντρικού υπολογιστή μπορεί να είναι δύσκολη και δαπανηρή. Τέλος, η μετεγκατάσταση από έναν πάροχο σε έναν άλλο μπορεί να εκθέσει τα δεδομένα ενός οργανισμού σε νέους κινδύνους ασφαλείας και ελαττώματα απορρήτου.

- **Κόστος και συμφέρον των παρόχων στο σύννεφο**

Αν και το υπολογιστικό νέφος μπορεί να είναι αρκετά δαπανηρό όσον αφορά τα μικρά έργα, τις βραχυπρόθεσμες πρωτοβουλίες και τις μικρές επιχειρήσεις, εντούτοις αποδεικνύεται ότι μπορεί να προσφέρει εξοικονόμηση χρημάτων σε έναν οργανισμό σε μακροπρόθεσμα μεγέθη, ή ακόμη και με βραχυπρόθεσμους όρους όταν αναφέρεται σε τεράστιες πολυεθνικές εταιρείες. Αν και αρχικά δίνεται η δυνατότητα να περιοριστούν οι υπάλληλοι, τα έξοδα υλικού και οι απαιτήσεις του φυσικού χώρου, το τελικό κόστος μπορεί να είναι μεγαλύτερο από το αναμενόμενο.

Όπως είναι κατανοητό, οι πάροχοι έχουν επενδύσει πολλά χρήματα σε υποδομές στα διάφορα κέντρα δεδομένων και τα έξοδα που πραγματοποιήθηκαν για την απόκτησή τους θα πρέπει να ανακτηθούν από τον τελικό καταναλωτή. Έτσι, η αρχική χρέωση υπηρεσιών στις περισσότερες περιπτώσεις είναι σχετικά φθηνή ώστε η λύση να μοιάζει πιο ελκυστική. Κάθε πελάτης θα πρέπει να παρέχει μια σταθερή και αυξανόμενη ροή εισοδήματος για να λειτουργήσει το επιχειρηματικό μοντέλο. Από την άλλη, καθώς η ζήτηση για υπηρεσίες *cloud* αυξάνονται, τα μεγάλα υπολογιστικά κέντρα θα πρέπει να επεκτείνονται. Αυτό βέβαια σημαίνει επιπλέον κόστη για τον πάροχο.

- **Συνεργασία αλλά όχι κοινή λήψη αποφάσεων**

Τέλος, θα πρέπει οι οργανισμοί που εξετάζουν την μετάβαση στο σύννεφο, να έχουν υπόψιν τους ότι οι πάροχοι συνεργάζονται με τους πελάτες τους, όμως τελικά κανένας πελάτης δεν ασκεί σημαντική επιρροή στις τελικές αποφάσεις. Οι πάροχοι σε ορισμένες περιπτώσεις κάνουν περιστασιακά χρήση αποκλειστικών τεχνολογιών, συχνά από ανάγκη, με το κόστος επιλογής τους να μετακυλίεται στον τελικό καταναλωτή.

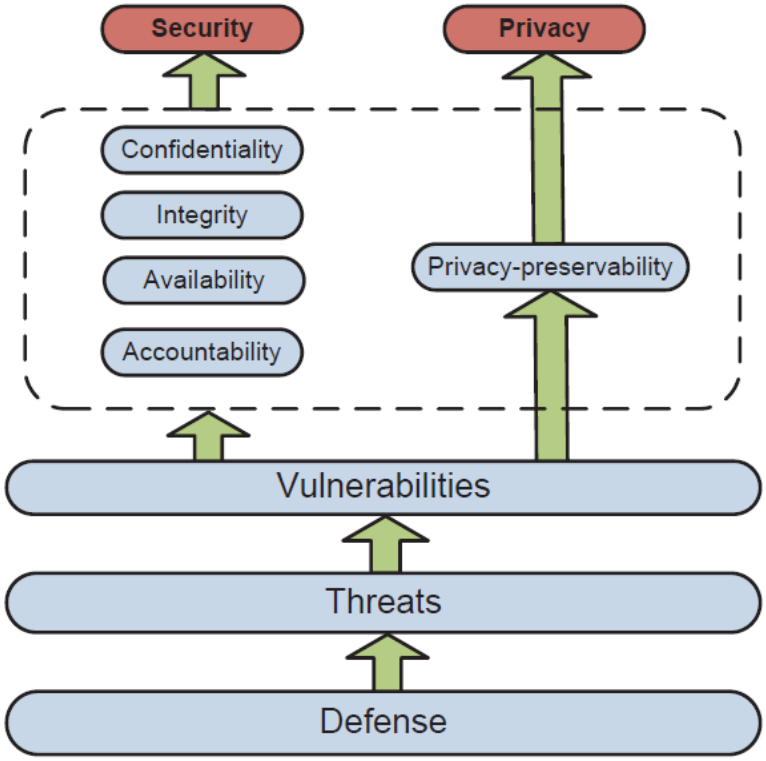
## 3. ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ

Η ασφάλεια των πληροφοριών και των δεδομένων διέπεται από την Τριάδα της *CIA*(*CIA triad: Confidentiality, Integrity, and Availability*) εστιάζοντας στις τρεις βασικές έννοιες της

εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Οι πολιτικές και οι έλεγχοι ασφάλειας που μειώνουν τους κινδύνους για αυτά τα τρία κρίσιμα, βασικά στοιχεία που διέπουν τις πληροφορίες αποτελούν μέρος ενός διεξοδικού σχεδίου ασφάλειας και συνιστούν το βασικό υπόβαθρο της ασφάλειας των πληροφοριών.

Το οικοσύστημα της ασφάλειας και της ιδιωτικότητας συνθέτουν ακόμη δύο έννοιες που αφορούν στην Λογοδοσία και στην Διατήρηση της Ιδιωτικότητας. Ορισμένοι ερευνητές θεωρούν το Απόρρητο/Ιδιωτικότητα ως ένα συστατικό της ασφάλειας. Στην μελέτη τους οι Xiao&Xiao (2013) διαχωρίζουν το απόρρητο από την ασφάλεια λόγω της μεγάλης σημασίας του σε περιβάλλοντα υπολογιστικού νέφους. Η σχέση μεταξύ ιδιωτικού απορρήτου και ασφάλειας θεωρείται ότι είναι πολύ σημαντική, όπως και άλλα χαρακτηριστικά ασφάλειας που είτε ενισχύουν είτε υπονομεύουν το απόρρητο.

Θα πρέπει να τονιστεί ότι το παραπάνω πλαίσιο δεν αποτελεί προνόμιο του υπολογιστικού νέφους. Αντιθέτως, οποιοδήποτε σύστημα υπολογιστών και δικτύων μπορεί να χρησιμοποιήσει το οικοσύστημα ασφαλείας δεδομένου ότι αυτό είναι καθολικό και βρίσκει εφαρμογή σε όλα τα υπολογιστικά συστήματα που αποθηκεύουν και διαχειρίζονται δεδομένα ή πληροφορίες. Οι πέντε συνιστώσες που αναφέρθηκαν συνεισφέρουν στην ασφάλεια και την ιδιωτικότητα του υπολογιστικού νέφους με τον τρόπο που απεικονίζεται παρακάτω:

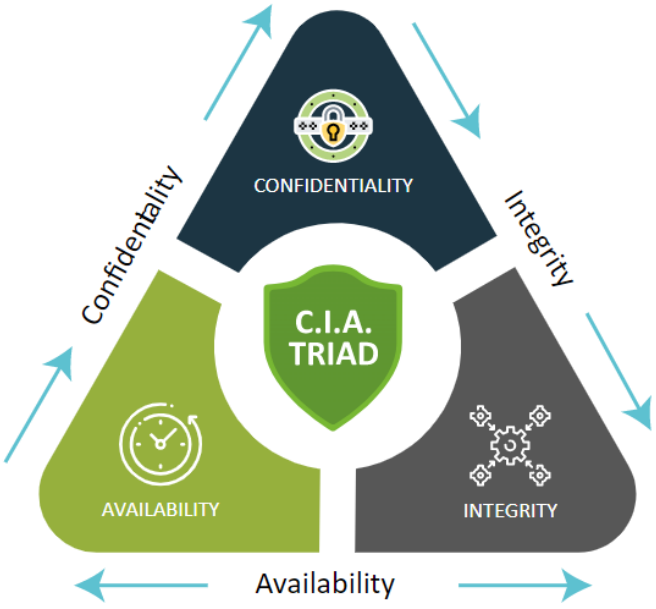



***Εικόνα** 7: Οικοσύστημα ασφάλειας και ιδιωτικότητα στο υπολογιστικό νέφος*
**Πηγή**: Xiao&Xiao, 2013

## 3.1 CIAτριάδα

Οι τρεις συνιστώσες της *CIA*τριάδας χρησιμεύουν ως ένα γενικό πλαίσιο προκειμένου να καταστεί δυνατή η προστασία των δεδομένων των ατόμων τόσο από αδυναμίες (*vulnerabilities*)τις οποίες μπορεί να εκμεταλλευτούν οι επιτιθέμενοι όσο και από κακό χειρισμό (*mishandling*) ή από μη εξουσιοδοτημένη πρόσβαση (*unauthorized access*). Τα τρία αυτά βασικά ζητήματα αφορούν την ασφάλεια των δεδομένων γενικά και κατ' επέκταση την ασφάλεια των δεδομένων στο υπολογιστικό νέφος. Το μοντέλο της τριάδας *CIA*, έχει σχεδιαστεί για να καθοδηγεί τις πολιτικές και την ασφάλεια των πληροφοριών σε έναν οργανισμό. Ένα πρόγραμμα ασφαλείας πρέπει να χειρίζεται κατάλληλα την πλήρη Τριάδα της *CIA* προκειμένου να θεωρείται ολοκληρωμένο και πλήρες (Abdulsalam&Hedabou, 2022; Alleweldt, 2012; Bhatia&Malhotra; CertMike.com, 2023; El-Sofany&El-Seoud, 2019; ICO, 2023; Krutz&DeanVines, 2010; Mather et al., 2009; Neumann, 1977; Office of Information Security, 2023; Sen, 2015; Toth, - NIST, 2022).

Μερικές φορές η τριάδα CIA αναφέρεται και ως τριάδα *AIC* για την αποφυγή της σύγχυσης με την Κεντρική Υπηρεσία Πληροφοριών των Ηνωμένων Πολιτειών Αμερικής (*CIA: Central Intelligence Agency*) (Krzyzanowski, 2022) . Ο ορισμός του μοντέλου φαίνεται να αναφέρθηκε για πρώτη φορά σε μια δημοσίευση του *NIST* το 1977 (Wikipedia, 2023).




***Εικόνα 8**: Τριάδα CIA*
**Πηγή**:Content Team, 2021

Συνοπτικά, η εμπιστευτικότητα (*Confidentiality*)διασφαλίζει ότι τα δεδομένα, τα αντικείμενα και οι πόροι προστατεύονται από μη εξουσιοδοτημένη προβολή. Η ακεραιότητα (*Integrity*)ορίζει ότι τα δεδομένα προστατεύονται από μη εξουσιοδοτημένες αλλαγές για να

επικυρωθεί ότι αυτά είναι αξιόπιστα και σωστά. Τέλος, η διαθεσιμότητα (*Availability*) πιστοποιεί ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα συστήματα και στους πόρους που χρειάζονται.

Παρακάτω αναλύονται πιο διεξοδικά οι παραπάνω ορισμοί (Abdulsalam&Hedabou, 2022; Alleweldt, 2012; Bhatia&Malhotra; CertMike.com, 2023; ICO, 2023; Krutz&Dean Vines, 2010; Matheretal., 2009; Neumann, 1977; Office of Information Security, 2023; Sen, 2015; Toth- NIST, 2022; Wakelyn, 1976):

### *3.1.1Εμπιστευτικότητα (Confidentiality)*

Η εμπιστευτικότητα αναφέρεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Η διατήρησή της βοηθά σε μια σειρά από ζωτικούς στόχους, συμπεριλαμβανομένης της προστασίας του απορρήτου και της πρόληψης επιθέσεων τύπου λυτρισμικού (*ransomware*).

Τα περισσότερα πληροφοριακά συστήματα αποθηκεύουν δεδομένα που έχουν κάποιο βαθμό ευαισθησίας. Μπορεί να είναι εμπιστευτικές εμπορικές γνώσεις τις οποίες θα μπορούσαν να εκμεταλλευτούν οι ανταγωνιστές ή μπορεί να είναι ιδιωτικές πληροφορίες σχετικά με το προσωπικό, τους πελάτες ή τους καταναλωτές μιας εταιρείας.

Καθώς οι εμπιστευτικές πληροφορίες έχουν σχεδόν πάντοτε αξία, τα συστήματα δέχονται συχνά επιθέσεις από κυβερνοεγκληματίες που αναζητούν ευπάθειες προς εκμετάλλευση. Οι φορείς κινδύνου περιλαμβάνουν πολυεπίπεδες τακτικές όπως η κοινωνική μηχανική και το ηλεκτρονικό ψάρεμα(*phishing*) καθώς και άμεσες επιθέσεις όπως η κλοπή διαπιστευτηρίων και η υποκλοπή δεδομένων δικτύου. Ωστόσο, θα πρέπει να σημειωθεί ότι δεν είναι όλες οι παραβιάσεις της εμπιστευτικότητας σκόπιμες. Οι συνήθεις ακούσιες παραβιάσεις περιλαμβάνουν την αποστολή προσωπικών δεδομένων μέσω *e-mail* σε λάθος παραλήπτη, την τοποθέτηση προσωπικών πληροφοριών σε ανοιχτούς διακομιστές Ιστού και την παραμονή ιδιωτικών δεδομένων ορατά σε μια οθόνη υπολογιστή χωρίς επίβλεψη.

Οι οργανισμοί εφαρμόζουν μια ποικιλία αντίμετρων για την εγγύηση της εμπιστευτικότητας. Το λογισμικό εξασφαλίζει τη διαχείριση της πρόσβασης σε πόρους με τη χρήση κωδικών πρόσβασης, λιστών ελέγχου πρόσβασης και μεθόδων ελέγχου ταυτότητας. Εκτός από τα παραπάνω μέτρα ελέγχου πρόσβασης, η κρυπτογράφηση χρησιμοποιείται για την προστασία των δεδομένων, όπου εξακολουθεί να είναι δυνατή η πρόσβαση παρά τους περιορισμούς, όπως κατά τη διαβίβαση των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Οι φυσικοί έλεγχοι που περιορίζουν την πρόσβαση σε κτίρια και εξοπλισμό, καθώς και άλλα

διοικητικά μέτρα όπως πολιτικές και εκπαίδευση είναι ορισμένες πρόσθετες άμυνες για τη διατήρηση της εμπιστευτικότητας.

Η επικοινωνία μεταξύ ενός πελάτη και της τράπεζάς του, καθώς και μεταξύ ενός πελάτη και του δικηγόρου του ή ενός ασθενούς και του γιατρού του, έχει συχνά χαρακτηριστεί ως «εμπιστευτική». Ο τομέας της υγειονομικής περίθαλψης είναι ένας τομέας όπου υπάρχει πολύ ισχυρό καθήκον να διασφαλίζονται οι πληροφορίες των πελατών. Εκτός από τις απαιτήσεις και τις προσδοκίες των ασθενών, υπάρχουν αυστηροί κανόνες που υπαγορεύουν τον τρόπο με τον οποίο τα ιδρύματα υγειονομικής περίθαλψης χειρίζονται την ασφάλεια. Ο νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (*HIPAA: Health Insurance Portability and Accountability Act*) αντιμετωπίζει τέτοια ζητήματα ασφάλειας, συμπεριλαμβανομένης της προστασίας του απορρήτου, όταν οι ασφαλιστές, οι πάροχοι και οι υπεύθυνοι επεξεργασίας αξιώσεων χειρίζονται ευαίσθητες πληροφορίες υγείας. Σύμφωνα με τους κανονισμούς *HIPAA* απαιτούνται διοικητικές, φυσικές και τεχνικές προφυλάξεις και οι εταιρείες υποχρεούνται στην διεξαγωγή της ανάλυσης και της αξιολόγησης των κινδύνων.

Όσον αφορά τα χρηματοπιστωτικά ιδρύματα, ο πελάτης αναμένει ότι η τράπεζά του θα διατηρήσει την εμπιστοσύνη που συνεπάγεται η σχέση τους, μην αποκαλύπτοντας σε τρίτους πληροφορίες που το ίδρυμα έχει στην κατοχή του σχετικά με τις οικονομικές του υποθέσεις. Φυσικά δεν αναμένει αυτές να προστατεύονται νομικά ούτε να εξαιρούνται από τη γνωστοποίησή τους, εφόσον αποδειχθεί πιθανή αιτία παραπτωμάτων από μέρους του πελάτη. Ενώ οι προσδοκίες των πελατών έχουν συχνά χαρακτηριστεί ως δικαίωμα στην «ιδιωτικότητα» πολλές φορές οι προσδοκίες τους σχετίζονται με το «απόρρητο». Να σημειωθεί ότι οι δύο έννοιες δεν είναι εννοιολογικά ισοδύναμες. Η υποχρέωση της τράπεζας να προστατεύει τα αρχεία των πελατών ορίζεται συνήθως με όρους «εμπιστευτικότητας».

Το Κογκρέσο αγκάλιασε τη γλωσσική διάκριση μεταξύ αυτών των δύο λέξεων, η οποία εμφανίστηκε για πρώτη φορά σε μια έρευνα της Εθνικής Ακαδημίας Επιστημών (*National Academy of Sciences*) το 1972, όταν ψήφισε τον σχετικό νόμο το 1974. Σύμφωνα με αυτή τη μελέτη, η «εμπιστευτικότητα» αναφέρεται στη διατήρηση των ελέγχων για την πρόληψη της μη εξουσιοδοτημένης απελευθέρωσης των πληροφοριών που έχουν συλλεχθεί, ενώ το «απόρρητο» αναφέρεται στην κοινωνική πολιτική σχετικά με το ποιες πληροφορίες πρέπει να συλλέγονται και πόσες πληροφορίες θα πρέπει να διατηρούνται σε ένα ενιαίο σύστημα. Τα τραπεζικά αρχεία θα πρέπει επομένως να αναφέρονται ως «εμπιστευτικά» αντί ως «ιδιωτικά», καθώς ο πελάτης ενδιαφέρεται περισσότερο για τη δημοσιοποίηση πληροφοριών μετά τη λήψη τους παρά για το δικαίωμα της τράπεζας να συλλέγει τις πληροφορίες που απαιτούνται για τη διαχείριση των υποθέσεων που σχετίζονται με τους λογαριασμούς και τις επενδύσεις του.

### *3.1.2 Ακεραιότητα (Integrity)*

Η ακεραιότητα διασφαλίζει ότι τα δεδομένα είναι αξιόπιστα, πλήρη και αμετάβλητα δεν έχουν δηλαδή τροποποιηθεί είτε σκόπιμα είτε ακούσια από εξουσιοδοτημένο ή μη χρήστη. Λάθη κατά την εισαγωγή των δεδομένων, αστοχίες συστημάτων ή παραμέληση της διατήρησης αντιγράφων ασφαλείας μπορεί να θέσουν ακούσια σε κίνδυνο την ακεραιότητα των δεδομένων. Επίσης, μια προσπάθεια παραβίασης δεδομένων από κακόβουλα μέρη ενδέχεται να θέσει σε κίνδυνο την ακεραιότητα. Για παράδειγμα, μια απάτη ηλεκτρονικού ψαρέματος που στοχεύει στο να αλλάξει τους αριθμούς των τραπεζικών λογαριασμών στο σύστημα μισθοδοσίας μιας εταιρίας αποτελεί απειλή για την ακεραιότητα των δεδομένων.

Δημιουργώντας ασφαλείς διαδρομές μέσα από ειδικά κανάλια για τη δημιουργία αντιγράφων ασφαλείας δεδομένων και την κοινή τους χρήση από εξουσιοδοτημένους χρήστες, οι οργανισμοί μπορούν να προστατεύσουν την ακεραιότητα των δεδομένων τους.

Οι πληροφορίες πρέπει να προστατεύονται τόσο κατά τη διατήρησή τους σε υπολογιστές και συστήματα (διακομιστές, βάσεις δεδομένων) όσο και κατά τη μεταφορά τους μεταξύ συστημάτων, όπως η χρήση του ηλεκτρονικού ταχυδρομείου, η ανταλλαγή της πληροφορίας μεταξύ των πολλαπλών διαστρωματώσεων μιας εφαρμογής (*tiers* ή *layers*) ή κατά την ανάκτηση της πληροφορίας από μια βάση δεδομένων. Προκειμένου να διατηρηθεί η ακεραιότητα, είναι ζωτικής σημασίας όχι μόνο να περιοριστεί η πρόσβαση σε επίπεδο συστήματος αλλά και να διασφαλιστεί ότι οι χρήστες ενός συστήματος μπορούν να αλλάξουν εκείνες μόνο τις πληροφορίες που είναι νόμιμα εξουσιοδοτημένοι να πράξουν.

Ενώ όλοι οι κάτοχοι συστημάτων πρέπει να είναι σίγουροι για την ακρίβεια των δεδομένων τους, ο χρηματοπιστωτικός τομέας κατέχει μια ιδιαίτερα πιεστική απαίτηση να εγγυηθεί ότι οι συναλλαγές των πελατών προστατεύονται από παραβιάσεις. Η απόσυρση με δόλιο τρόπο ενός δισεκατομμυρίου δολαρίων από κυβερνοεγκληματίες από τον λογαριασμό της κεντρικής τράπεζας του Μπαγκλαντές στην *Federal Reserve Bank* της Νέας Υόρκης τον Φεβρουάριο του 2016, αποτέλεσε μια από τις πιο διαβόητες παραβιάσεις της ακεραιότητας των οικονομικών δεδομένων στην πρόσφατη μνήμη. Οι επιτιθέμενοι εκτέλεσαν ένα περίπλοκο σχέδιο που περιλάμβανε τη λήψη των απαιτούμενων πληροφοριών σύνδεσης για την έναρξη των αναλήψεων, τη μόλυνση του τραπεζικού συστήματος με κακόβουλο λογισμικό που διέγραφε τα αρχεία της βάσης δεδομένων των μεταφορών και την απόκρυψη των μηνυμάτων επιβεβαίωσης που θα ειδοποιούσαν τις τραπεζικές αρχές για την απάτη.

Η πλειονότητα των συναλλαγών είτε σταμάτησαν είτε τα χρήματα ανακτήθηκαν μόλις αποκαλύφθηκε η απάτη, αλλά οι χάκερς κατάφεραν να διαφύγουν με περισσότερα από 60 εκατομμύρια δολάρια.

Όπως και με την προστασία του απορρήτου, η προστασία της ακεραιότητας των δεδομένων εκτείνεται πέρα και από τις σκόπιμες παραβιάσεις. Τα αποτελεσματικά αντίμετρα ακεραιότητας πρέπει επίσης να προστατεύουν τα δεδομένα και από ακούσιες αλλαγές, όπως λάθη που έγιναν από χρήστες ή απώλεια δεδομένων που δύναται να προκληθεί από μια συσκευή που δεν λειτουργεί σωστά.

Υπάρχουν πολλά αντίμετρα που μπορούν να χρησιμοποιηθούν για τη διαφύλαξη της ακεραιότητας. Οι εξουσιοδοτημένοι χρήστες θα πρέπει να αδυνατούν να κάνουν μη εξουσιοδοτημένες τροποποιήσεις, με τη βοήθεια των ελέγχων πρόσβασης και των αυστηρών ελέγχων ταυτότητας. Οι ψηφιακές υπογραφές και οι επαληθεύσεις κατακερματισμού μπορούν να συμβάλουν στην εγγύηση της ακεραιότητας των δεδομένων και της εξασφάλισης της αυθεντικότητας των συναλλαγών. Εξίσου κρίσιμοι για την προστασία της ακεραιότητας των δεδομένων είναι οι διοικητικοί έλεγχοι όπως ο διαχωρισμός των καθηκόντων και η εκπαίδευση.

### *3.1.3 Διαθεσιμότητα (Availability)*

Η διαθεσιμότητα των δεδομένων αναφέρεται στη δυνατότητα πρόσβασης σε αυτά όταν είναι απαραίτητο. Η προσβασιμότητα των δεδομένων είναι απαραίτητη για τις καθημερινές λειτουργίες ενός οργανισμού.

Ένα πληροφοριακό σύστημα πρέπει να είναι προσβάσιμο στους εξουσιοδοτημένους χρήστες τους, όποτε απαιτείται, προκειμένου να είναι χρήσιμο και να επιτελεί το σκοπό του. Τα μέτρα για την εξασφάλιση της διαθεσιμότητας εγγυώνται την άμεση και αδιάλειπτη πρόσβαση στο σύστημα. Οι δυσλειτουργίες του υλικού, οι απρογραμμάτιστες διακοπές λογισμικού και οι προκλήσεις των ευρών ζώνης των δικτύων είναι μερικοί από τους πιο θεμελιώδεις μη κακόβουλους κινδύνους για τη διαθεσιμότητα. Οι κακόβουλες επιθέσεις μπορεί, επίσης, να λάβουν πολλές διαφορετικές μορφές δολιοφθοράς, οι οποίες δύνανται να στοχεύουν στο να βλάψουν μια εταιρεία εμποδίζοντας τους ανθρώπους να έχουν πρόσβαση στα διάφορα σύστηματά της.

Πολλές επιχειρήσεις δίνουν μεγάλη σημασία στην προσβασιμότητα και την ανταπόκριση ενός ιστότοπου. Ακόμη και μια μικρή διακοπή στην προσβασιμότητά του μπορεί να οδηγήσει σε απώλεια πωλήσεων, σε δυσαρεστημένους πελάτες και σε βλάβη στη φήμη του οργανισμού.

Οι κυβερνοεγκληματίες χρησιμοποιούν τακτικά την επίθεση άρνησης υπηρεσίας (*DOS: Denial of Service*) για να παρέμβουν στις υπηρεσίες Ιστού. Μια επίθεση *DoS* περιλαμβάνει επιθέσεις που κατακλύζουν έναν διακομιστή με περιττά αιτήματα, γεγονός που

βλάπτει την υπηρεσία στους εξουσιοδοτημένους χρήστες. Οι πάροχοι υπηρεσιών έχουν δημιουργήσει διαχρονικά προηγμένες άμυνες ενάντια στις επιθέσεις τύπου *DOS*, αλλά οι απειλές από τέτοιες ενέργειες εξακολουθούν να υφίστανται λόγω της πολυπλοκότητας της φύσης τους και της ανάγκης των κυβερνοεγκληματιών να βρίσκονται πάντα ένα βήμα μπροστά από την πρόληψη.

Ο κατάλογος των αντιμέτρων για τη διασφάλιση της διαθεσιμότητας είναι μακρύς μιας και οι προκλήσεις για τον κατακερματισμό της είναι τόσες πολλές. Τα συστήματα που στοχεύουν σε υψηλή διαθεσιμότητα θα πρέπει να έχουν πλεονασμό υλικού, με διακομιστές αντιγράφων ασφαλείας και αποθήκευση δεδομένων άμεσα διαθέσιμες και προσβάσιμες. Είναι σύνηθες οι μεγάλες επιχειρήσεις να έχουν πλεονάζοντα συστήματα σε πολλές φυσικές τοποθεσίες. Η κυκλοφορία δικτύου και η απόδοση ενός συστήματος θα πρέπει να παρακολουθούνται χρησιμοποιώντας εργαλεία λογισμικού. Τα τείχη προστασίας και οι δρομολογητές είναι δύο τύποι άμυνας έναντι των *DOS* επιθέσεων.

## 3.2 Λογοδοσία (Accountability) και Διατήρηση της Ιδιωτικότητας (Privacy-preservability)

### *3.2.1 Λογοδοσία*

Ο θεμελιώδης στόχος του υπολογιστικού νέφους είναι να παρέχει ένα μέσο για την εξωτερική ανάθεση ορισμένων πτυχών του οργανωσιακού υπολογιστικού περιβάλλοντος ενός οργανισμού σε ένα εξωτερικό τρίτο μέρος μέσω ενός δημόσιου νέφους. Με αυτή την ανάθεση όπως συμβαίνει με κάθε εξωτερική ανάθεση υπηρεσιών τεχνολογίας, αφθονούν οι ανησυχίες σχετικά με τις συνέπειες για το διαδικτυακό απόρρητο και την ασφάλεια των δεδομένων. Η κύρια ανησυχία αφορά τους κινδύνους που ενέχει η μετατόπιση κρίσιμων προγραμμάτων ή δεδομένων από τις εγκαταστάσεις του υπολογιστικού κέντρου ενός οργανισμού σε ένα αποθετήριο που είναι άμεσα διαθέσιμο στο ευρύ κοινό (Jansen&Grance, 2011).

Ενώ η λογοδοσία έχει εξεταστεί αναλυτικά σε άλλα υπολογιστικά συστήματα, στο πλαίσιο του υπολογιστικού νέφους είναι κρίσιμης σημασίας ο απολογισμός αυτής της διάστασης, προκειμένου να καθοριστούν οι κατάλληλες σχέσεις εμπιστοσύνης. Η λογοδοσία υποδηλώνει την ικανότητα ταυτοποίησης ενός ατόμου που, βάσει συγκεκριμένων γεγονότων, ευθύνεται για συγκεκριμένα περιστατικά και γεγονότα. Οι δυο βασικοί εταίροι που εμπλέκονται σε μια υποδομή νέφους είναι οι πάροχοι των υπηρεσιών και οι πελάτες τους, ενώ οι δημόσιοι καταναλωτές που χρησιμοποιούν εφαρμογές που παρέχονται από τους πελάτες είναι η τρίτη κατηγορία των πελατών (Xiao&Xiao, 2013).

Οι κύριοι λόγοι για τη μετάβαση σε ένα δημόσιο σύννεφο είναι τόσο η εξοικονόμηση του κόστους όσο και η βελτίωση της αποτελεσματικότητας. Η απαλλαγή από τις ευθύνες

ασφαλείας δεν πρέπει, ωστόσο, να είναι ένας από αυτούς. Ο οργανισμός είναι τελικά υπεύθυνος για την επιλογή του δημόσιου νέφους καθώς και για την ασφάλεια και το απόρρητο της συμβατικής υπηρεσίας. Εξακολουθεί να είναι υπεύθυνος για την παρακολούθηση και τη φροντίδα τυχόν αναδυόμενων τρωτών σημείων ασφαλείας, καθώς και για τη διατήρηση του ελέγχου άλλων κρίσιμων ζητημάτων όπως η λογοδοσία και το απόρρητο δεδομένων. Μια εταιρία θα πρέπει να παρακολουθεί και να ελέγχει τον τρόπο με τον οποίο ο πάροχος *cloud* προστατεύει και διατηρεί το περιβάλλον υπολογιστών και να εγγυάται ότι τα δεδομένα διατηρούνται και παραμένουν ασφαλή (Jansen&Grance, 2011).

### *3.2.2 Διατήρηση της Ιδιωτικότητας ή Απόρρητο*

Επειδή τα δεδομένα των πελατών και η επιχειρηματική λογική αποθηκεύονται σε «αμφίβολους» διακομιστές υπηρεσιών νέφους που ανήκουν και διατηρούνται από τον εκάστοτε πάροχο, το απόρρητο εξακολουθεί να είναι ένα άλλο σημαντικό ζήτημα όσον αφορά τις ανησυχίες στο υπολογιστικό νέφος. Υπάρχουν επίσης πιθανοί κίνδυνοι ότι προσωπικές πληροφορίες, όπως ένα προσωπικό προφίλ ή άλλα μυστικά δεδομένα, όπως οικονομικά αρχεία ή αρχεία υγείας, θα δημοσιοποιηθούν ή θα κοινοποιηθούν σε δημόσιους ή επιχειρηματικούς ανταγωνιστές. Η διατήρηση της ιδιωτικής ζωής είναι θεμελιώδες συστατικό του απορρήτου. Ορισμένα χαρακτηριστικά ασφαλείας, όπως η εμπιστευτικότητα, η ακεραιότητα, η λογοδοσία κ.λπ., έχουν άμεσο ή έμμεσο αντίκτυπο στην ικανότητα διατήρησης της ιδιωτικής ζωής. Προφανώς, η εμπιστευτικότητα και η ακεραιότητα καθίστανται απαραίτητες προκειμένου να αποτραπεί η αποκάλυψη ιδιωτικών δεδομένων. Η λογοδοσία, αντίθετα, μπορεί να υπονομεύσει το απόρρητο λόγω του γεγονότος ότι οι μέθοδοι επίτευξης των δύο ιδιοτήτων συνήθως συγκρούονται(Xiao&Xiao, 2013).

Η διαφύλαξη του απορρήτου είναι κατά κάποιο τρόπο ένας αυστηρότερος τύπος εμπιστευτικότητας, εξαιτίας της ιδέας ότι και οι δύο περιορίζουν τη διαρροή πληροφοριών. Η έννοια του απορρήτου στο *cloud* είναι διπλή, όπως και σε άλλες υπηρεσίες ασφαλείας: απόρρητο δεδομένων και απόρρητο υπολογιστών (Xiao&Xiao, 2013).

Οι υποστηρικτές του απορρήτου έχουν εκφράσει πολλές ανησυχίες για τη διασφάλισή του στα πλαίσια του υπολογιστικού νέφους. Αυτά τα ζητήματα συνδυάζουν συχνά την ιδιωτικότητα και το απόρρητο. Μερικοί παράγοντες για τους οποίους οι χρήστες θα πρέπει να είναι ενημερωμένοι είναι οι εξής (Matheretal., 2019):

- **Πρόσβαση (*Access*):** Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να γνωρίζουν ποιες προσωπικές πληροφορίες αποθηκεύονται και, σε ορισμένες περιπτώσεις, να μπορούν να ζητήσουν τη διακοπή της επεξεργασίας τέτοιων πληροφοριών. Αυτό είναι

ιδιαίτερα σημαντικό σε σχέση με τις δραστηριότητες μάρκετινγκ, οι οποίες σε ορισμένες χώρες υπόκεινται σε πρόσθετους νόμους και καλύπτονται σχεδόν πάντα από τις πολιτικές απορρήτου των τελικών χρηστών. Η ικανότητα της εταιρείας να παρέχει στο άτομο πρόσβαση σε όλες τις προσωπικές πληροφορίες και να εκπληρώνει τις δηλωμένες απαιτήσεις είναι η κύρια ανησυχία κατά τη χρήση του νέφους. Θα πρέπει να εξασφαλίζεται ότι όλες οι πληροφορίες και τα δεδομένα ενός υποκειμένου που τηρούνται στο σύννεφο θα καταστραφούν εάν ασκηθεί το δικαίωμα της διαγραφής τους.

- **Συμμόρφωση (*Compliance*):**Πολλά ερωτήματα προκύπτουν κατά τη χρήση των υπηρεσιών υπολογιστικού νέφους που έχουν να κάνουν με το ποιες είναι οι απαιτήσεις συμμόρφωσης όσον αφορά το απόρρητο στο *cloud*, ποιος είναι υπεύθυνος για την τήρηση της συμμόρφωσης με τους νόμους, τους κανόνες, τα πρότυπα και τις συμβατικές υποχρεώσεις που ισχύουν για αυτές τις πληροφορίες, ακόμη και το πώς επηρεάζει τις τρέχουσες απαιτήσεις συμμόρφωσης, μια μετάβαση στο νέφος. Τα σύννεφα μπορούν να καλύπτουν πολλές νομικές δικαιοδοσίες. Για παράδειγμα, τα δεδομένα μπορεί να διατηρούνται σε πολλά διαφορετικά κράτη ή πολιτείες ανά τον κόσμο με διαφορετικούς νομικούς κανόνες. Θα πρέπει να είναι σαφής ο καθορισμός της εφαρμοστέας δικαιοδοσίας για τα δεδομένα, οποιασδήποτε οντότητας που τηρείται στο σύννεφο.
- **Αποθήκευση (*Storage*):** Ερωτήματα προκύπτουν όσον αφορά και στην αποθήκευση των δεδομένων, όταν κανείς εξετάζει μια μετάβαση στο νέφος. Τα ερωτήματα αυτά έχουν να κάνουν με το πού φυλάσσονται τα αρχεία δεδομένων του κάθε χρήστη, αν αυτά δύνανται να μεταφερθούν σε διαφορετική εγκατάσταση που μπορεί να ανήκει σε διαφορετική χώρα ή περιοχή χωρίς τη γνώση του υποκειμένου, ακόμη και αν τα δεδομένα αναμειγνύονται με δεδομένα από άλλες εταιρείες που χρησιμοποιούν τον ίδιο πάροχο υπολογιστικού νέφους (*CSP: Cloud Service Provider*). Οι οργανισμοί δεν επιτρέπεται σε ορισμένες περιπτώσεις να αποστέλλουν κάποιες κατηγορίες προσωπικών πληροφοριών σε άλλα έθνη λόγω περιορισμών του απορρήτου που τηρούν έναντι των δεύτερων. Εξαιτίας του γεγονότος ότι τα δεδομένα διατηρούνται στο νέφος, μια τέτοια μεταφορά μπορεί να πραγματοποιηθεί εν αγνοία του οργανισμού, παραβιάζοντας ενδεχομένως τους τοπικούς ή τους εθνικούς νόμους.
- **Διατήρηση (*Retention*):**Ζητήματα εγείρονται όσον αφορά και το διάστημα τήρησης τον δεδομένων όταν αυτά μεταφορτώνονται στο νέφος. Επίσης, πολλές φορές δεν είναι

ξεκάθαρο ποια πολιτική διατήρησης δεδομένων ισχύει ή αν τελικά τα δεδομένα ανήκουν στον οργανισμό ή στον πάροχο. Σε κάθε περίπτωση, θα πρέπει να είναι ξεκάθαρο στον τελικό χρήστη, του ποιος είναι υπεύθυνος για την τήρηση της πολιτικής διατήρησης των δεδομένων τους στο σύννεφο και πώς αντιμετωπίζονται οι εξαιρέσεις σε αυτήν.

- **Καταστροφή (*Destruction*):**Πολλά και ποικίλα ερωτήματα τίθενται όσον αφορά και στην καταστροφή των δεδομένων. Για παράδειγμα, μετά την ολοκλήρωση της περιόδου διατήρησης των δεδομένων, ποιος είναι ο τρόπος διαγραφής των προσωπικών στοιχείων ταυτοποίησης (*PII: Personally Identifiable Information*) από τον πάροχο; Πως μπορούν οι επιχειρήσεις να διασφαλίσουν, ότι τα στοιχεία αυτά διαγράφονται σωστά, την κατάλληλη στιγμή και ότι δεν είναι προσβάσιμα σε άλλους χρήστες του νέφους; Τέλος, πώς μπορούν να είναι σίγουροι οι καταναλωτές ότι ο πάροχος δεν κράτησε άλλα αντίγραφα;

  Η αυξημένη διαθεσιμότητα είναι ένα από τα πλεονεκτήματα που προσφέρουν οι πάροχοι, οι οποίοι συχνά αναπαράγουν τα δεδομένα σε διάφορα συστήματα και τοποθεσίες. Όταν μια εταιρεία επιδιώκει να διαγράψει τα δεδομένα, αυτό το όφελος καθίσταται προβληματικό καθώς είναι δύσκολο έως και αδύνατο σε ορισμένες περιπτώσεις, να διαγραφεί πραγματικά οτιδήποτε έχει αποθηκευτεί στο σύννεφο. Εν τέλει, προκύπτει η αγωνία αν τα δεδομένα καταστράφηκαν πράγματι από τον πάροχο ή απλώς κατέστησαν μη διαθέσιμα στον οργανισμό και αν τελικά τα δεδομένα διατηρούνται για μεγαλύτερο χρονικό διάστημα από αυτό που έχει συμφωνηθεί με τον χρήστη, προκειμένου ο πάροχος να τα εξορύξει για δικούς του σκοπούς (στατιστικά, προβλέψεις) ή για ακόμη ενδεχομένως και για πιο ανέντιμες δραστηριότητες.
- **Παρακολούθηση και έλεγχος (*Monitoring and auditing*):**Η παρακολούθηση και ο έλεγχος είναι υψίστης σημασίας ζητήματα, αλλά πώς μπορούν οι επιχειρήσεις να διασφαλίσουν ότι τα πρότυπα απορρήτου διατηρούνται ενώ τα προσωπικά στοιχεία ταυτοποίησης των εργαζομένων και των πελατών τους βρίσκονται στο νέφος, δίνοντας την απαραίτητη διαβεβαίωση στους ενδιαφερόμενους;
- **Παραβιάσεις απορρήτου (*Privacy violations*):**Η ιστορία έχει αποδείξει ότι οι παραβιάσεις του απόρρητου στο υπολογιστικό νέφος βρίθουν ποικιλομορφίας και οι κυβερονοεγκληματίες βρίσκουν πάντοτε τρόπο για να εξαπολύσουν μια κακόβουλη επίθεση. Αυτό που πολλές φορές δεν είναι σαφές ή δεν συμβαίνει πάντοτε στην πράξη είναι ο τρόπος που θα πρέπει ο τελικός καταναλωτής να μάθει εάν έχει συμβεί μια

παραβίαση και ποιος είναι υπεύθυνος για την επίβλεψη της διαδικασίας ειδοποίησης παραβίασης, μαζί με τυχόν χρεώσεις που σχετίζονται με αυτήν. Θα πρέπει να διασφαλίζεται ο τρόπος που εκτελούνται οι συμβάσεις και τελικά ποιος ευθύνεται εάν αυτές συνεπάγονται υπαιτιότητα που προκλήθηκαν από αμέλεια του παρόχου. Πολλές από αυτές τις ανησυχίες ισχύουν για άλλες μορφές πληροφοριών καθώς και για ένα ευρύτερο φάσμα αναγκών συμμόρφωσης και όχι απλώς για τις προσωπικές πληροφορίες.

# 4.ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΑΠΕΙΛΩΝ ΚΑΙ ΚΙΝΔΥΝΟΙ

Υπάρχουν πολλοί και διαφορετικοί τρόποι να ταξινομηθούν οι απειλές στο υπολογιστικό νέφος. Στην παρούσα διπλωματική εργασία έχει επιλεγεί να παρουσιαστεί η κατηγοριοποίησή τους με πολλές και διαφορετικές οπτικές προκειμένου ο αναγνώστης να αποκτήσει μια πλήρη διάσταση όσον αφορά στο ζήτημα αυτό. Έτσι παρατίθεται αρχικά μια ευρύτερη γενική κατηγοριοποίηση, ενώ στη συνέχεια επιχειρείται μια ταξινόμηση ανάλογα με το αν η απειλή σχετίζεται με την τεχνολογία (λογισμικό ή υλικό) ή τον ανθρώπινο παράγοντα.

## 4.1 Γενική ταξινόμηση των απειλών

Παρακάτω περιγράφεται η κατηγοριοποίηση των απειλών όπως την παρουσίασαν οι Gupta. &Kumar (2013) μιας και η αφαιρετική διάσταση με την οποία παρουσιάζουν το θέμα παρέχει στον αναγνώστη μια συνολική οπτική των απειλών:

- **Κατάχρηση των πόρων του υπολογιστικού νέφους**

Πολλές επιχειρήσεις παρέχουν δοκιμαστική πρόσβαση σε πόρους του υπολογιστικού νέφους. Οι ερευνητές ανακάλυψαν ότι κακόβουλα άτομα χρησιμοποιούν τέτοιες ανώνυμες και κοινές μεθόδους εγγραφής για να έχουν πρόσβαση στους πόρους του νέφους για παράνομους σκοπούς. Εκτελώντας τις επιβλαβείς ενέργειές τους υπό την προστασία του *cloud* περιβάλλοντος, οι εγκληματίες του κυβερνοχώρου βελτιώνουν την ασυλία τους. Το *PaaS* είναι το επίπεδο υπηρεσίας που επηρεάζεται συχνότερα από αυτή την κατηγορία των απειλών, αλλά με την πάροδο του χρόνου, η στόχευση αφορά και στις *IaaS* πλατφόρμες. Η διάρρηξη κωδικού πρόσβασης, η άρνηση και η κατανεμημένη άρνηση επιθέσεων, η παρακολούθηση και ο έλεγχος μέσω *Botnet* και τέλος η φιλοξενία κακόβουλων δεδομένων είναι μερικές από τις θεμελιώδεις επιθέσεις που πραγματοποιούνται για την πραγματοποίηση τέτοιων καταχρήσεων.

- **Η ασφάλεια των διεπαφών**

Οι παρεχόμενες διεπαφές χρησιμοποιούνται από έναν χρήστη για την επικοινωνία με τις υπηρεσίες *cloud*. Αυτά τα *APIs*(*Application Programming Interfaces*) χειρίζονται και εκτελούν όλες τις εργασίες παροχής και διαχείρισης των υπηρεσιών. Ως εκ τούτου, η ασφάλεια αυτών των διεπαφών είναι απαραίτητη προϋπόθεση για την ασφάλεια του νέφους εν γένει. Αν αυτές οι διεπαφές είναι είτε αδύναμες, είτε έχουν τροποποιηθεί σκόπιμα, ενδέχεται να επιτρέψουν σε εξωτερικές οντότητες να παρακάμψουν τις καθορισμένες πολιτικές χρήσης και εργασίας στο νέφος.

Οι βασικές επιθέσεις για τέτοιου είδους απειλές προέρχονται από αδυναμίες που προκαλούνται από λανθασμένες ή ακατάλληλες εξουσιοδοτήσεις, σαφή μετάδοση κειμένου υλικού, έλλειψη εργαλείων καταγραφής και μη αναγνωρισμένες εξαρτήσεις διεπαφών. Ως εκ τούτου, για την εξάλειψη τέτοιων κινδύνων, θα χρειαστεί ένα μοντέλο ασφαλείας με βελτιωμένο έλεγχο πρόσβασης, καθώς και ένα σύστημα με έναν εκτεταμένο μηχανισμό ελέγχου ταυτότητας και μια κρυπτογραφημένη μεταφορά δεδομένων. Επίσης, θα πρέπει κανείς να εξετάσει, να κατανοήσει και να αναλύσει τυχόν εξωτερικές εξαρτήσεις διεπαφών και πώς αυτές μπορεί να επηρεάσουν την ασφάλεια του περιβάλλοντος. Και τα τρία μοντέλα υπηρεσιών του υπολογιστικού νέφους επηρεάζονται από αυτές τις επιθέσεις.

- **Προβλήματα κοινόχρηστης τεχνολογίας**

Η εικονική πρόσβαση σε φυσικούς πόρους υπολογιστή καθίσταται δυνατή χάρη στην τεχνολογία του υπερπιστωτή, όπως αναλύθηκε σε προηγούμενο κεφάλαιο της παρούσας εργασίας, επιτρέποντας σε ένα επισκέπτη να έχει πρόσβαση σε φυσικούς πόρους που έχουν εικονικοποιηθεί. Οι τεχνικές που χρησιμοποιούνται από τις διάφορες πλατφόρμες για εικονικοποίηση των μηχανών, όπως το *VM Escape* το *VM Hoping*και άλλες, έχουν δείξει ότι αυτές οι πλατφόρμες δεν είναι ασφαλείς από επιθέσεις.

Η ιδέα της ατομικής απομόνωσης των δεδομένων ενός χρήστη του υπολογιστικού νέφους στερείται της «εκ των ων ουκ άνευ» εφαρμογής της φύσης του νέφους. Επομένως, είναι σημαντικό να δημιουργηθούν και να τεθούν σε χρήση μοντέλα και υλοποιήσεις ασφαλείας, που να εμποδίζουν έναν χρήστη να έχει πρόσβαση στις ιδιωτικές πληροφορίες και στους πόρους ενός άλλου χρήστη. Επίσης, ένας χρήστης δεν πρέπει και δεν θα μπορεί να παρεμβαίνει στη λειτουργικότητα και την προσβασιμότητα των υπηρεσιών άλλων ενοικιαστών. Το σύστημα θα πρέπει να παρακολουθείται για μη εξουσιοδοτημένες αλλαγές και τροποποιήσεις, με σάρωση ευπαθειών, με επιδιορθώσεις και με διάφορους ελέγχους διαμόρφωσης

προκειμένου να σταματήσουν τέτοιες επιθέσεις. Το επίπεδο *IaaS* της αρχιτεκτονικής του νέφους γίνεται συνήθως στόχος αυτού του τύπου των επιθέσεων.

- **Απώλεια και διαρροή δεδομένων**

Υπάρχουν διάφορες μέθοδοι για να χαθούν τα δεδομένα στο σύννεφο. Μερικές από αυτές περιλαμβάνουν την φυσική διαγραφή των εγγραφών, τη διαγραφή των κλειδιών κωδικοποίησης ή την αποσύνδεση μιας εγγραφής. Οποιαδήποτε από τις παραπάνω μεθοδολογίες μπορεί να οδηγήσει σε απώλεια δεδομένων. Επιπλέον, τα μέτρα πρόληψης για την αποτροπή της διαρροής των δεδομένων μειώνουν τον κίνδυνο οι ευαίσθητες πληροφορίες να πέσουν σε λάθος χέρια. Λόγω του όγκου των δραστηριοτήτων πρόσβασης δεδομένων και της φύσης των δεδομένων που αποθηκεύονται στο νέφος, το ζήτημα είναι σημαντικό. Τα δεδομένα θα πρέπει να διατηρούνται τηρώντας τα πλαίσια για την ασφάλεια, διεξάγοντας παράλληλα τακτικούς ελέγχους παρακολούθησης της ακεραιότητας. Σε γενικές γραμμές, αυτός ο κίνδυνος επηρεάζει όλα τα μοντέλα διάθεσης.

## 4.2 Κατηγοριοποίηση: Τεχνολογία και Ανθρώπινος παράγοντας

Η ιδέα του *cloud computing* είναι μια έννοια που έχει πολλές και διαφορετικές ιδιότητες και χαρακτηριστικά. Μια από αυτές είναι το κοινωνικό περιβάλλον στο οποίο λειτουργεί μια υπηρεσία υπολογιστικού νέφους, επομένως τόσο τα τεχνικά όσο και τα ανθρώπινα στοιχεία, συμπεριλαμβανομένων των κοινωνικοτεχνικών προκλήσεων, των ανησυχιών του πολιτιστικού και κοινωνικού πλαισίου, των τοπικών ή των διεθνών κανόνων, των ψηφιακών δεξιοτήτων των χρηστών είναι μεταβλητές που πρέπει θα πρέπει να λαμβάνονται υπόψη.

Αν και ενώ οι ανησυχίες για την ασφάλεια και οι κίνδυνοι που προκύπτουν από τη χρήση αυτής της τεχνολογίας είναι σημαντικοί είναι δύσκολο να αποφανθεί κανείς ότι ενδεχόμενη παραβίαση του περιβάλλοντος αντιπροσωπεύει την αποτυχία της τεχνολογίας γενικότερα. Οι απειλές για το υπολογιστικό νέφος ενδέχεται να μην περιορίζονται σε ζητήματα της αρχιτεκτονικής. Αντίθετα, πρέπει να ληφθούν υπόψη όλες οι σημαντικές και εννοιολογικές πτυχές του, συμπεριλαμβανομένων των χρηστών καθώς και όλων των παρόχων, των ενδιάμεσων, του διαδικτύου και των εταιριών που προσφέρουν τις υπηρεσίες τους χρησιμοποιώντας την *cloud* υποδομή.

Οι διάφορες απειλές, έχουν ταξινομηθεί ανάλογα με το είδος τους όπως παρουσιάζονται στην παρακάτω εικόνα (Ahmed&Litchfield,2017):


***Εικόνα 9**: Ταξινόμηση βάσει των τεχνολογικών και ανθρώπινων παραγόντων*
**Πηγή**:Ahmed&Litchfield, 2017

Σε ένα υψηλότερο επίπεδο ταξινόμησης, οι απειλές του *cloud computing* μπορούν να κατηγοριοποιηθούν ως τεχνολογικοί παράγοντες (ή σκληρές απειλές) και ανθρώπινοι παράγοντες (ή ήπιες απειλές).Σύμφωνα με μελέτες, τόσο η τεχνολογία όσο και οι ανθρώπινες πτυχές είναι εξίσου σημαντικές στο περιβάλλον του υπολογιστή. Αυτή η προσέγγιση κάνει διάκριση μεταξύ σκόπιμων και ακούσιων κινδύνων που προκαλούνται από την ανθρώπινη συμπεριφορά και σκόπιμων και τυχαίων κινδύνων που προκαλούνται από το υλικό και το λογισμικό ως τεχνολογία(Ahmed&Litchfield,2017).

### *4.2.1 Ανθρώπινος παράγοντας*

Ο όρος «ήπιες απειλές» αναφέρεται σε κινδύνους που προκύπτουν από ανθρωποκεντρικές συμπεριφορές και ενέργειες. Τέτοιοι κίνδυνοι θα μπορούσαν να συνδέονται με τοπικούς ή εθνικούς κυβερνητικούς κανονισμούς, έλλειψη ασφάλειας δεδομένων και συνέπειας, οι οποίοι

θα πρέπει να είναι ανεξάρτητοι από την τοποθεσία. Η έλλειψη ενημέρωσης των πελατών για την κοινωνικής μηχανική[2], η ανεπαρκή ψηφιακή εκπαίδευση μεταξύ των χρηστών των υπηρεσιών του νέφους, η έλλειψη εμπιστοσύνης μεταξύ των διαφορετικών ενδιαφερομένων (*stakeholders*)του *cloud*, η αδυναμία συμμόρφωσης ή η έλλειψη σαφώς καθορισμένων προτύπων συμμόρφωσης, οι κοινωνικές νόρμες και η κουλτούρα του πληθυσμού που δεν οδηγεί στη συμμόρφωση με τα πρότυπα είναι μερικοί από αυτούς τους κινδύνους. Αυτό δεν σχετίζεται με καταστάσεις όπου η ασφάλεια δεδομένων έχει τεθεί σε κίνδυνο, επειδή, για παράδειγμα, ένα μέλος του προσωπικού άφησε κατά λάθος έναν φορητό δίσκο σε μια δημόσια περιοχή (Ahmed&Litchfield,2017).

Δύο ανθρώπινες μεταβλητές, η συμμόρφωση και η ικανότητα, είναι απαραίτητες να υπάρχουν τόσο από τους τελικούς χρήστες όσο και από τους παρόχους υπηρεσιών νέφους καθώς εξελίσσονται δυναμικά τα ζητήματα ασφάλειας. Ελλείψει συμμόρφωσης, επιτρέπονται ασυνήθιστες πρακτικές και ενδέχεται να προκύψουν κίνδυνοι ασφάλειας. Οι χρήστες, οι προγραμματιστές και οι πάροχοι υπηρεσιών *cloud* θα πρέπει όλοι να επιδεικνύουν βέλτιστες πρακτικές για την πρόληψη των ανεπιθύμητων συμβάντων (Ahmed&Litchfield,2017).

Η κοινωνική μηχανική είναι μια συνεχής πρόκληση για την ασφάλεια του διαδικτύου και, κατ' επέκταση και για το περιβάλλον του νέφους. Η χρήση του *cloud computing* από την κοινότητα συνδέεται άμεσα με το κοινωνικό πλαίσιο των χρηστών, το οποίο με τη σειρά του του σχετίζεται με άλλα στοιχεία όπως η εμπιστοσύνη, η έλλειψη γνώσης ή εκπαίδευσης ή έλλειψη προσοχής ή επαγρύπνησης κατά τη χρήση των υπηρεσιών του υπολογιστικού νέφους. Αυτοί οι όροι παραπέμπουν σε σοβαρούς κινδύνους που σχετίζονται με την εμπιστευτικότητα, την ακεραιότητα και το απόρρητο των πληροφοριών (Ahmed&Litchfield,2017, Krombholzetal., 2013).

Στη μελέτη περίπτωσης της *Snapchat*, παρόλο που, η πρόσβαση στις φωτογραφίες περιορίζεται μετά από σύντομο χρονικό διάστημα, αυτές είναι αποθηκευμένες σε ενδιάμεσους διακομιστές καθώς διέρχονται μέσω του διαδικτύου. Κακόβουλοι χρήστες χρησιμοποίησαν ένα πρόγραμμα τρίτου μέρους για να παρακάμψουν τους όρους και τις προϋποθέσεις του *Snapchat* ώστε να κατεβάσουν και να αποθηκεύσουν φωτογραφίες από τους ενδιάμεσους διακομιστές του. Δεδομένα ή φωτογραφίες υπεκλάπησαν από το πρόγραμμα ακόμη και εικόνες που τραβήχτηκαν από τον αρχικό χρήστη ο οποίος δεν σχεδίαζε να τις αποθηκεύσει ή να τις κοινοποιήσει. Σε ορισμένες περιπτώσεις, οι φωτογραφίες αυτές χρησιμοποιήθηκαν για

[2]Η πράξη επηρεασμού ή χειραγώγησης ατόμων για την ανάκτηση πληροφοριών πρόσβασης σε εμπιστευτικές πληροφορίες είναι γνωστό ως κοινωνική μηχανική (Πηγή: https://el.wikipedia.org/wiki/Κοινωνική_μηχανική).

τον εκβιασμό ή την ακούσια έκθεση κάποιων χρηστών. Στους τελικούς χρήστες είχε δοθεί ένα ψεύτικο αίσθημα ασφάλειας αφού δεν γνώριζαν τον τρόπο που το σύστημα διαχειρίζεται τα δεδομένα. Το παράδειγμα αυτό αποδεικνύει πως ένας κοινωνικά επιβεβλημένος κανόνας δεν ισχύει για τα άτομα που έχουν κακόβουλες προθέσεις (Ahmed&Litchfield,2017).

Τα μηνύματα ηλεκτρονικού ψαρέματος που έχουν ως κύριο στόχο τους τραπεζοπιστωτικά ιδρύματα, δημόσιες υπηρεσίες και οργανισμούς υγείας είναι αρκετά συνηθισμένα στις μέρες μας. Παρά τις επανειλημμένες προειδοποιήσεις και ενημερώσεις των χρηστών να μην ανοίγουν συνημμένα αρχεία από ηλεκτρονική αλληλογραφία αγνώστων παραληπτών, καθώς και να μην κλικάρουν σε ανεπιβεβαίωτους συνδέσμους *URL* (*Uniform Resource Locator*) που περιέχονται στο κύριο σώμα της αλληλογραφίας εκείνοι το κάνουν συχνά. Επίσης, μπορεί να κλικάρουν έναν σύνδεσμο προς έναν ιστότοπο που φαίνεται να είναι αυθεντικός αλλά στην πραγματικότητα είναι απλώς ένα αρχείο *Adobe Flash* το οποίο περιέχει κακόβουλο λογισμικό ή κώδικα. Οι παραπάνω ενέργειες μπορεί να είναι αποτέλεσμα είτε κοινωνικής μηχανικής είτε έλλειψης ψηφιακών δεξιοτήτων.

Όποια και αν είναι η περίπτωση, αρκετοί χρήστες που πέφτουν θύματα αυτής της απάτης επιτρέπουν την ανάπτυξη *botnet*, τα οποία παρέχουν στον κάτοχό του, τον έλεγχο ενός τεράστιου αριθμού μηχανών. Θύμα τέτοιας επίθεσης υπήρξε η *Spark*, μια εταιρεία τηλεπικοινωνιών της Νέας Ζηλανδίας, η οποία υπέστη διακοπή των υπηρεσιών της, ως αποτέλεσμα επίθεσης άρνησης υπηρεσίας σε τουλάχιστον έναν από τους διακομιστές της. Χιλιάδες καταναλωτές έχασαν την πρόσβαση σε ευρυζωνικές υπηρεσίες διαδικτύου, απώλεια που προκλήθηκε όχι από την ίδια την εταιρία ή από τους υπαλλήλους της αλλά από τους πελάτες της, οι οποίοι άνοιξαν κακόβουλα επισυναπτόμενα ηλεκτρονικής αλληλογραφίας και με αυτό τον τρόπο κατέβασαν και εγκατέστησαν κακόβουλο λογισμικό στους υπολογιστές τους (Ahmed&Litchfield,2017).

Επειδή δεν υπάρχουν στοιχεία στην ταξινόμηση που να αλληλοαποκλείονται, μια συγκεκριμένη παραβίαση μπορεί να περιλαμβάνει τελικά πολλές απειλές ή και να έχει αμφισβητούμενα κίνητρα. Το παράδειγμα της *JPMorgan* είναι μια τέτοια περίπτωση. Ενώ δεν υπάρχουν στοιχεία για τον τρόπο που αποκτήθηκαν τα κλεμμένα δεδομένα των πελατών, τα οποία μπορεί να είχαν πωληθεί τόσο σε αποστολείς ανεπιθύμητης αλληλογραφίας όσο και σε εγκληματίες η εμπιστοσύνη προς την εταιρία κλονίστηκε. Ως εκ τούτου, είτε η αιτία μιας τέτοιας παραβίασης είναι τεχνολογική είτε οφείλεται σε ανθρώπινο παράγοντα, η διαφύλαξη του απορρήτου των δεδομένων των χρηστών τίθεται υπό αμφισβήτηση (Ahmed&Litchfield,2017).

Η διαφάνεια τοποθεσίας είναι ένα ζήτημα ασφάλειας που σχετίζεται πιο στενά με τις κοινωνικές ή τις κυβερνητικές συνθήκες και τα πλαίσια παρά με τεχνικά προβλήματα. Δεν υπάρχει καμία διασφάλιση ότι τα δεδομένα θα αντιμετωπίζονται με τον ίδιο τρόπο όταν μεταδίδονται από μια τοποθεσία (ένα κράτος ή μια πολιτεία, για παράδειγμα) σε μια άλλη. Ο βαθμός ασφάλειας καλύπτεται από ένα γενικό πλαίσιο όσον αφορά την επεξεργασία και την αποθήκευση των δεδομένων, μιας και ο ιδανικός στόχος για τη θέσπιση ενιαίων κανονισμών σε όλα τα νομικά συστήματα που αφορούν τη διαχείριση των δεδομένων δεν έχει επιτευχθεί ακόμη (Ahmed&Litchfield,2017).

Οι συμφωνίες επιπέδων εξυπηρέτησης / συμφωνίες επιπέδου υπηρεσιών (*SLA: Service Level Agreement*), απαιτούν διεξοδική αξιολόγηση, καθώς οι υποδομές του υπολογιστικού νέφους είναι περίπλοκες (Casalicchio&Silvestri, 2013).Να σημειωθεί ότι, τα σφάλματα στην ασφάλεια υπηρεσιών νέφους συνδέονται πολλές φορές με παρερμηνείες του *SLA*(Srinivasan et al., 2012). Σε πολλές περιπτώσεις οι πελάτες, ίσως εξαιτίας της έλλειψης γνώσης νομικών ορολογιών να συνάπτουν μια συμφωνία χωρίς να έχουν διαβάσει ή καλύτερα κατανοήσει το πραγματικό νόημα της άδειας του τελικού χρήστη. Η ανάληψη δέσμευσης ενός *SLA* είναι ζωτικής σημασίας προκειμένου να διασφαλιστεί ότι πληρούνται οι απαιτήσεις (Sunetal, 2012). Από την άλλη πλευρά, μπορεί να υποστηριχθεί ότι η έλλειψη δέσμευσης οδηγεί και σε έλλειψη παρακολούθησης(Ahmed&Litchfield,2017; Emeakarohaetal., 2012).

Εν τέλει, είτε λόγω παρανόησης του *SLA*, είτε λόγω μη ρεαλιστικών προσδοκιών, η ασφάλεια και η ιδιωτικότητα στο *cloud* αποτελούν σοβαρά ζητήματα και θα πρέπει να αντιμετωπίζονται ως βασικές προκλήσεις (Gonzalezetal., 2012; Nickersonetal., 2013). Οι πελάτες των υπηρεσιών υπολογιστικού νέφους αναμένεται να εκχωρήσουν τις πιο ιδιωτικές και ευαίσθητες πληροφορίες τους στον εκάστοτε πάροχο (Robertsetal., 2011). Αν και μπορεί να μην είναι σκόπιμη σκέψη, η έλλειψη εμπιστοσύνης είναι μια συνειδητή προϋπόθεση που έχει ο κάθε πελάτης αυτού του τύπου των υπηρεσιών. Να σημειωθεί ότι πρόκειται για μια τεχνολογικά ανεξάρτητη στάση που βασίζεται στην αντίληψη της σχέσης υπηρεσία-καταναλωτής. Το επίπεδο πολιτικής ή οργανωσιακής ανάπτυξης σε μικρο-οργανωτικό ή μακρο-περιφερειακό επίπεδο, καθώς και η ισχύς και η στιβαρότητα ενός ρυθμιστικού πλαισίου, είναι όλοι παράγοντες που επηρεάζουν την εμπιστοσύνη. Ο τρόπος με τον οποίο εφαρμόζονται τα πρότυπα καθώς και το εάν η επιβολή της συμμόρφωσης είναι αρκετά αποτελεσματική σε μια συγκεκριμένη γεωγραφική κάλυψη στην οποία φιλοξενούνται οι υποδομές των υπολογιστικών κέντρων του νέφους (*datacenters*) είναι επίσης βασικά ζητήματα (Ahmed&Litchfield,2017; Srinivasan et al., 2012).

Η συμμόρφωση με τους κανονισμούς και τα πλαίσια διαφέρει από τη διακυβέρνηση, η έλλειψη της οποίας κλονίζει και πάλι την εμπιστοσύνη των τελικών χρηστών. Μια τέτοια περίπτωση αφορά τη διαρροή ευαίσθητων δεδομένων σε πάνω από 68 εκατομμύρια χρηστών του *Dropbox*. Στην επίθεση αυτή το πρόβλημα δεν είχε να κάνει με τη συμμόρφωση όσον αφορά τους κανονισμούς, αλλά στον τρόπο με τον οποίο η ασφάλεια έπρεπε να ενσωματωθεί στις υπηρεσίες του υπολογιστικού νέφους. Η περίπτωση αυτή, αποδεικνύει ότι η εμπιστοσύνη στο *cloud computing* μπορεί να επηρεαστεί είτε από έλλειψη δεξιοτήτων είτε από αδυναμία πρόβλεψης απαιτήσεων ασφαλείας (Ahmed&Litchfield,2017; Guardian News&Media, 2016).

Σε μερικές περιπτώσεις οι επιτιθέμενοι δεν στοχεύουν απευθείας στην αρχιτεκτονική του *cloud*. Μια τέτοια επίθεση αφορά την υπόθεση της *Apple*, όπου οι λογαριασμοί των χρηστών παραβιάστηκαν χρησιμοποιώντας τεχνικές επίθεσης ωμής βίας[3] (*brute-force attack*), γεγονός που είχε ως αποτέλεσμα η ζημιά να είναι περιορισμένη. Παρόλο που η ίδια η εταιρία είχε λάβει ισχυρά μέτρα και μηχανισμούς ασφαλείας για την προστασία της αρχιτεκτονικής της στο νέφος, οι λογαριασμοί και ίσως άλλα συστήματα είναι ευάλωτα σε επιθέσεις εξαιτίας των αδύναμων κωδικών πρόσβασης των χρηστών (Ahmed&Litchfield,2017; Grobauer et al., 2011).

Φυσικά οι απειλές που σχετίζονται με τον ανθρώπινο παράγοντα μπορούν να εισαχθούν στο περιβάλλον του νέφους και εσωτερικά. Για παράδειγμα, οι υπηρεσίες συντήρησης όπως η απόκριση περιστατικού (*incident response*) ή η τακτική προγραμματισμένη συντήρηση (*maintenance*) δίνουν σε πρόσωπα (εσωτερικούς ή εξωτερικούς υπαλλήλους) την ευκαιρία να έχουν πρόσβαση σε πόρους που ενδεχομένως δεν είναι εξουσιοδοτημένοι να χρησιμοποιούν (Ahmed&Litchfield,2017).

### *4.2.2 Τεχνολογικοί παράγοντες*

Οι απειλές που δεν σχετίζονται με ανθρώπινους ή κοινωνικούς παράγοντες αναφέρονται ως τεχνολογικές δυνάμεις. Οι κίνδυνοι και οι απειλές σε αυτήν την κατηγορία μπορούν να χωριστούν σε δύο ομάδες: α) σε αυτούς που σχετίζονται με το υλικό, δηλαδή με την υποδομή και το δίκτυο του υπολογιστικού νέφους και β) σε εκείνους που σχετίζονται με το λογισμικό, δηλαδή με τους πόρους της πλατφόρμας και των εφαρμογών που τρέχουν πάνω από την υποδομή του *cloud*. Επειδή το διαδίκτυο είναι ο πρωταρχικός τρόπος πρόσβασης στους πόρους του νέφους, τα ελαττώματα που βασίζονται σε αυτό εγείρουν ζητήματα ασφάλειας και για τους δύο τύπους (Ahmed&Litchfield,2017; Grobauer et al., 2011).

[3]Η επίθεση ωμής βίας αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα (Πηγή: https://el.wikipedia.org/wiki/Brute-force_attack).

Οι υπηρεσίες Ιστού (*Web Services*), οι εφαρμογές, η εικονικοποίηση και η κρυπτογραφία συνδέονται επίσης με τρωτά σημεία. Μια ποικιλία από τρωτά σημεία ασφαλείας που βασίζονται στο λογισμικό προέρχονται από την εικονικοποίηση. Επιθέσεις άρνησης υπηρεσίας, εκμεταλλεύσεις των hypervisors, όπως hyper-jacking, επιθέσεις στα πλευρικά κανάλια *VM* και διαφυγή υπερπιστωτών είναι μερικά τέτοια παραδείγματα(Ahmed&Litchfield,2017; Grobauer et al., 2011; Perez-Botero et al., 2013).

Τα ζητήματα ασφαλείας επιδεινώνονται από τις υπηρεσίες *web*, όπως ελαττώματα *HTTP*(*Hypertext Transfer Protocol*) που θέτουν σε κίνδυνο τους καταναλωτές κατά τη χρήση των υπηρεσιών *Cloud* (Modietal., 2013). Οι κίνδυνοι περιλαμβάνουν συχνά *SQL Injection*, *Cross-Site Scripting*, *Directory Traversal*, έλλειψη ασφάλειας *AJAX* λόγω ανεπαρκούς προγραμματισμού, τρωτά σημεία σε εξυπηρετητές Ιστού (*Apache web server*) και έλλειψη μέτρων ασφαλείας για χρήση ενός δημόσιου παρόχου *cloud* σε ελεύθερα και ανοικτού κώδικα λογισμικά που χρησιμοποιούνται για τη δημιουργία ιστότοπων όπως στο *WordPress* (Ahmed&Litchfield,2017).

Ενώ οι παραδοσιακοί κρυπτογραφικοί μηχανισμοί μπορεί να συνδέονται με αδυναμίες αποτροπής ορισμένων τύπων επιθέσεων (Fan&Huang, 2013), για παράδειγμα, μια υποκλοπή δεδομένων σε *man-in-the-middle* εκμεταλλεύσεις με επακόλουθη υποκλοπή των δεδομένων δεν λειτουργεί επιτυχώς ως αντίμετρο, σε άλλες όμως περιπτώσεις η κρυπτογραφία χρησιμοποιείται όταν άλλα μέτρα δεν μπορούν να εγγυηθούν την ασφάλεια. Μια τέτοια περίπτωση είναι όταν για παράδειγμα, τα δεδομένα θα πρέπει να κρυπτογραφηθούν πριν αποσταλούν σε μια *cloud* υπηρεσία. Επίσης η κρυπτογραφία δεν είναι επαρκές μέτρο ασφαλείας όταν πραγματοποιηθεί κλοπή των κρυπτογραφικών κλειδιών κατά τη διάρκεια των επιθέσεων πλευρικών καναλιών (*Cross VM Side-Channel Attacks*) (Ahmed&Litchfield,2017).

Η πρακτική «Φέρε τη δική σου συσκευή» (*BYOD: Bring YourOwn Device*) προέκυψε καθώς ο φορητός υπολογιστής έγινε μια δημοφιλής κατανεμημένη και ευρεία συσκευή κατοχής υπολογιστικού μηχανήματος(Chowetal., 2010). Έτσι το φορητό *cloud computing* έγινε αναπόσπαστο μέρος της διαδικασίας χρήσης του υπολογιστικού νέφους(Cheng, 2011). Τα ελαττώματα ασφάλειας της κινητής τεχνολογίας γίνονται όλο και πιο ορατά, ιδιαίτερα στο πιο ανοιχτό περιβάλλον ανάπτυξης των *Android* συσκευών. Οι απειλές και τα τρωτά σημεία που βασίζονται στις εφαρμογές και το δίκτυο εισάγονται στο σύννεφο με τη χρήση αυτών των φορητών υπολογιστικών συσκευών (Ahmed&Litchfield,2017; Fernando et al., 2013; Kulkarni&Khanai, 2015; Vaquero et al., 2011).

Υλικό που είναι κατεστραμμένο ή δεν λειτουργεί σωστά μπορεί να οδηγήσει σε ευπάθειες ασφαλείας. Ωστόσο, οι εταιρείες είναι σε ορισμένες περιπτώσεις απρόθυμες να

αποκαλύψουν μια παραβίαση ή την ακριβή αιτία της, εξαιτίας της ανησυχίας τους για απώλεια της εμπιστοσύνης των τελικών χρηστών ή ακόμη και των βασικών ενδιαφερομένων μερών (*stakeholders*). Οι απειλές που προκύπτουν από δυσλειτουργία υλικού ή εξαρτημάτων δικτύου, ακατάλληλη εγκατάσταση, ασυνεπή συντήρηση ή ανεπαρκή διαχείριση απόκρισης συμβάντων ενδέχεται να υπάρχουν σε ορισμένες από τις παραβιάσεις που περιγράφονται. Σε κάποιες περιπτώσεις, μπορεί να είναι δυνατή ακόμη και η εκμετάλλευση των αδυναμιών στα πρωτόκολλα ομότιμων δικτύων[4](*P2P: peer-to-peer*)(Tong et al., 2013). Τέλος, μια εξωτερική ανάθεση υπηρεσιών *cloud* σε τρίτα μέρη, μπορεί επίσης να έχει ως αποτέλεσμα διαρροή εμπιστευτικών πληροφοριών μέσω παράνομης πρόσβασης, είτε εντός της εγκατάστασης είτε μέσω απομακρυσμένης πρόσβασης σε πόρους του νέφους (Ahmed&Litchfield,2017; Duncanetal., 2012).

Καθώς οι εφαρμογές που εγκαθίστανται στα έξυπνα τηλέφωνα (*smartphones*) των τελικών χρηστών απαιτούν συχνά πρόσβαση σε περισσότερα δεδομένα από όσα χρειάζονται για να λειτουργήσουν, οι χρήστες καταλήγουν να έχουν τελικά ελάχιστο έλεγχο των δεδομένων που διατηρούν στις συσκευές τους. Επίσης, σε αρκετές περιπτώσεις δεν είναι κατανοητό ή ακόμη και κοινοποιημένο στον χρήστη για το αν τα δεδομένα του είναι αποθηκευμένα μόνο τοπικά ή και σε απομακρυσμένα αποθετήρια(Fernando et al., 2013).

Ο κυβερνοκόσμος, ο οποίος έχει κοινωνικο-τεχνικό χαρακτήρα, συχνά εκφράζει τις προσδοκίες κοινωνικής ή πολιτιστικής συμπεριφοράς. Στη μελέτη περίπτωσης της *Spark*, διεξήχθη μια επιτυχημένη επίθεση στο δίκτυο διακομιστών της εταιρείας χρησιμοποιώντας υπολογιστές τελικών χρηστών σε ένα περίπλοκο σχέδιο κοινωνικής μηχανικής.

Στην παραβίαση της *Uber* το 2015 χρησιμοποιήθηκε η κοινωνική μηχανική ως τακτική επίθεσης. Ο κυβερνοεγκληματίας χρησιμοποίησε την ταυτότητα ενός υπαλλήλου πληροφορικής της επιχείρησης. Στη συνέχεια, ο εισβολέας έστειλε μηνύματα κειμένου σε έναν υπάλληλο της *Uber* για να τον πείσει να αποκαλύψει την άδεια εισόδου του με έλεγχο ταυτότητας δύο παραγόντων (*2FA: Two-factor-authentication*). Ο έλεγχος ταυτότητας δύο παραγόντων επέτρεψε την πρόσβαση στο δίκτυο αφού ο επιτιθέμενος είχε ήδη τα διαπιστευτήρια του υπαλλήλου, τα οποία είχαν κλαπεί στο παρελθόν από έναν κλέφτη πληροφοριών (Munson, 2015).

Η πιο πρόσφατη παραβίαση της *Uber* (2022) ξεχωρίζει, ωστόσο, σε αντίθεση με τις προηγούμενες αστοχίες ασφάλειας, επειδή είναι αντιπροσωπευτική ενός μοτίβου επιθέσεων

[4]Ενα ομότιμο δίκτυο είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (*bandwidth*) των κόμβων (Πηγή: https://el.wikipedia.org/wiki/Peer-to-peer).

στην αλυσίδα εφοδιασμού από τρίτους προμηθευτές, οι οποίες καθίστανται όλο και πιο διαδεδομένες. Η παραβίαση των δεδομένων αυτή τη φορά ήταν αποτέλεσμα μιας παραβίασης απόκτησης πρόσβασης στα εσωτερικά συστήματα της *Teqtivity*, ενός τρίτου προμηθευτή διαχείρισης περιουσιακών στοιχείων, και της διαρροής των πληροφοριών λογαριασμού και των προσωπικών στοιχείων ταυτοποίησης (*PII*) περίπου 77.000 υπάλληλων της *Uber* σε φόρουμ κυβερνοεγκληματιών. Σύμφωνα με μια έρευνα της *Security Scorecard*, το 51% των εταιρειών είχαν παραβίαση δεδομένων που προκλήθηκε από τρίτο μέρος. Η παραβίαση δείχνει ότι οι επιχειρήσεις δεν έχουν την πολυτέλεια να βασίζονται σε διαδικασίες ασφαλείας τρίτων προμηθευτών για την ασφάλεια των δεδομένων τους και θα πρέπει να είναι πολύ πιο προσεκτικές στην εκτέλεση της δέουσας επιμέλειας με τις εταιρείες που επιλέγουν να συνεργαστούν (Reed, 2023).

Θα πρέπει να σημειωθεί ότι περισσότερες από μία κατηγορίες μπορούν να χρησιμοποιηθούν για την αντιστοίχιση κάποιων περιπτώσεων κυβερνοεπιθέσεων με την ταξινόμηση. Ενώ η παραβίαση στην περίπτωση του *LastPass* είναι τεχνολογική, αφού επετεύχθη μέσω της πλατφόρμας *cloud*, οι χρήστες συνέβαλαν λόγω του κοινωνικού τους πλαισίου και του βαθμού δεξιοτήτων τους και επομένως σχετίζεται και με τον ανθρώπινο παράγοντα.

Οι περιπτωσιολογικές μελέτες που καλύφθηκαν παραπάνω συνοψίζονται στον παρακάτω Πίνακα, ο οποίος περιέχει επίσης μια σύντομη περίληψη της κάθε επίθεσης και των πιθανών κατηγοριών κινδύνου που σχετίζονται με αυτή.

***Πίνακας 1**: Σύνοψη των επιθέσεων ως προς την ταξινόμηση.*

| **Περιγραφή επίθεσης** | **Τύπος απειλής στην ταξινόμηση** | **Περίπτωση μελέτης** |
|---|---|---|
| Σπάσιμο κωδικού πρόσβασης με τεχνικές επίθεσης ωμής βίας. Στοχευμένη επίθεση σε χρήστες αντί για επίθεση στην αρχιτεκτονική του *cloud* για την απόκτηση των κωδικών πρόσβασης και των διαπιστευτηρίων συγκεκριμένων χρηστών. | Κοινωνικό πλαίσιο, Έλλειψη ικανότητας | *AppleiCloud* |
| Ο κυβερνοεγκληματίας εγγράφηκε στο *VM* και στη συνέχεια απέκτησε πρόσβαση στο εικονικό σύστημα της *SONY* μέσω του διακομιστή *Amazon EC2*. Πρόκειται για μια επίθεση πλευρικού καναλιού. | Υπηρεσίες υπολογιστών, Εικονοποίηση | Επίθεση διακομιστή *SONY* μέσω *VM* της *Amazon* |
| Η ευπάθεια εκτέλεσης αδύναμου κώδικα βοήθησε τους εισβολείς να αποκτήσουν πρόσβαση σε συνολικά 76 εκατομμύρια προσωπικά στοιχεία χρηστών και 7 εκατομμυρίων μικρών επιχειρήσεων (ονόματα, διευθύνσεις *e-mail* και φυσικές διευθύνσεις). | Εργαλεία λογισμικού, Υπηρεσίες Ιστού (Web Services), Κοινωνικό πλαίσιο | Παραβίαση διακομιστή *JPMorgan* |
| Για 4 ολόκληρες ώρες, οποιοσδήποτε λογαριασμός *Dropbox* μπορούσε να προσπελαστεί χρησιμοποιώντας οποιονδήποτε κωδικό πρόσβασης. | Έλλειψη ικανότητας, Εμπιστοσύνη | *Dropbox* |
| Ο διακομιστής *Snapchat* παραβιάστηκε και η εταιρία ισχυρίστηκε ότι αυτό επετεύχθει με τη μέθοδο της αντίστροφης ή ανάστροφης μηχανικής (*reverse engineering*) του *API* μιας τρίτης εφαρμογής, η οποία οδήγησε επίσης σε μη συμμόρφωση με τη συμφωνία άδειας χρήσης του τελικού χρήστη. | Κοινωνικό πλαίσιο, Ικανότητα, Κακή ερμηνεία SLA | *Snapchat* |
| Οι εισβολείς κατέστρεψαν τις υπηρεσίες του προμηθευτή εγκαθιστώντας κακόβουλο λογισμικό στις συσκευές των τελικών χρηστών. Ο προμηθευτής ισχυρίστηκε ότι το κενό βρισκόταν στους υπολογιστές των τελικών χρηστών και δεν είχε καμία σχέση με την αρχιτεκτονική του *cloud*. | Κοινωνική μηχανική, Έλλειψη ικανότητας, Λογισμικό, Εργαλεία, Υπηρεσίες *web*, Πλατφόρμα *Cloud*, Υπηρεσίες υπολογιστών, Εικονικοποίηση | *Spark* |

| | | |
|---|---|---|
| Τα στοιχεία σύνδεσης των χρηστών κλάπηκαν και πωλήθηκαν στο *Dark Net*. Η *Uber* επεσήμανε ότι η ευθύνη βάραινε τους χρήστες, οι οποίοι χρησιμοποίησαν τα ίδια διαπιστευτήρια σύνδεσης σε διαφορετικούς ιστότοπους. | Κοινωνική μηχανική, Έλλειψη ικανότητας, Εμπιστοσύνη, Κανονισμός λειτουργίας | *Uber taxi* (2015) |
| Μια παραβίαση απόκτησης πρόσβασης στα εσωτερικά συστήματα της *Teqtivity*, μέσω ενός τρίτου προμηθευτή, είχε ως αποτέλεσμα τη διαρροή των πληροφοριών λογαριασμών και των προσωπικών στοιχείων ταυτοποίησης περίπου 77.000 υπάλληλων της *Uber* σε φόρουμ χάκερ. | Υπηρεσίες υπολογιστών, Εικονικοποίηση | *Uber taxi* (2022) |
| Εντοπίστηκαν ασυνήθιστες δραστηριότητες στον διακομιστή που είχαν ως αποτέλεσμα την απώλεια δεδομένων χρηστών. Η απροσδόκητη παραβίαση απαιτούσε από τους διακομιστές να μεταβούν στη λειτουργία «*lock-down*». | Πλατφόρμα υπολογιστικού νέφους, Κοινωνικό πλαίσιο, Έλλειψη ικανότητας. | *LastPass* |
| Τα δεδομένα 24 εκατομμυρίων χρηστών παραβιάστηκαν. Η εταιρία δεν αποκάλυψε ποτέ συγκεκριμένες πληροφορίες για το πώς προέκυψε η επίθεση. | Έλλειψη ικανότητας | *Zappos* |

## 4.3Ζητήματα ασφαλείας και κίνδυνοι ανά περιοχή του *cloud*

Στους παρακάτω πίνακες γίνεται μια σύντομη παράθεση των προβλημάτων ασφαλείας σε κάθε περιοχή του υπολογιστικού νέφους. Οι πίνακες διαμορφώθηκαν και αναθεωρήθηκαν μετά από αξιολογήσεις ασφαλείας από διάφορες δημοσιεύσεις και έγγραφα. Σε αυτούς περιγράφονται ορισμένοι συχνοί κίνδυνοι για την ασφάλεια, που προκύπτουν από κυβερνοεπιθέσεις, τους λόγους και τις αιτίες που αυτές οι επιθέσεις είναι αποτελεσματικές καθώς και τις επιδιωκόμενες λύσεις (Khan et al., 2022).

### *4.3.1 Ζητήματα που σχετίζονται με την αποθήκευση των δεδομένων*

Ο παρακάτω Πίνακας εστιάζει στο θέμα της **αποθήκευσης δεδομένων**. Να σημειωθεί ότι οι διαθέσιμες τεχνικές σχετικά με αυτό το θέμα είναι ικανοποιητικές, ωστόσο απαιτούνται ολοένα και πιο αποτελεσματικά μέτρα ασφαλείας για την κάλυψη των μελλοντικών απαιτήσεων (Khan et al., 2022).

| Πρόβλημα | Αιτία | Επιπτώσεις | Τρέχων Αμυντικός Μηχανισμός | Επιδιωκόμενη Λύση |
|---|---|---|---|---|
| **Απομόνωση των δεδομένων αποθήκευσης και δυνατότητα ελέγχου της πηγής αποθήκευσης.** | Έλλειψη σωστής διαχείρισης της αποθήκευσης των δεδομένων. | Απώλεια δεδομένων, παραβίαση της ασφάλειας των δεδομένων και παραβίαση των ίδιων των δεδομένων. | Ικανοποιητικός. | Καλύτεροι και πιο αποτελεσματικοί μηχανισμοί όσον αφορά στην ασφάλεια των δεδομένων.<br>Τα πρωτόκολλα *Harm Cloud* θα πρέπει να εγγυώνται την ασφάλεια των δεδομένων κατά την αποθήκευση, τη διαγραφή και τη ανάκτησή τους. |

***Πίνακας 2**: Ζήτημα αποθήκευσης δεδομένων*

### *4.3.2 Ζητήματα που σχετίζονται με την επεξεργασία των δεδομένων*

Ο επόμενος Πίνακας εστιάζει σε **αναξιόπιστους υπολογισμούς και επεξεργασία δεδομένων** (Khan et al., 2022).

***Πίνακας 3**: Μη αξιόπιστος υπολογισμός*

| Πρόβλημα | Αιτία | Επιπτώσεις | Τρέχων Αμυντικός Μηχανισμός | Επιδιωκόμενη Λύση |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Κακόβουλος καταναλωτής, μη έγκυροι υπολογισμοί, λανθασμένη θέση εκκίνησης σε αντίγραφα ασφαλείας, προβλήματα μετακίνησης και επαναφοράς.** | Συμφωνίες επιπέδου ασφαλείας με μη αξιόπιστα μέρη, έλλειψη ελαστικότητας στο πλαίσιο ασφαλείας. Ανεκπαίδευτη και ανειδίκευτη επίβλεψη της ασφάλειας. | Διαρροές, απώλεια, παραβίαση και καταστροφή δεδομένων. | Χαμηλό επίπεδο ασφαλείας. | Μια μη διαδραστική χαμηλού κόστους λύση για την διασφάλιση πρωτίστως των χρηματοοικονομικών και των δεδομένων υγείας στο *cloud*. |

### *4.3.1 Ζητήματα που σχετίζονται με τα σφάλματα υλικού*

Τα κρίσιμα ζητήματα που αναφέρονται στον παρακάτω Πίνακα περιλαμβάνουν την **προσβασιμότητα των δεδομένων και τα σφάλματα υλικού** (Khanetal., 2022).

***Πίνακας 4**: Διαθεσιμότητα δεδομένων και υπηρεσιών*

| **Πρόβλημα** | **Αιτία** | **Επιπτώσεις** | **Τρέχων Αμυντικός Μηχανισμός** | **Επιδιωκόμενη Λύση** |
|---|---|---|---|---|
| **Χρήση ψεύτικων πόρων και διακοπή των υπηρεσιών του νέφους. Προσβασιμότητα υλικού συμπερι-λαμβανομένων των σφαλμάτων υλικού.** | Τρωτά σημεία κατά την αποθήκευση. Μεγάλος όγκος αποθηκευμένων δεδομένων, Κακή διαχείριση των δεδομένων. | Επιθέσεις *DoS*. Τεράστιοι χρόνοι απόκρισης. | Ικανοποιητικός. | Σωστή προσέγγιση για την κάθε υπηρεσία και τη διαθεσιμότητα των δεδομένων. Μέγιστη επανακρυπτογράφηση, εφαρμόζοντας κατάλληλους μηχανισμούς, σε συνδυασμό με τα πιο πρόσφατα εργαλεία/μοντέλα ασφαλείας. |

### *4.3.1 Ζητήματα που σχετίζονται με κενά στους αμυντικούς μηχανισμούς*

Ο παρακάτω Πίνακας επικεντρώνεται στα ζητήματα τα οποία αντιμετωπίζονται ανεπαρκώς από τους **αμυντικούς μηχανισμούς της ασφάλειας** του *cloud*. Αυτά αναφέρονται ως ερευνητικά κενά ή προβλήματα (Khan et al., 2022).

***Πίνακας 5**: Γενικά Θέματα*

| **Πρόβλημα** | **Αιτία** | **Επιπτώσεις** | **Τρέχων Αμυντικός Μηχανισμός** | **Επιδιωκόμενη Λύση** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Ανεπαρκής κρυπτογράφηση.** | Κακή επιλογή αλγορίθμων. | *Hacking* δικτύου. | Ικανοποιητικός. | Τεχνικές κρυπτογραφίας υψηλών προδιαγραφών. |
| **Ανακύκλωση δεδομένων *cloud*.** | Λανθασμένη χρήση λογισμικού. | Μη αξιόπιστα περιβάλλοντα και τεχνολογίες. | Έξοχος. | Ασφαλής και σωστή διαγραφή δεδομένων. |
| **Κακόβουλο λογισμικό.** | Προγράμματα προστασίας από ιούς. | Επιθέσεις κακόβουλου λογισμικού. | Ανεπαρκής. | Σύστημα ανίχνευσης κακόβουλου λογισμικού. |
| **Διαχείριση εικονικών μηχανών (*VMs*).** | Το σύστημα επιβαρύνεται λόγω του μεγάλου πλήθους των εικονικών μηχανών. | Απώλεια δεδομένων κατά τη μετε-γκατάσταση των VMs και επιβλαβής εισαγωγή κώδικα. | Έξοχος | Απαιτείται πιο αποτελεσματικό σύστημα ώστε να καλυφθούν οι μελλοντικές ανάγκες. |
| **Εικονικοποίηση δικτύου.** | Έλλειψη τυπικών τεχνικών απορρήτου και ασφάλειας. | Μη αναγνωρι-σμένη και μη αξιόπιστη εικονικοποίη ση δικτύου. | Ανεπαρκής | Δημιουργία νέου σχήματος ασφαλείας για την εξασφάλιση της εικονικοποίησης του δικτύου. |
| **Κινητές πλατφόρμες.** | Η χρήση φορητών συσκευών και φορητών εφαρμογών είναι αρκετά περίπλοκη | *Hacking* των *Mobile IPs'*. | Ανεπαρκής | Απαιτούμενο σύστημα ασφαλείας κρυπτογράφησης για κινητά. |

## 4.4Επίπεδα επιθέσεων στο υπολογιστικό νέφος

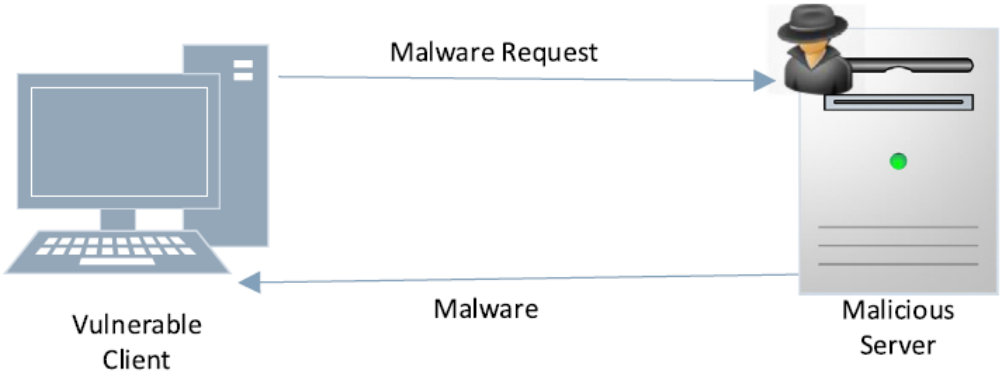
Οι επιθέσεις στο υπολογιστικό νέφος δύνανται να λαμβάνουν χώρα σε διάφορα επίπεδα. Έτσι, ανάλογα με αυτό το κριτήριο κατηγοριοποιούνται σε επιθέσεις μεταξύ εικονικών μηχανημάτων (*VM-to-VM attacks*), επιθέσεις μεταξύ πελατών (*Client-to-Client attacks*)και επιθέσεις μεταξύ φιλοξενούμενων (*Guest-to-guest attacks*). Πιο αναλυτικά στοιχεία για κάθε επίπεδο επίθεσης παρατίθενται στις επόμενες παραγράφους (Iqbal et al., 2016):

### *4.4.1 Επιθέσεις εικονικών μηχανημάτων (VM-to-VM attacks)*

Οι εικονικές μηχανές θεωρούνται κοντέινερ (απομονωμένα κιβώτια) που φιλοξενούν λειτουργικά συστήματα, προγράμματα και εφαρμογές. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους δημιουργούν ένα περιβάλλον πολλαπλών μισθώσεων με τη βοήθεια των υπερπιστωτών. Υπερεπόπτες που βασίζονται στην τεχνολογία εικονοποίησης, όπως οι *VMware vSphere*, *Microsoft Virtual PC*, *Xen* κ.λπ. χρησιμοποιούνται από το υπολογιστικό νέφος για την κατάτμηση και τον διαμοιρασμό των φυσικών μηχανημάτων σε εικονικές μηχανές. Τα περιβάλλοντα που δημιουργούνται είναι δυνητικά ευάλωτα μιας και συμβαίνουν επιθέσεις ως αποτέλεσμα των ελαττωμάτων αυτών των τεχνολογιών (Iqbal et al., 2016; Sabahi, 2011).

### *4.4.2. Επιθέσεις από πελάτη σε πελάτη (Client-to-client attacks)*

Εκμεταλλευόμενοι ελαττώματα που εκτελούνται σε έναν διακομιστή, οι πελάτες μπορούν να εξαπολύσουν επιθέσεις στους υπολογιστές άλλων πελατών. Ένα μολυσμένο εικονικό μηχάνημα μπορεί να μολύνει όλα τα άλλα *VMs* που λειτουργούν στο ίδιο φυσικό μηχάνημα - διακομιστή όπως απεικονίζεται στην παρακάτω εικόνα:

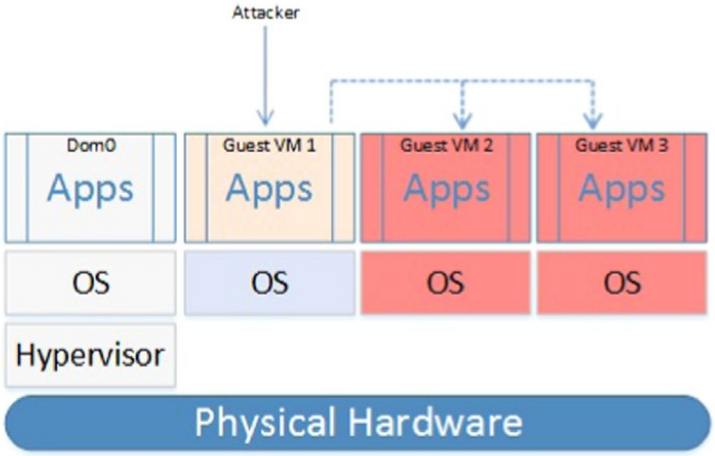



***Εικόνα10:****Επιθέσεις μεταξύ πελατών (Client-to-client attacks)*
**Πηγή**: Iqbal et al., 2016

Εδώ, η επίθεση ξεκινά από την εικονική μηχανή ενός πελάτη και εξαπλώνεται σε άλλους που στεγάζονται στον ίδιο φυσικό υπολογιστή. Εξαιτίας αυτού, ολόκληρο το περιβάλλον εικονικοποίησης μπορεί να τεθεί σε κίνδυνο, επιτρέποντας στους εχθρικούς πελάτες να αποκτήσουν πρόσβαση στα δικαιώματα διαχειριστή του εικονικού περιβάλλοντος και σε όλα τα *VMs*, διαφεύγοντας τον υπερεπόπτη. Υπό το πρίσμα αυτό, οι «επιθέσεις πελάτη σε πελάτη» αποτελούν σοβαρή απειλή για την ασφάλεια του εικονικού συστήματος (Iqbal et al., 2016; Sabahi, 2011).

### *4.4.3. Επιθέσεις μεταξύ επισκεπτών / φιλοξενούμενων (Guest-to-guest attacks)*

Η προστασία του περιβάλλοντος φιλοξενίας των εικονικών μηχανών από δυνητικές επιθέσεις είναι ζωτικής σημασίας, διότι εάν ένας εισβολέας είναι σε θέση να αποκτήσει πρόσβαση στο υλικό διαχείρισης, είναι σχεδόν βέβαιο ότι θα έχει πρόσβαση σε όλες τις εικονικές μηχανές που φιλοξενούνται σε αυτό. Οι επιθέσεις τέτοιου τύπου ονομάζονται επιθέσεις μεταξύ επισκεπτών / φιλοξενούμενων και έχουν παρόμοιες επιπτώσεις με την επίθεση μεταξύ των εικονικών μηχανημάτων. Στην παρακάτω εικόνα απεικονίζονται οι δυο αυτές κατηγορίες επιθέσεων:




***Εικόνα 11**: Επιθέσεις μεταξύ εικονικών μηχανών (VM-to-VM attacks) και μεταξύ φιλοξενούμενων (Guest-to-guest attacks)*

**Πηγή**: Iqbaletal., 2016

Επειδή το υποκείμενο σύστημα ασφαλείας έχει παραβιαστεί, οι εισβολείς μπορούν να μετακινούνται μεταξύ πολλών εικονικών μηχανών (Iqbal et al., 2016; Reuben, 2007).

## 4.5. Επιφάνεια επιθέσεων ανά μοντέλο διάθεσης

Ένας επιτιθέμενος ή μη εξουσιοδοτημένος χρήστης μπορεί να επιχειρήσει να διεισδύσει σε ένα σύστημα μέσω οποιουδήποτε σημείου στην επιφάνεια επίθεσης του περιβάλλοντος λογισμικού και να βλάψει το περιβάλλον. Η κοινή χρήση πόρων είναι ένα από τα πιο σημαντικά προβλήματα σε ένα σύστημα *cloud* πολλαπλών ενοικιαστών, καθώς όπως έχει γίνει κατανοητό με όσα έχουν προαναφερθεί, στο υπολογιστικό νέφος ανοίγονται νέοι δρόμοι επίθεσης(Iqbal et al., 2016).

Θα πρέπει να σημειωθεί ότι η πράξη και η θεωρία διαφέρουν μεταξύ τους. Κατ' αρχήν, οι μεγάλοι υπερεπόπτες μπορεί να φαίνεται ότι έχουν λίγα διανύσματα επιφανειακής επίθεσης, ωστόσο υπάρχει ένας αυξανόμενος αριθμός πραγματικών επιθέσεων που στοχεύουν σε

αυτούς, όπως η χρήση *rootkit*[5] και τα πλευρικά κανάλια. Ως εκ τούτου, η εικονικοποίηση καθίσταται ως μια νέα επιφάνεια επίθεσης. Οι πληροφορίες που ανατίθενται σε εξωτερικούς συνεργάτες στο cloud είναι πιθανό να διαρρεύσουν από έναν υπερεπόπτη που εκμεταλλεύεται μια επίθεση πλευρικού καναλιού. Σε ένα εικονικοποιημένο περιβάλλον, οι παραβιασμένοι υπερεπόπτες μπορούν να χρησιμεύσουν ως πρόσθετοι φορείς επίθεσης(Iqbal et al., 2016).

Ο εντοπισμός της επιφάνειας επίθεσης που είναι ευάλωτη σε απειλές ασφαλείας είναι ζωτικής σημασίας (Scarfone, 2011) για την κατανόηση της επίθεσης και τη λήψη μέτρων για την αποφυγή της. Οι βασικοί στόχοι μπορούν να κατηγοριοποιηθούν ως εξής ανάλογα με τον τύπο διάθεσης του υπολογιστικού νέφους (Iqbal et al., 2016):

- Στο μοντέλο *SaaS*: Το πρόγραμμα περιήγησης Ιστού.
- Στο μοντέλο *PaaS*: Οι υπηρεσίες Ιστού και ταAPI: πρωτόκολλα*SOAP* (*Simple Object Access Protocol*), *REST*(*Representational State Transfer*) και*RPC* (*Remote Procedure Call*).
- Στο μοντέλο *IaaS*:Τα*VMs* και οι υπηρεσίες αποθήκευσης: *VPN* (*Virtual Private Network*) και *FTP* (*File Transfer Protocol*).

Συνοπτικά στον παρακάτω πίνακα παρατίθενται οι εν δυνάμει επιφάνειες επίθεσης ανά μοντέλο διάθεσης(Turnbull&Shropshire, 2013):

***Πίνακας 6****: Επιφάνειες επίθεσης ανά μοντέλο διάθεσης*

| **Attack surface** (Επιφάνεια επίθεσης) | **Attack Vectors** (Επιτιθέμενο μοντέλο διάθεσης) | | |
|---|---|---|---|
| | **SaaS** | **PaaS** | **IaaS** |
| **Application level** (Επίπεδο εφαρμογών) | Input/output validation | Runtime engine that runs customer's applications | Virtual workgroups |
| **Data Segregation** (Διαχωρισμός δεδομένων) | Unauthorized Access of Data | Data Service Portal | Multi-Tenancy and Isolation |
| **Data Availability** (Διαθεσιμότητα δεδομένων) | Hosted Virtual Server | Network traffic | Virtual Network |
| **Secure Data Access** (Ασφάλεια πρόσβασης δεδομένων) | Encryption/ Decryption Keys | Third Party Components | Cloud Multi-tenant Architecture |

[5]Ενα *rootkit* είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών. Ο όρος *rootkit* είναι μια συνένωση των λέξεων «*root*» (το παραδοσιακό όνομα του προνομιούχου λογαριασμού σε λειτουργικά συστήματα τύπου *Unix*) και της λέξης «*kit*» (Πηγή: https://el.wikipedia.org/wiki/Rootkit).

| | | | |
|---|---|---|---|
| **Data Center Security** (Ασφάλεια κέντρου δεδομένων) | Server based Data Breaches | Datacenter Vulnerabilities | Virtual Domain Environments |
| **Authentication/Authorization**(Αυθεντικοποίηση / Εξουσιοδότηση) | ID and Password | Client API Password Reset Attack | Poor Quality Credentials |

Στις επόμενες παράγραφοι αναλύονται διεξοδικά τα όσα συνοπτικά αναφέρονται στον παραπάνω πίνακα.

### *4.5.1. Επιφάνεια επίθεσης στο SaaS μοντέλο διάθεσης*

Στο υπολογιστικό νέφος, οι εφαρμογές Ιστού αναφέρονται ως λογισμικό και είναι ένας τύπος υπηρεσίας. Αυτές οι δυναμικές υπηρεσίες χρησιμοποιούν μια κατανεμημένη αρχιτεκτονική *cloud* για τη συλλογή πληροφοριών από πολλές πηγές. Λόγω αυτής της λειτουργικότητας, το περιεχόμενο της ιστοσελίδας μπορεί περιστασιακά να δεχθεί επίθεση από χάκερ χρησιμοποιώντας ένα σενάριο με τη μορφή *script* (*Scale of Children's Readiness in Printing*). Αυτά τα σενάρια παράγουν την ανεπιθύμητη συμπεριφορά όταν εκτελούνται στο πρόγραμμα περιήγησης (Iqbal et al., 2016).

### *4.5.2. Επιφάνεια επίθεσης στο PaaS μοντέλο διάθεσης*

Η ασφάλεια είναι το πιο κρίσιμο συστατικό των υπηρεσιών *PaaS*, καθώς σε αυτό το μοντέλο παρέχεται στους πελάτες του υπολογιστικού νέφους το περιβάλλον εκτέλεσης λογισμικού χωρίς να χρειάζεται να αγοράζουν διακομιστές, αποθηκευτικό χώρο ή δίκτυα. Οι προμηθευτές *PaaS* πρέπει να χρησιμοποιούν ισχυρές μεθόδους κρυπτογράφησης εάν θέλουν να συνεχίσουν να προσφέρουν αδιάλειπτες υπηρεσίες στους πελάτες τους. Είναι καθήκον τους να προστατεύουν τις μηχανές του χρόνου εκτέλεσης από τους κυβερνοεγκληματίες που στοχεύουν στις εφαρμογές των πελατών τους. Θα πρέπει, επίσης, να παρέχουν στους πελάτες τους τα εργαλεία προγραμματισμού που να προστατεύουν τις εφαρμογές που αναπτύσσουν από επιβλαβείς επιθέσεις. Σε αυτό το μοντέλο η πολυμίσθωση είναι ένας σημαντικός φορέας επίθεσης μιας και πέραν του μεγάλου πλήθους των πελατών υποστηρίζει λειτουργικότητες σε πολλές και διαφορετικές πλατφόρμες, είτε όσον αφορά στα λειτουργικά συστήματα είτε στις εικονικές μηχανές. Πολλοί χρήστες μπορούν να έχουν πρόσβαση σε υπηρεσίες *cloud* ταυτόχρονα, η οποία δίνει στους κακόβουλους χρήστες πολλές ευκαιρίες να παρεμβαίνουν και να διαταράσσουν την τακτική λειτουργία των κοντέινερ (Iqbal et al., 2016).

### *4.5.3. Επιφάνεια επίθεσης στο IaaS μοντέλο διάθεσης*

Ο υπερεπόπτης, γνωστός και ως οθόνη εικονικής μηχανής, είναι ένα επιπλέον επίπεδο μεταξύ του λειτουργικού συστήματος και του υλικού στις τεχνολογίες εικονικοποίησης. Το *IaaS*

χρησιμοποιεί αυτήν την τεχνολογία για να δημιουργήσει και να ενεργοποιήσει τις εικονποιημένες υπηρεσίες. Οι υπερπιστωτές χρησιμοποιούνται για αυτή την ανάπτυξη *APIs*που αφορούν σε διοικητικές εργασίες. Μια διευρυμένη επιφάνεια επίθεσης προκύπτει από την παρουσία των *hypervisors*. Αυτό συμβαίνει επειδή υπάρχουν πολλές διαφορετικές τεχνικές που μπορούν να χρησιμοποιηθούν, συμπεριλαμβανομένων των *APIs*, των socket συνδέσμων των καναλιών και άλλων αντικειμένων δεδομένων όπως οι συμβολοσειρές εισόδου (Iqbal et al., 2016;Szeferetal., 2011).

# 5. ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ

Στο παρόν κεφάλαιο εντοπίζονται και αναλύονται οι διάφοροι πιθανοί τύποι επιθέσεων στο *cloud* και πώς αυτοί μπορούν να επηρεάσουν τις υπηρεσίες του υπολογιστικού νέφους. Η ταξινόμηση έγινε βάσει των μοντέλων διάθεσης. Σε ένα περιβάλλον υπολογιστικού νέφους, υπάρχει ένας αριθμός πιθανών κινδύνων που έχουν αναγνωριστεί από το *Cloud SecurityAlliance*[6](*CSA*) και την *Gartner*[7]. Η πληθώρα των διαφορετικών επιθέσεων ανά μοντέλο διάθεσης καθώς και οι διαφορετικές επιφάνειες όσον αφορά τις επιθέσεις απαιτούν την κατάρτιση μιας ολοκληρωμένης μελέτης και τη σύνταξη μιας αναλυτικής στρατηγικής όσον αφορά στην ασφάλεια και στις σχετικές ρυθμίσεις του υπολογιστικού νέφους (Iqbal et al., 2016).

## 5.1 Επιθέσεις που στοχεύουν στο SaaS μοντέλο διάθεσης

Το *SaaS* μοντέλο του υπολογιστικού νέφους και οι διαδικτυακές υπηρεσίες μοιράζονται πολλά κοινά ζητήματα ασφάλειας. Για να διασφαλιστεί το απόρρητο και η ασφάλεια, τα δεδομένα που έχουν ανατεθεί σε εξωτερικούς συνεργάτες ενδέχεται να είναι κρυπτογραφημένα. Ζητήματα ασφάλειας που σχετίζονται με τα δεδομένα, όπως το: ποιος κατέχει τα δεδομένα, η δημιουργία αντιγράφων ασφαλείας, η πρόσβαση των δεδομένων, η τοποθεσία των δεδομένων, η διαθεσιμότητά τους, η διαχείριση και ο έλεγχος της ταυτότητας, αποτελούν, μεταξύ άλλων, πιθανές προκλήσεις σε αυτό το μοντέλο παροχής υπηρεσιών. Οι παραβιάσεις ασφαλείας προκαλούνται επίσης ακόμη και από ενέργειες αξιόπιστων χρηστών (Iqbal et al., 2016).

### *5.1.1 Επίθεση άρνησης υπηρεσίας (Denial of Service Attacks)*

*5.1.1.1 Περιγραφή επίθεσης*

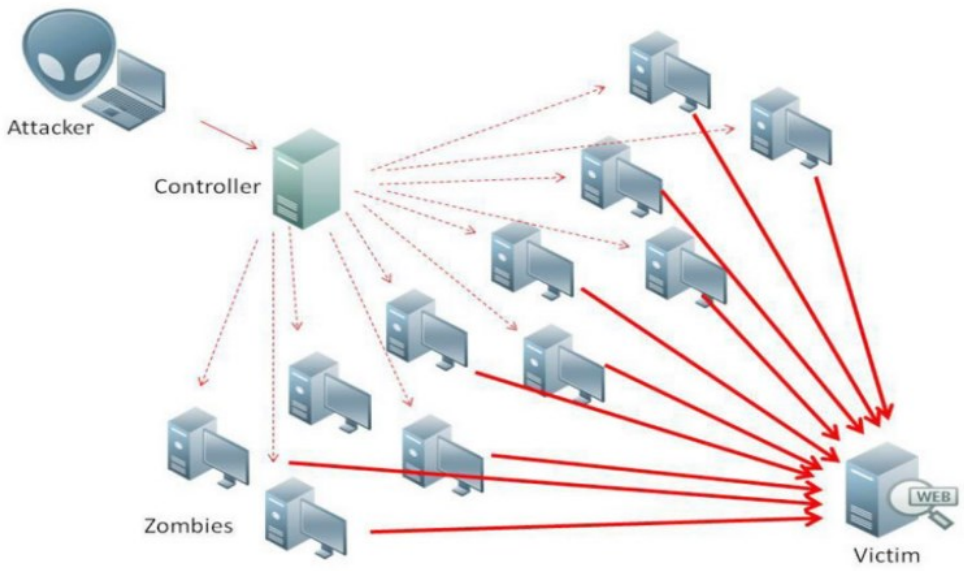
Οι επιθέσεις άρνησης υπηρεσίας (*DoS: Denial of Service Attacks*), ιδίως εκείνες που βασίζονται σε πρωτόκολλα*HTTP*, *XML*(*Extensible Markup Language*) και *REST* ,ευθύνονται για την πλειονότητα των σοβαρών κακόβουλων επιθέσεων στο υπολογιστικό νέφος. Ένας εισβολέας που χρησιμοποιεί μια *DoS* επίθεση σε μια κοινόχρηστη υποδομή θα καταναλώσει κάθε φυσικό πόρο που είναι διαθέσιμος στο φυσικό μηχάνημα. Με αυτό τον τρόπο ο διακομιστής δεν είναι σε θέση να καλύψει τις απαιτήσεις πόρων για τις υπόλοιπες εικονικές μηχανές (Sureshkumar&Baranidharan, 2021). Η επίθεση αυτή επιτυγχάνεται με την αποστολή

[6]Η *Cloud SecurityA lliance* είναι ένας μη κερδοσκοπικός οργανισμός με αποστολή να «προωθεί τη χρήση βέλτιστων πρακτικών για την παροχή διασφάλισης ασφάλειας στο *cloud computing* και να παρέχει εκπαίδευση σχετικά με τις χρήσεις του για να βοηθήσει στην ασφάλεια όλων των άλλων μορφών υπολογιστών (Πηγή: https://en.wikipedia.org/wiki/Cloud_Security_Alliance).

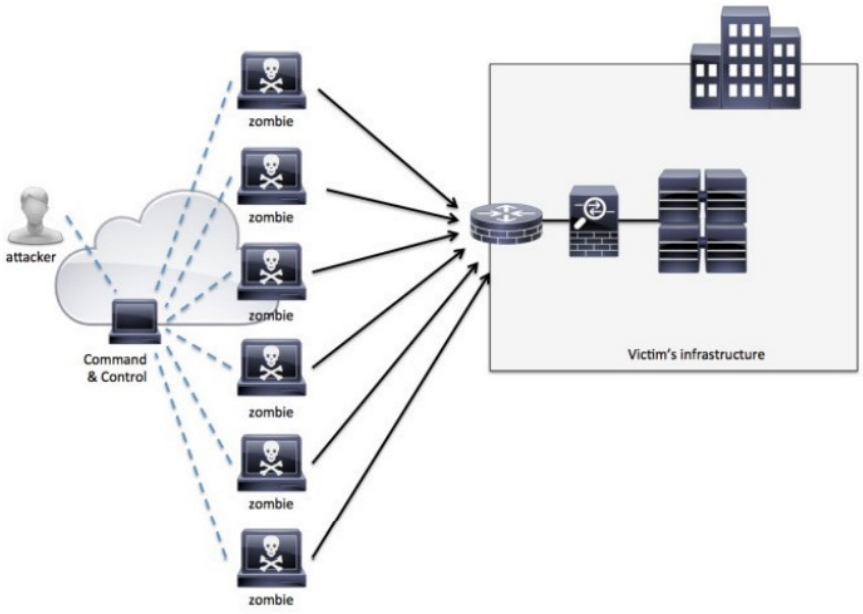
[7] Η *GartnerInc*. είναι μια εταιρεία τεχνολογικής έρευνας και συμβούλων με έδρα το Στάνφορντ του Κονέκτικατ που διεξάγει έρευνα για την τεχνολογία και μοιράζεται αυτήν την έρευνα τόσο μέσω ιδιωτικών συμβουλών όσο και μέσω προγραμμάτων εκτελεστικών στελεχών και συνεδρίων (Πηγή: https://en.wikipedia.org/wiki/Gartner).

πλήθους αιτημάτων σε μια εφαρμογή Ιστού ή σε μια υπηρεσία προκειμένου να διαταραχθεί η κανονική λειτουργία της υποκείμενης μηχανής (μηχανής που φιλοξενεί την εφαρμογή ή την υπηρεσία).Οι χρήστες του νέφους ξεκινούν τα ερωτήματά τους σε *XML*, τα υποβάλλουν μέσω *HTTP* και συχνά αναπτύσσουν τη διεπαφή του συστήματός τους χρησιμοποιώντας πρωτόκολλα τύπου *REST*, όπως αυτά που βρίσκονται στο *Microsoft Azure* και στο *Amazon EC2*(Khalil et al., 2014).

Οι επιθέσεις *DoS* είναι απλούστερες στην εκτέλεση και είναι εξαιρετικά δύσκολο για τους ειδικούς ασφαλείας να τις αντικρούσουν αποτελεσματικά, εξαιτίας των ελαττωμάτων στις διεπαφές των συστημάτων. Λόγω της ευρείας χρήσης τόσο της *XML markup* γλώσσας όσο και του *HTTP* πρωτοκόλλου στο υπολογιστικό νέφος καθώς και της έλλειψης αποτελεσματικών τεχνικών αποτροπής, αυτά τα πρωτόκολλα είναι πιο ευάλωτα σε κατανεμημένες επιθέσεις άρνησης υπηρεσίας (*DDoS: Distributed Denial of Service*) από ότι στο κλασικό DoS. Οι επιθέσεις αυτές ονομάζονται αντίστοιχα *XML-based DDoS* και *HTTP-based DDoS*(Khalil et al, 2014).




***Εικόνα 12**:Επίθεση άρνησης υπηρεσίας (DoS)*
**Πηγή**: Dey&Sen, 2017




***Εικόνα 13**:Κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS)*
**Πηγή**: Dey&Sen, 2017

Η ασφάλεια αυτών των οντοτήτων είναι απαραίτητη για τη διασφάλιση της υγιούς ανάπτυξης μιας πλατφόρμας *cloud*, καθώς το *HTTP* και το *XML* είναι βασικά, δομικά στοιχεία του υπολογιστικού νέφους(Khalil et al., 2014).

*5.1.1.2 Αντίμετρα*

Πέντε φίλτρα συνθέτουν το πλαίσιο που ονομάζεται «σύννεφο υπεράσπισης» και που προσφέρουν οι Karnwal et al. στη μελέτη τους το 2012(Khalil et al, 2014):

1. **Το φίλτρο αισθητήρα**: Παρακολουθεί τα εισερχόμενα μηνύματα αιτήματος και επισημαίνει ένα μήνυμα ως ύποπτο εάν παρατηρηθεί μια πλασματική αύξηση στον αριθμό των μηνυμάτων που προέρχονται από έναν μόνο ή από κάποιον συγκεκριμένο πελάτη.
2. **Το φίλτρο καταμέτρησης κόμβων**: Αυτό το φίλτρο μετρά τον αριθμό των αναπηδήσεων που χρειάζεται ένα μήνυμα για να φτάσει από την αρχική πηγή στον προορισμό του και συγκρίνει αυτόν τον αριθμό με έναν προκαθορισμένο αριθμό αναπήδησης. Εάν ανακαλυφθεί μια ασυμφωνία κατά τη δρομολόγηση, το φίλτρο επισημαίνει το μήνυμα το ως ύποπτο.
3. **Το φίλτρο απόκλισης συχνότητας *IP***: Όταν οι επικοινωνίες συμβαίνουν με την ίδια ακριβώς συχνότητα, ένα μήνυμα επισημαίνεται ως ύποπτο.

4. **Το φίλτρο διπλής υπογραφής**: Το φίλτρο αυτό προσθέτει δύο υπογραφές σε ένα *XML* έγγραφο, μία στην κεφαλίδα και μία στο υποσέλιδο. Και οι δύο υπογραφές θα πρέπει να επικυρωθούν σε περίπτωση επίθεσης.
5. **Το φίλτρο επίλυσης παζλ**: Το φίλτρο αυτό απαιτεί οι απαντήσεις να περιλαμβάνονται σε μια *SOAP* κεφαλίδα. Σε περίπτωση *HTTP DDoS* επίθεσης, το «σύννεφο υπεράσπισης» θα στείλει πίσω στην *IP*, από την οποία λαμβάνει μηνύματα, το παζλ που εμπεριέχεται στην κεφαλίδα. Τα αιτήματα θεωρούνται γνήσια εάν ληφθεί πίσω το ολοκληρωμένο παζλ, διαφορετικά, ταξινομούνται ως επιθέσεις *HTTP DDoS*.

Τα πρώτα τέσσερα φίλτρα αναγνωρίζουν επιθέσεις *DDoS* χρησιμοποιώντας *HTTP* πρωτόκολλο και το πέμπτο φίλτρο αναγνωρίζει επιθέσεις που βασίζονται στην *XML* γλώσσα. Οι επιθέσεις που βασίζονται σε *REST* πρωτόκολλο εντοπίζονται αλλά δεν παρέχεται μηχανισμός για να τις αποτρέψει. Μία από τις βασικές αιτίες είναι η στενή σχέση μεταξύ των επιθέσεων που βασίζονται σε *REST* και της δομής των διεπαφών χρήστη, οι οποίες μπορεί να κυμαίνονται από προγράμματα που αναφέρονται στο επίπεδο του χρήστη έως προγράμματα που προορίζονται για συστήματα. Δεν υπάρχει μια αυστηρή οδηγία για τον τρόπο εφαρμογής των μέτρων ασφαλείας σε επίπεδο διεπαφής, επειδή οι εφαρμογές και τα συστήματα διαφέρουν όλα ως προς τον τύπο και εξυπηρετούν στην πραγματικότητα διαφορετικές ανάγκες των τελικών πελατών (Khalil et al., 2014).

Το πρόβλημα σε αυτό το πλαίσιο είναι ότι στερείται πρακτικής επικύρωσης και βασίζεται στην υπόθεση ότι ο αριθμός των μονάδων στο σύστημα είναι ευθέως ανάλογος με τον αριθμό των αναμενόμενων επιθέσεων. Επιπλέον, η εξαντλητική παρακολούθηση των μηνυμάτων σε κάθε κόμβο επιβραδύνει σημαντικά την κίνηση του δικτύου. Τέλος, το πλαίσιο δεν διαθέτει τους κατάλληλους μηχανισμούς για τον συντονισμό των κόμβων σε περίπτωση ανίχνευσης περιστατικών επίθεσης(Khalil et al., 2014).

Οι Riquet et al. (2012) ισχυρίζονται ότι δεν υπάρχει διαθέσιμη ισχυρή λύση για την πρόληψη των επιθέσεων *DDoS*. Για να επικυρώσουν τον ισχυρισμό τους, οι συγγραφείς διεξήγαγαν ένα πείραμα για να αξιολογήσουν την αποτελεσματικότητα των πραγματικών λύσεων ασφαλείας έναντι των κατανεμημένων επιθέσεων. Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι η αποτυχία των συστημάτων ασφαλείας έγκειται σε δύο πτυχές: είτε η λύση ασφαλείας μπορεί να είναι ήδη ξεπερασμένη επειδή δεν έχει ενημερωθεί, είτε η λύση μπορεί να βασίζεται σε ακατάλληλες μεθόδους. Να σημειωθεί ότι οι ίδιοι δεν πρότειναν καμία λύση που να μπορεί να αποτρέψει τις κατανεμημένες επιθέσεις άρνησης υπηρεσίας(Khalil et al., 2014).

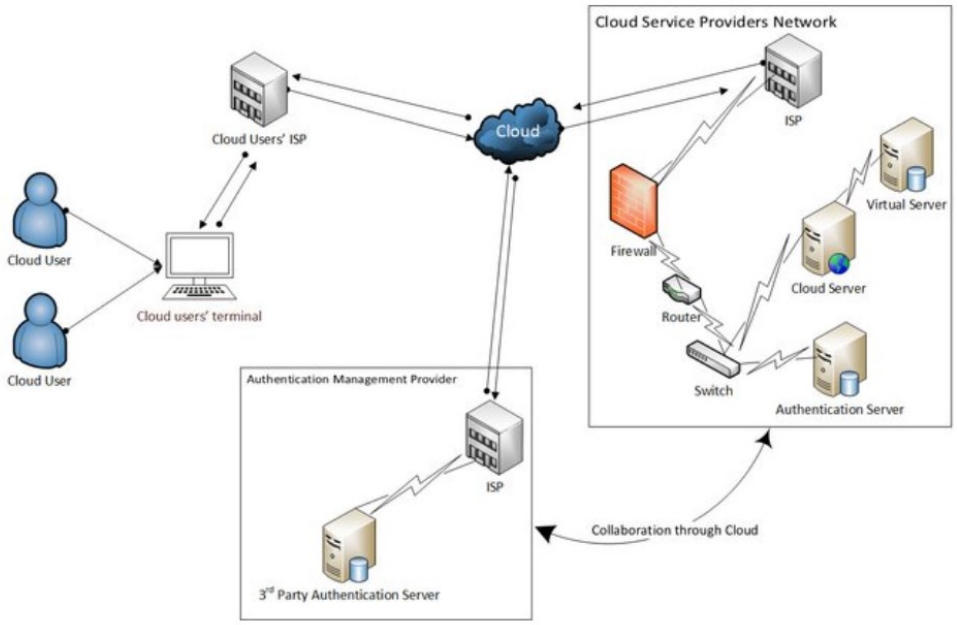
Άλλα ευρέως χρησιμοποιούμενα αντίμετρα *DDoS* είναι τα τείχη προστασίας. Ωστόσο, λόγω της θέσης ενός τείχους προστασίας (στα όρια του δικτύου), αυτό δεν είναι σε θέση να ανιχνεύσει τις κατανεμημένες επιθέσεις εντός του δικτύου(Khalil et al., 2014).

### *5.1.2 Επίθεση αυθεντικοποίησης (AuthenticationAttack)*

*5.1.2.1 Περιγραφή επίθεσης*

Η Πολιτική Ασφάλειας Περιεχομένου (*CSP: Content Security Policy*), που είναι ένα πρότυπο για την ασφάλεια των υπολογιστικών συστημάτων επιβάλλει ότι ο έλεγχος ταυτότητας είναι απαραίτητος τόσο για τους χρήστες των απλών εφαρμογών και των συστημάτων, όσο και για τους χρήστες του υπολογιστικού νέφους. Σύμφωνα με τις πολιτικές των *CC* παρόχων, ο κύριος στόχος του ελέγχου ταυτότητας είναι να περιοριστεί η πρόσβαση στα σύστημα επεξεργασίας των δεδομένων μόνο σε όσους επιτρέπεται. Οι εισβολείς, συχνά στοχεύουν στους μηχανισμούς και τις διαδικασίες ελέγχου ταυτότητας ενός συστήματος (Iqbal et al., 2016).

Στην παρακάτω εικόνα παρουσιάζεται η κατάσταση ελέγχου ταυτότητας για εφαρμογές που βασίζονται στο *cloud*:




***Εικόνα14****:Έλεγχος ταυτότητας χρήστη για μια υποδομή που βασίζεται στο υπολογιστικό νέφος*
**Πηγή**:Ahmed&Hossain, 2014

Όταν ο χρήστης ζητά πληροφορίες από έναν πάροχο *SaaS*, θα πρέπει πρωτίστως να γίνει η επαλήθευση της ταυτότητάς του. Δεδομένου ότι η πλατφόρμα *SaaS* βασίζεται στον Ιστό, κάποιος τύπος κρυπτογράφησης πρέπει να περιλαμβάνεται είτε στη διεύθυνση *URL* είτε σε ένα *cookie*. Έπειτα, τα δεδομένα επαληθεύονται έναντι του καταλόγου των χρηστών – πελατών χρησιμοποιώντας μια απευθείας κλήση υπηρεσίας *web*, σε έναν εξυπηρετητή

αυθεντικοποίησης (*authentication server*). Αυτός απαντά, μετά τον έλεγχο της ταυτότητας, και εφόσον το αίτημα εγκριθεί, εφόσον δηλαδή επαληθευτούν τα στοιχεία της ταυτότητας του χρήστη – πελάτη, με κάποιο είδος εξουσιοδότησης.

Πρέπει να αναφερθεί ότι η ταυτότητα είναι το βασικό συστατικό οποιουδήποτε εικονικού συστήματος στο *cloud*. Για να αποκτήσει πρόσβαση ένας χρήστης σε ένα σύστημα, μια υπηρεσία, έναν διακομιστή ή άλλους πόρους του υπολογιστικού νέφους θα πρέπει να αναγνωριστεί από την πλατφόρμα. Τα διαθέσιμα δεδομένα, οι πληροφορίες και οι υπηρεσίες συνδέονται με μια συγκεκριμένη οντότητα. Ένα ενοποιημένο σύνολο λύσεων διαχείρισης ταυτότητας θα πρέπει να παρέχεται από τους παρόχους υπολογιστικού νέφους. Τα τρέχοντα πρότυπα, όπως τα *SPML*(*Services Provisioning Markup Language*), *SAML*(*Security Assertion Markup Language*), *OAuth*(*Open Authorization*) και *XACML*(*Extensible Access Control Markup Language*), χρησιμοποιούνται για την προστασία των ταυτοτήτων μεταξύ των διαφόρων τομέων και των πλατφορμών στο σύννεφο καθώς και μεταξύ των διαφόρων οντοτήτων (Bouayad et al., 2012).

Σε μια επιτυχημένη παραβίαση, που έλαβε χώρα το 2013,επηρεάστηκαν τα συστήματα της εταιρείας *LastPass* η οποία αποθηκεύει και διαχειρίζεται κωδικούς πρόσβασης χρηστών – πελατών υπηρεσιών υπολογιστικού νέφους. Οι ειδικοί ασφαλείας παρατήρησαν περίεργη δραστηριότητα στα συστήματά τους καθώς υπήρχαν περισσότερα δεδομένα που έφευγαν (*output data*/*response data*) έναντι εκείνων που εισάγονταν (*input data/request data*). Λόγω αυτών των ενεργειών, η επιχείρηση υποψιάστηκε ότι επρόκειτο για επιχείρηση εισβολής, συμπεριλαμβανομένης της κλοπής ευαίσθητων δεδομένων πελατών και κωδικών πρόσβασης σύνδεσης. Προκειμένου να προστατεύσει καλύτερα τα ευαίσθητα δεδομένα των διακομιστών της, η εταιρεία βελτίωσε τις τεχνικές κρυπτογράφησης και έθεσε πρόσθετες δικλείδες ασφαλείας. Μεταξύ των πιο κοινών τακτικών και μεθοδολογιών για την κλοπή της ταυτότητας των χρηστών είναι:

- Η απάτη καταναλωτή (*customer fraud*) και οι εσωτερικές επιθέσεις (*insider attacks*).
- Οι επιθέσεις καταγραφέα πλήκτρων(*keylogger attacks*).
- Οι επιθέσεις τύπου «άνθρωπος στη μέση» (*man-in-the-middle attack*).
- Οι επιθέσεις ηλεκτρονικού ψαρέματος(*phishing*) και ανακάλυψης κωδικού πρόσβασης (*password discovery attacks*).
- Οι επιθέσεις κλοπής συνεδριών ή πειρατείες συνεδρίας (*session hijacking attacks*).

*5.1.2.2 Αντίμετρα*

Λόγω της συμβατικής διαδικασίας ελέγχου ταυτότητας, η κοινή τεχνολογία επιβαρύνει σημαντικά τους πελάτες. Οι συγγραφείς *Kang&Zhang*(2010) πρότειναν την ιεραρχική στρατηγική ελέγχου ταυτότητας (*IBA: Identity-Based Authentication*), η οποία χρησιμοποιεί για τον έλεγχο της ταυτότητας ένα μικρό μέγεθος κλειδιού που επιτρέπει την κρυπτογράφηση ενός αρχείου και την αποθήκευση του αντίστοιχου κρυπτογραφημένου κειμένου στο νέφος.

Οι συγγραφείς *Revar&Bhavsar*(2011) εξέτασαν το σχήμα ελέγχου ταυτότητας*SSO*[8](*Single sign-on*) και άλλες υπάρχουσες μεθόδους ελέγχου ταυτότητας. Επειδή προσφέρει εξαιρετικούς τρόπους για την προστασία των χρηστών έναντι μη ασφαλών δικτύων, ο έλεγχος ταυτότητας χρήστη με χρήση τεχνολογιών όπως το *cURL*[9] και το *SSL* (*Secure Sockets Layer*) είναι ιδιαίτερα επιτυχημένος. Προσφέροντας μια συλλογή από πιστοποιημένες και αξιόπιστες σουίτες κρυπτογράφησης και πιστοποιητικά διακομιστή, οι χρήστες ενδέχεται να προστατεύονται από τις επιθέσεις τύπου*man-in-the-middle*. Όταν οι χρήστες δημιουργούν πράκτορες *SSO* και οι πληροφορίες αποστέλλονται μέσω αιτημάτων *http*, η διαδικασία κρυπτογράφησης πραγματοποιείται χρησιμοποιώντας *RSA*(*Rivest-Shamir-Adleman*) αλγόριθμους. Ωστόσο, οι συγγραφείς δεν εξήγησαν πώς θα μπορούσε να χρησιμοποιηθεί το *SSO* για πρόσβαση σε υπηρεσίες *cloud* από φορητή συσκευή ή άλλη συσκευή συμβατή με το *cloud*. Ωστόσο, για την προστασία του συστήματος από τις εγγενείς αδυναμίες του διαδικτυακού ελέγχου ταυτότητας, (Sawesi et al., 2013) ο έλεγχος ταυτότητας βάσει ψηφιακής υπογραφής *XML* μπορεί να είναι η καλύτερη επιλογή.

Το *MiLAMoB*(*Middleware Layer for Mobile Devices*) είναι μια τεχνική ελέγχου ταυτότητας που ελέγχει την ταυτότητα των χρηστών για λογαριασμό της συσκευής του πελάτη (Lomotey and Deters., 2013). Ο έλεγχος ταυτότητας είναι η διαδικασία εντοπισμού των εξουσιοδοτημένων χρηστών χρησιμοποιώντας ένα αναγνωριστικό ή κάποιον κωδικό πρόσβασης. Καθώς το υπολογιστικό νέφος επεκτείνεται υπάρχει η ανάγκη για πολλούς ελέγχους ταυτότητας. Επίσης, καθώς αυξάνεται ο αριθμός των ατόμων που χρησιμοποιούν τα συστήματα *cloud*,αυξάνονται και οι ταυτότητες και οι διαδικασίες για τον έλεγχο ταυτότητας των χρηστών. Η χρήση συστημάτων ελέγχου ταυτότητας πολλαπλών επιπέδων είναι μια προσέγγιση για την προστασία του συστήματος από παράνομη χρήση. Το σύστημα ελέγχου ταυτότητας πολλαπλών επιπέδων (Dinesha and Agrawal, 2012; Yassin et al., 2012) απαιτούν

[8]Το *Single sign-on* είναι ένα σχήμα ελέγχου ταυτότητας που επιτρέπει σε έναν χρήστη να συνδεθεί με ένα μόνο αναγνωριστικό σε οποιοδήποτε από πολλά σχετικά, αλλά ανεξάρτητα συστήματα λογισμικού (Πηγή:https://en.wikipedia.org/wiki/Single_sign-on).

[9]Το *cUrl* είναι ένα εργαλείο γραμμής εντολών για τη λήψη ή την αποστολή δεδομένων καθώς και αρχείων που χρησιμοποιούν την *URL* σύνταξη. (Πηγή: https://en.wikipedia.org/wiki/CURL).

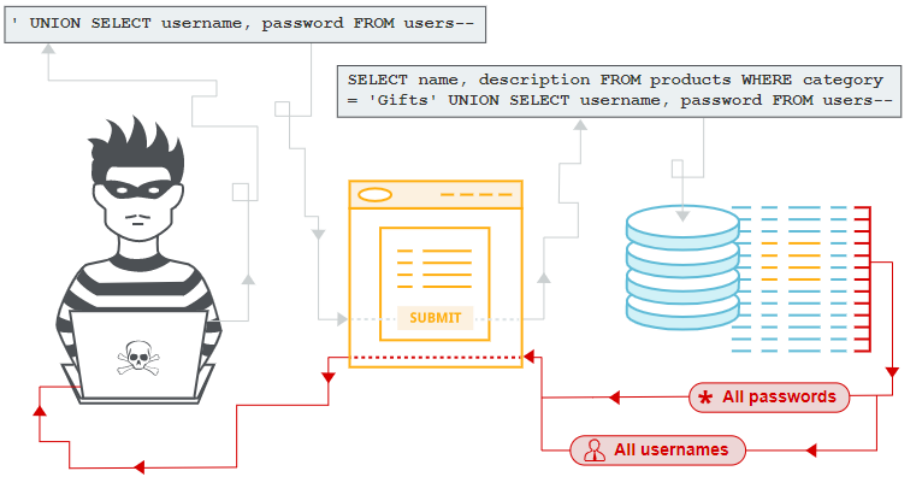
συνδυαστικά και άλλες μορφές ελέγχου ταυτότητας εκτός από το όνομα χρήστη και τον κωδικό πρόσβασης. Ορισμένες μέθοδοι συνδυάζουν δακτυλικά αποτυπώματα, βιομετρικά δεδομένα, ψηφιακές υπογραφές ή τη χρήση ενός (*OTP: One Time Password)*κωδικού τον οποίο ο χρήστης λαμβάνει μέσω ενός άλλου καναλιού (*SMS*, *e-mail*, *viber*, *push notification*).

### *5.1.3 SQL Injection attacks*

#### *5.1.3.1 Περιγραφή επίθεσης*

Το *SQL-injection* (*SQLi*) και το *Cross-SiteScripting* (*XSS*) είναι οι δύο πιο διαδεδομένες επιθέσεις που χρησιμοποιούνται για την κλοπή της ταυτότητας του χρήστη από μια ηλεκτρονική εφαρμογή. Οι επιθέσεις πετυχαίνουν τον σκοπό τους με τη βοήθεια της έγχυσης κακόβουλου κώδικα στις εφαρμογές Ιστού. Οι κυβερνοεγκληματίες εισάγουν ειδικούς χαρακτήρες κατά την υποβολή των δεδομένων μιας ιστοσελίδας από τους επισκέπτες, ενέργειες οι οποίες τροποποιούν ένα τυπικό ερώτημα *SQL*(*Sequel Query Language*) από τον κακόβουλο κώδικα που έχει εισαχθεί σε αυτό. Το τροποποιημένο αυτό ερώτημα δίνει στους επιτιθέμενους τη δυνατότητα τόσο να μεταβάλλουν όσο και να αφαιρέσουν εγγραφές από την βάση στην οποία αποκτούν πρόσβαση, ακόμη και να τροποποιήσουν την ίδια την βάση(*alter db schema*)(Bhadauria et al., 2011).

Οι βάσεις δεδομένων και οι διακομιστές Ιστού αποτελούν ένα σημαντικό μέρος των συστημάτων μέσα στις διάφορες πλατφόρμες υπολογιστικού νέφους, συνεπώς είναι και ιδανικοί υποψήφιοι για την εξαπόλυση των παραπάνω επιθέσεων (Siemons, 2018).




***Εικόνα 15****: SQL Injection attack*
**Πηγή**:PortSwigger, unkown

#### *5.1.3.2Αντίμετρα*

Υπάρχουν αρκετά αντίμετρα που μπορούν να εφαρμοστούν για να αποτραπεί η επιτυχία μιας τέτοιας επίθεσης. Ωστόσο οι περισσότερες λύσεις είναι προληπτικές. Η κύρια και βασική

προληπτική στρατηγική είναι η απολύμανση (*sanitization*) της εισόδου των ιστοτόπων. Μεταξύ των βέλτιστων πρακτικών, είναι ο προγραμματιστής να αποφεύγει τη χρήση μεμονωμένων χαρακτήρων, τη χρήση των χαρακτήρων διαφυγής (*escape characters*) και να χρησιμοποιεί έτοιμες δηλώσεις (*Prepared Statements*) (Siemons, 2018).

Η χρήση ενός τείχους προστασίας εφαρμογών Ιστού (*WAF: Web Application Firewall*)ή μιας λύσης *IDS*(*Intrusion Detection System*)*/IPS*(*Intrusion Prevention System*) για τον έλεγχο της εισερχόμενης κυκλοφορίας είναι κάποιες άλλες επιλογές. Αυτές οι λύσεις καθιστούν δυνατή την απόρριψη ή την προειδοποίηση για ένα αίτημα πριν αυτό φτάσει στον διακομιστή Ιστού, ωστόσο, είναι συνήθως ακριβές και θέτουν ορισμένες δυσκολίες στην κρυπτογραφημένη *HTTPS* (*Hypertext Transfer Protocol Secure*) επικοινωνία. Προκειμένου μια συσκευή *WAF* ή *IDS*/*IPS* να μπορεί να ελέγχει την κυκλοφορία για κακόβουλο περιεχόμενο, απαιτείται η υποκλοπή του *SSL*, πρακτική που μπορεί να έχει αρνητικές επιπτώσεις στην απόδοση και ταυτόχρονα να είναι πολύ δαπανηρή για την ανάπτυξη και τη συντήρησή της. Αυτές οι επιλογές σε καμία περίπτωση δεν χρησιμεύουν ως υποκατάστατο των διαδικασιών απολύμανσης εισόδου του ίδιου του διακομιστή (Siemons, 2018).

Το *Microsoft Azure* παρέχει προστασία έναντι τέτοιων επιθέσεων με το εργαλείο *SQL Database Threat Detection*. Αυτή η υπηρεσία δημιουργεί προειδοποιήσεις με βάση το *SQL-injection script*. Η προστασία επιτυγχάνεται εντοπίζοντας πιθανές ευπάθειες με την σύγκριση των αναμενόμενων έναντι των ασυνήθιστων μοτίβων πρόσβασης στις προστατευμένες βάσεις δεδομένων. Φυσικά, υπάρχουν και άλλοι προμηθευτές που παρέχουν αυτού του είδους την ασφάλεια. Για παράδειγμα, η *Amazon* παρέχει μια παραλλαγή του τείχους προστασίας εφαρμογών Ιστού που αναφέρθηκε παραπάνω. Να σημειωθεί ότι η τοποθέτηση του *WAF* στο ίδιο φυσικό μηχάνημα που φιλοξενεί τον διακομιστή Ιστού ή την βάση των δεδομένων παρέχει ορισμένα επιπρόσθετα πλεονεκτήματα(Siemons, 2018).

### *5.1.4 Cross-site scripting*

*5.1.4.1 Περιγραφή επίθεσης*

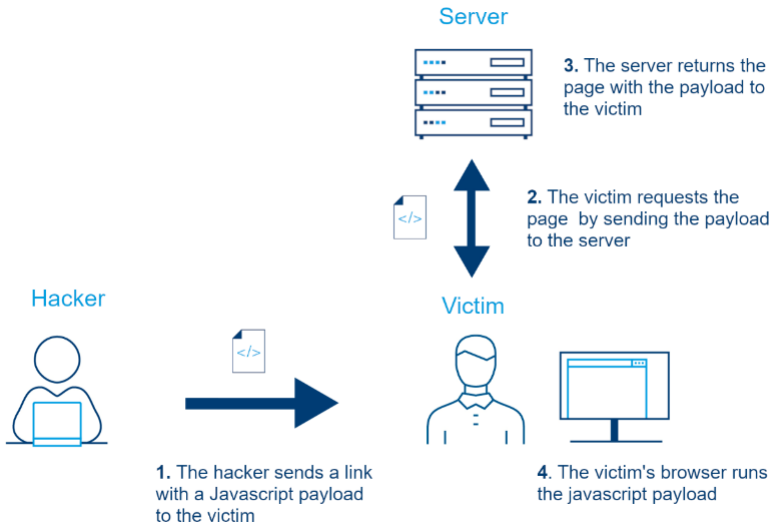
Το *cross-site scripting* (*XSS*), είναι μια από τις πιο δημοφιλείς τεχνικές επίθεσης στο επίπεδο των εφαρμογών. Ανήκει στους τύπους επίθεσης με έγχυση, καθώς κακόβουλα σενάρια εισάγονται στο διαδικτυακό περιεχόμενο (Rodero-Merino et al., 2012). Επειδή το σύννεφο προσφέρει ένα κοινόχρηστο περιβάλλον, οι εισβολείς προσπαθούν να ενσωματώσουν κακόβουλα σενάρια, γραμμένα είτε σε*JavaScript*, είτε σε*HTML*(*Hypertex tMark-up Language*) ή ακόμη και σε *VBSCRIPT*, σε δυναμικές εφαρμογές Ιστού προκειμένου να ανακτήσουν σημαντικά δεδομένα από τους υπολογιστές πολλών χρηστών(Iqbal et al., 2016).

Σε αυτό το σενάριο επίθεσης, οι χρήστες ενδέχεται να εισάγουν τη σωστή διεύθυνση *URL* κατά καιρούς, αλλά οι εισβολείς μπορούν να την παραβιάσουν και να ανακατευθύνουν τον χρήστη στον δικό τους ιστότοπο προκειμένου να κλέψουν τα στοιχεία σύνδεσής τους. Παρόμοια με το *XSS*, οι επιθέσεις τύπου *DOS* και οι υπερχειλίσεις *buffer* μπορούν να χρησιμοποιηθούν για την κλοπή των κωδικών πρόσβασης των χρηστών (Iqbal et al., 2016).

Υπάρχουν πολλές παραλλαγές αυτού του τύπου της επίθεσης. Πιο αναλυτικά (Tozzi, 2023):

- ***Non-persistent or reflected XSS attacks* (Μη επίμονες ή αντανακλαστικές*XSS* επιθέσεις):**Σε αυτού του είδους των *XSS* επιθέσεων, οι επιτιθέμενοι εξαπατούν τους χρήστες ώστε να επισκεφτούν μια ειδικά σχεδιασμένη *URL* διεύθυνση προκειμένου να πετύχουν την έγχυση του κακόβουλου κώδικα. Η διεύθυνση αυτή είναι συνήθως ένας αξιόπιστος ιστότοπος, ο οποίος περιλαμβάνει κακόβουλο κώδικα εξαιτίας κάποιας ευπάθειας που ανακάλυψαν και εκμεταλλεύτηκαν οι κυβερνοεγκληματίες. Η διεύθυνση *URL* συχνά αποκρύπτει τον κακόβουλο κώδικα, καθιστώντας πιο δύσκολη την αναγνώριση αυτού του είδους την επίθεση.

  Σε μια μη επίμονη *XSS* επίθεση, ο εισβολέας εισάγει κώδικα που μπορεί να εκτελεστεί στο πρόγραμμα περιήγησης του χρήστη μέσα σε μία *HTTP* απάντηση. Οι μέθοδοι τύπου *POST* και *GET* χρησιμοποιούνται σε αυτές τις περιπτώσεις στέλνοντας τον κακόβουλο κώδικα στον φυλλομετρητή (*browser*) του χρήστη μόνο για μια φορά.

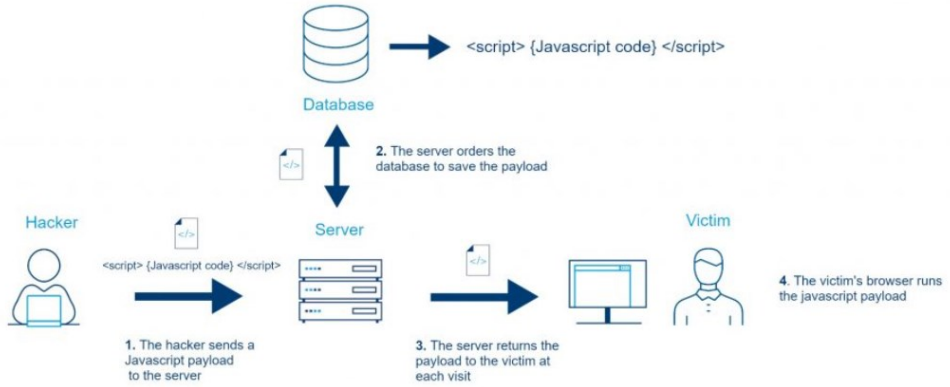



***Εικόνα 16**: Non-persistent or reflected XSS attacks*
**Πηγή**:UBIKA, 2022

- ***Persistent or stored XSS attacks* (Επίμονες ή αποθηκευμένες επιθέσεις τύπου *XSS*):** με παρόμοιο τρόπο όπως και πριν οι κακόβουλοι χρήστες εισαγάγουν κώδικα σε

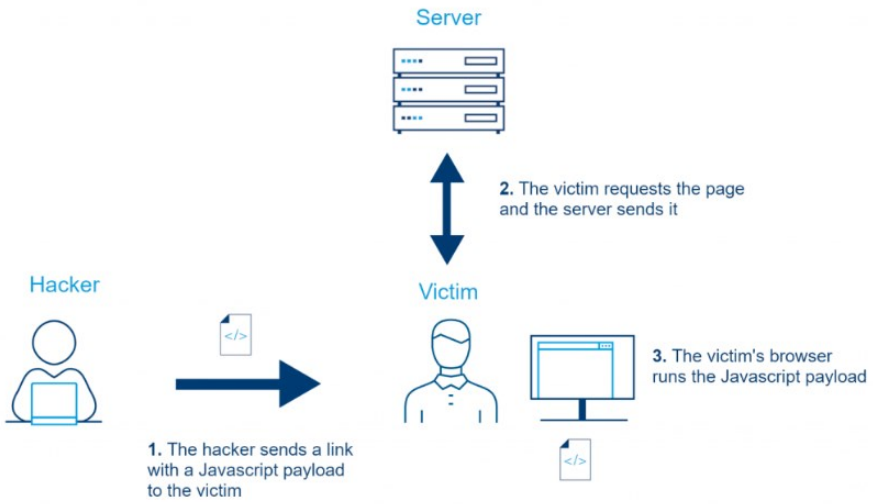
ιστότοπο ή κάποια διαδικτυακή εφαρμογή ενός τρίτου μέρους. Οι χρήστες που επισκέπτονται τον μολυσμένο ιστότοπο τροφοδοτούνται με τον κακόβουλο κώδικα, ο οποίος στη συνέχεια εκτελείται στα προγράμματα περιήγησής τους.

Σε μια επίμονη επίθεση *XSS*, η εφαρμογή Ιστού αποθηκεύει τα δεδομένα που δημιουργούνται και τα στέλνει πίσω στο πρόγραμμα περιήγησης του χρήστη.




***Εικόνα 17**: Persistent or stored attacks*
**Πηγή**:UBIKA, 2022

- ***DOM-based XSS attacks* (Επιθέσεις *XSS* που βασίζονται σε *DOM*):** Αυτές οι επιθέσεις, είναι οι πιο δύσκολες τόσο στην πραγματοποίηση όσο και στον εντοπισμό τους, αφού αλλάζουν το μοντέλο του αντικειμένου εγγράφου (*DOM:Document Object Model*) μιας ιστοσελίδας προκειμένου να εισαχθεί με αυτόν τον τρόπο ο κακόβουλος κώδικας.




***Εικόνα 18**: DOM-based XSS attacks*
**Πηγή**:UBIKA, 2022

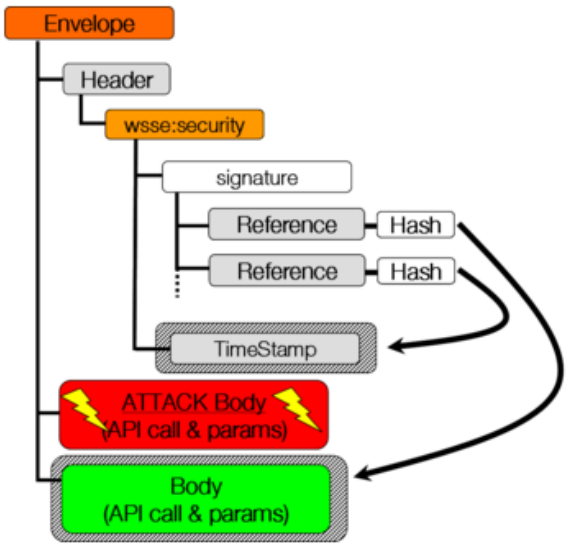
*5.1.4.2 Αντίμετρα*

Η προσέγγιση του ελέγχου μοντέλου προτείνεται στην έρευνα των Sun&He (2012) ως προστασία έναντι του *XSS*. Αυτή η τεχνική εντοπίζει σφάλματα σε εφαρμογές ηλεκτρονικού εμπορίου και παρέχει παραδείγματα για τον τρόπο άμυνας έναντι αυτών των επιθέσεων. Η λειτουργική συμπεριφορά του ιστότοπου εξετάζεται για την ανίχνευση τυχόν παράνομης δραστηριότητας. Αυτή είναι μια αυτοματοποιημένη μέθοδος που βασίζεται σε έναν αλγόριθμο μοντελοποίησης της *HTML* γλώσσας (Iqbal et al., 2016).

### *5.1.5 XML signature wrapping attack*

*5.1.5.1 Περιγραφή επίθεσης*

Ακόμη και τα *SOAP* μηνύματα είναι ευάλωτα στις επιθέσεις. Οι επιθέσεις αυτές είναι γνωστές ως *XML Signature Wrapping* επιθέσεις και λαμβάνουν χώρα στις υπηρεσίες δικτύου, επομένως βρίσκουν εφαρμογή και στο υπολογιστικό νέφος. Σε αυτή την κακόβουλη ενέργεια, οι εισβολείς μπορούν να χρησιμοποιήσουν τα *SOAP* μηνύματα για να στοχεύσουν στα θύματά τους. Όταν ένας χρήστης υποβάλλει ένα αίτημα χρησιμοποιώντας το πρόγραμμα περιήγησής του μέσω της εικονικής μηχανής του, ο διακομιστής δημιουργεί ένα *SOAP* μήνυμα. Τα δομικά δεδομένα που χρησιμοποιούνται για την επακόλουθη επικοινωνία μεταξύ του προγράμματος περιήγησης πελάτη και του διακομιστή περιέχονται σε αυτό το μήνυμα. Οι εισβολείς εκμεταλλεύονται τα τρωτά σημεία στο πρωτόκολλο ασφαλείας του διακομιστή Ιστού εκμεταλλευόμενοι τις *XML* υπογραφές για τον έλεγχο της ταυτότητας των ψηφιακά υπογεγραμμένων μηνυμάτων *SOAP*, εισάγοντας ένα ψεύτικο μήνυμα στη δομή των *SOAP* μηνυμάτων. Με αυτόν τον τρόπο ο εισβολέας μπορεί να κάνει πολλά αιτήματα για διάφορες υπηρεσίες διαδικτύου, ενώ εξακολουθεί να αναγνωρίζεται ως έγκυρος χρήστης (Iqbal et al., 2016; Qaisar&Khawaja, 2012).




***Εικόνα19**: XML signature attack*
Πηγή: Audenard, 2011

Οι υπηρεσίες του υπολογιστικού νέφους που χρησιμοποιούν *XML Signature* επηρεάζονται από τις επιθέσεις αυτού του τύπου. Το χειρότερο σενάριο λαμβάνει χώρα όταν αυτές οι επιθέσεις καταφέρνουν να θέσουν σε κίνδυνο το πλαίσιο ασφαλείας μεταξύ των προγραμμάτων περιήγησης και των υπηρεσιών του νέφους, με αποτέλεσμα να μπορεί ο εισβολέας να επωφεληθεί από τις κρίσιμες λειτουργίες των εικονικών μηχανών, όπως το κοινόχρηστο πρόχειρο (*shared clipboard*). Η κοινή χρήση δεδομένων σε εικονικές μηχανές καθίσταται δυνατή μέσω της λειτουργίας του κοινόχρηστου προχείρου. Όταν παραβιαστεί τελικά ο κεντρικός υπολογιστής, τίθενται σε κίνδυνο όλες οι εικονικές μηχανές του φυσικού διακομιστή (Iqbal et al., 2016).

Ερευνητές από το πανεπιστήμιο «*Ruhr-University Bochum*» ανακάλυψαν ένα ελάττωμα ασφαλείας στην κρυπτογράφηση που χρησιμοποιούσαν τα συστήματα *EC2* και *S3* της *Amazon* το 2011 (Barron et al., 2013). Το πρωτόκολλο ασφαλείας των υπηρεσιών Ιστού είχε μια αδυναμία που επέτρεπε στους εισβολείς να παρακάμψουν την ασφάλεια των ψηφιακά υπογεγραμμένων επικοινωνιών τύπου *SOAP*. Οι εισβολείς αναλάμβαναν με αυτό τον τρόπο τις διεπαφές ελέγχου που χρησιμοποιούνται για τη διαχείριση των πόρων του *cloud*. Οι εισβολείς στη συνέχεια μπορούσαν να αλλάξουν τον κωδικό πρόσβασης του διαχειριστή και να προβούν έπειτα στη δημιουργία, στην τροποποίηση ακόμη και στη διαγραφή των εικονικών μηχανών (Iqbal et al., 2016).

*5.1.5.2 Αντίμετρα*

Ένα βελτιωμένο σύστημα ελέγχου ταυτότητας ψηφιακών υπογραφών *XML* ήταν το αποτέλεσμα της μελέτης των Sawesi et al. (2013). Στην εργασία τους ανέπτυξαν ένα μοναδικό αλγοριθμικό πλαίσιο ασφαλείας για την ψηφιακή υπογραφή *XML* και τον έλεγχο ταυτότητας ελλειπτικής καμπύλης βάσει των *PKI* (*Public Key Infrastructure*) προτύπων σε πύλες *B2C* (*Business-To-Consumer*) *E-Commerce* (*Electronic-Commerce*) που βασίζονται στο σύννεφο. Το μοναδικό αλγοριθμικό πλαίσιο δοκιμάστηκε μέσω προσομοίωσης χρησιμοποιώντας το περιβάλλον *Microsoft Windows* και τη γλώσσα προγραμματισμού *C++*(Sawesi et al., 2013).

Η εφαρμογή της κρυπτογράφησης τόσο στο επίπεδο των ανταλλασσόμενων αρχείων και του μπλοκ των πληροφοριών όσο και σε επίπεδο εφαρμογών είναι ένα επιπλέον αντίμετρο έναντι τέτοιου τύπου επιθέσεων. Μια επιπρόσθετη λύση είναι η χρήση αυτοματοποιημένων σαρωτών για την εύρεση της πλειοψηφίας των τυπικών τρωτών σημείων. Μια ποικιλία σαρωτών διαδικτυακών εφαρμογών είναι χρήσιμοι για τον εντοπισμό διαφόρων τύπων ευπαθειών, συμπεριλαμβανομένων των επιθέσεων έγχυσης *XSS* και *SQL* (Iqbal et al., 2016).

## 5.2Επιθέσεις που στοχεύουν στο PaaS μοντέλο διάθεσης

Η αρχιτεκτονική *Service-Oriented Architecture* (*SOA*) χρησιμοποιείται στην πράξη για την υποστήριξη του *PaaS* μοντέλου διάθεσης. Υπάρχουν ελαττώματα σε αυτήν την προσέγγιση που μπορούν να οδηγήσουν σε επιθέσεις κατά του υπολογιστικού νέφους, συμπεριλαμβανομένων των επιθέσεων του ηλεκτρονικού ψαρέματος, της επίθεσης ανάκτησης και αρχικοποίησης *password*,της επίθεσης τύπου *Man-in-the-middle* και τέλος της επίθεσης με εισχώρηση κακόβουλου λογισμικού.

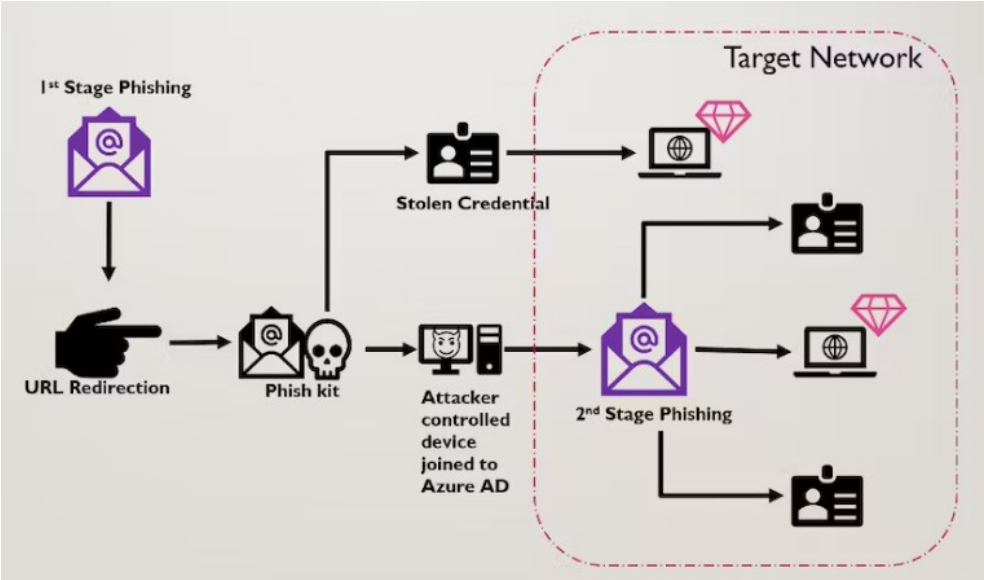
### *5.2.1 Ηλεκτρονικό ψάρεμα (Phishing Attacks)*

*5.2.1.1 Περιγραφή επίθεσης*

Οι επιθέσεις τύπου*phishing* συχνά περιλαμβάνουν ψεύτικα *e-mails* που συνδέονται με ψεύτικους ιστότοπους. Αυτές οι επιθέσεις έχουν αντίκτυπο τόσο στις επιχειρήσεις όσο και στους τελικούς χρήστες / πελάτες της *cloud PaaS* υποδομής. Σε αυτές τις επιθέσεις χρησιμοποιείται η κοινωνική μηχανική, παράλληλα με τους ψεύτικους ιστότοπους, τα παραπλανητικά *e-mails* ή τα κακόβουλα*blogs*.Οι κυβερνοεγκληματίες παραπλανούν τα θύματα τους ώστε να δώσουν ή να καταχωρίσουν τις προσωπικές τους πληροφορίες, όπως είναι οι κωδικοί πρόσβασης. Οι επιθέσεις ηλεκτρονικού ψαρέματος αποτελούν πρόβλημα για όλους τους διαδικτυακούς χρήστες. Τόσο οι οργανισμοί όσο και οι καταναλωτές του μοντέλου διάθεσης υπολογιστικού νέφους τύπου*PaaS*είναι υποψήφια θύματα. Τα γνωστά προγράμματα

περιήγησης Ιστού προσφέρουν πρόσθετα αντίμετρα για την προστασία έναντι αυτών των επιθέσεων, αλλά ακόμη δεν έχει εφαρμοστεί μια πλήρης, καθολική λύση (Iqbal et al., 2016).

Οι επιθέσεις ηλεκτρονικού ψαρέματος συχνά στοχεύουν στις αδυναμίες που σχετίζονται και με τον ανθρώπινο παράγοντα. Οι χρήστες είναι συνήθως το πιο αδύναμο στοιχείο ενός συστήματος ασφαλείας, καθώς πολλές απειλές διαδίδονται εκμεταλλευόμενοι τα τρωτά σημεία της ανθρώπινης φύσης. Εκτός από τους μεμονωμένος χρήστες και οι μεγάλες επιχειρήσεις επηρεάζονται επίσης από αυτούς τους κινδύνους. Τα ζητήματα με τέτοιες επιθέσεις δεν μπορούν να λυθούν πλήρως με μία μόνο στρατηγική. Διάφορες στρατηγικές μετριασμού έχουν παρουσιαστεί στους τομείς της ανίχνευσης, της άμυνας και της πρόληψης (Iqbal et al., 2016).




***Εικόνα 19**: Ηλεκτρονικό ψάρεμα που στοχεύει στο υπολογιστικό νέφος*
Πηγή: HACKERNOON, 2023

*5.2.1.2 Αντίμετρα*

Προκειμένου να αυξηθεί η ασφάλεια των επικοινωνιών ηλεκτρονικού ταχυδρομείου που βασίζονται στο σύννεφο, ένα νέο πλαίσιο που ονομάζεται *Intelligent Cloud Based Email Encryption and Decryption System* (*ICLEEDS*) αναπτύχθηκε από τους Ayodele και Adeegbe το 2013. Ο κύριος στόχος της μεθόδου τους είναι η κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου στο γραμματοκιβώτιο, πριν, δηλαδή, από την αποστολή τους. Αυτή η εξελιγμένη τεχνολογία κρυπτογράφησης που βασίζεται και στις τεχνικές της μηχανικής εκμάθησης βοηθά στη βελτίωση του συστήματος και προστατεύει τα μηνύματα ηλεκτρονικού ταχυδρομείου των χρηστών από επιθέσεις τύπου *phishing*, αλλά και από πλαστογράφηση και αναμετάδοση προηγούμενων μηνυμάτων. Να σημειωθεί ότι για την εφαρμογή αυτού του

πλαισίου στο νέφος είναι απαραίτητο να παρέχονται αυτοπροσαρμόσιμοι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης (Iqbal et al., 2016).

Παρακάτω παρατίθενται και άλλες τεχνικές που έχουν προταθεί για το μετριασμό αυτού του τύπου των επιθέσεων:

- **Ανίχνευση ηλεκτρονικού ψαρέματος βάσει κανόνων**

Η διαδικασία ανίχνευσης ιστοτόπων ηλεκτρονικού ψαρέματος χρησιμοποιώντας προκαθορισμένους κανόνες ή ευρετικές μεθόδους είναι γνωστή ως ανίχνευση βάσει κανόνων. Μπορεί να μην είναι τόσο αποτελεσματική έναντι νέων ή προηγμένων επιθέσεων ηλεκτρονικού ψαρέματος, αλλά μπορεί να φανεί χρήσιμη για τον εντοπισμό καθιερωμένων μορφών επιθέσεων *phishing* και βασίζεται στον έλεγχο ορισμένων κριτηρίων όπως είναι η ηλικία τομέα (*domain age*), το πιστοποιητικό *SSL*, το μήκος διεύθυνσης *URL* και ορισμένες λέξεις κλειδιά.Οι ερευνητές Basnet et al. (2012),Mohammad et al. (2014) και Fazliya & Naleer, (2019) παρουσίασαν στις εργασίες τους μια ποικιλία τεχνικών βασισμένων σε κανόνες που χρησιμοποιούν αλγόριθμους μηχανικής μάθησης για την ανάπτυξη των κανόνων και για την κατηγοριοποίηση των ιστοτόπων είτε ως *phishing* είτε ως αυθεντικοί. Ορισμένες στρατηγικές περιλαμβάνουν επιπλέον άλλες μεθόδους ανίχνευσης, όπως αλγόριθμους εξόρυξης δεδομένων και εκπαίδευση της ευαισθητοποίησης των χρηστών. Η ανίχνευση βάσει κανόνων είναι εξαιρετική στην αναγνώριση σε πραγματικό χρόνο άγνωστων επιθέσεων τύπου ηλεκτρονικού ψαρέματος, καθώς μπορεί να είναι ταυτόχρονα γρήγορη αλλά και αποτελεσματική (Chinguwo & Dhanalakshmi, 2023).

- **Ανίχνευση ηλεκτρονικού ψαρέματος βάσει ανωμαλιών**

Αντιπαραβάλλοντας τα χαρακτηριστικά των ιστοτόπων ηλεκτρονικού ψαρέματος με αυτά των αυθεντικών, μπορεί να χρησιμοποιηθεί μια τεχνική που ονομάζεται ανίχνευση βάσει ανωμαλιών για τον εντοπισμό τους. Πολυάριθμες έρευνες προτείνουν τη χρήση μεθόδων που βασίζονται σε ανωμαλίες για τον εντοπισμό των *URL* διευθύνσεων των ιστοσελίδων ηλεκτρονικού ψαρέματος. Στη μέθοδο που ανέπτυξαν οι Pan&Ding (2006) πληροφορίες από τα αντικείμενα/ιδιότητες της *DOM* διεπαφής όπως ορίζεται από τον*W3C*(*World Wide Web Consortium*) οργανισμό εξάγονται και χρησιμοποιούνται για τη δημιουργία ενός ταξινομητή οποίος επιτυγχάνει την διαφοροποίηση μεταξύ αυθεντικών και ψεύτικων ιστοτόπων. Σε μια άλλη μελέτη των Kaniuk. (2020) προτάθηκε μια μέθοδος δύο σταδίων. Στο πρώτο στάδιο η μέθοδος παρακολουθεί μέσω κινητού τις κινήσεις των ματιών των χρηστών ενώ εκείνοι διαβάζουν μια ιστοσελίδα και στο δεύτερο στάδιο προτείνεται μια μέθοδος ανίχνευσης για την αναγνώριση των *URL* διευθύνσεων ηλεκτρονικού ψαρέματος βάσει των εντοπισμένων

ανωμαλιών. Μια προσέγγιση για τον εντοπισμό ψευδών διευθύνσεων *URL*που εμπερικλείονται στα ηλεκτρονικά μηνύματα προτείνεται από μια άλλη μελέτη που πραγματοποίησαν οι Guan et al. (2020),η οποία χρησιμοποιεί αλγόριθμους που βασίζονται σε ανωμαλίες και σε ένα σχήμα βαθμονόμησης που βαθμολογεί 11 χαρακτηριστικά γνωρίσματα των μηνυμάτων (Chinguwo&Dhanalakshmi, 2023).

- **Ανίχνευση ηλεκτρονικού ψαρέματος με τη βοήθεια της μηχανικής μάθησης**

Προκειμένου να εντοπιστούν οι επιθέσεις ηλεκτρονικού ψαρέματος, έχουν επιστρατευτεί ακόμη και οι τεχνικές της μηχανικής μάθησης. Σε αυτή την προσέγγιση γίνεται χρήση των αλγορίθμων οι οποίοι εξετάζουν διάφορα δεδομένα ενός ιστότοπου. Αυτοί οι αλγόριθμοι μαθαίνουν να διακρίνουν με βάση διάφορα χαρακτηριστικά όπως είναι η δομή, το περιεχόμενο και η συμπεριφορά του *URL*. Με την εκπαίδευση τεράστιων συνόλων δεδομένων τόσο αυθεντικών όσο και γνωστών ιστοτόπων ηλεκτρονικού ψαρέματος επιτυγχάνεται τελικά η ανίχνευση των δεύτερων. Διάφοροι αλγόριθμοι συμπεριλαμβανομένων των *SVM* (*Support Vector Machine*- ΜΔΥ: Μηχανές Διανυσμάτων Υποστήριξης), *Multilayer Perceptron* (*MLP* – πολυεπίπεδοι αισθητήρες), *Decision Tree Induction*(επαγωγή με δέντρα απόφασης), *Naïve Bayes* (ταξινομητής *Bayes*)και *K-Nearest Neighbor* (αλγόριθμος πλησιέστερης γειτνίασης) έχουν προταθεί για την εκπαίδευση του συνόλου των δεδομένων και την κατηγοριοποίηση των *URL*διευθύνσεων. Σε αυτές τις μεθόδους χρησιμοποιούνται διαφορετικά χαρακτηριστικά, συμπεριλαμβανομένων των ποιοτικών χαρακτηριστικών των κειμένων, της αρχιτεκτονικής των συνδέσμων, του περιεχομένου της ιστοσελίδας, των *DNS* (*Domain Name System*) πληροφοριών και της κυκλοφορίας του δικτύου(Chinguwo&Dhanalakshmi, 2023).

- **Ανίχνευση ηλεκτρονικού ψαρέματος με τη βοήθεια της Συλλογικής Μάθησης**

Προκειμένου να αυξηθεί η ακρίβεια και η ανθεκτικότητα, χρησιμοποιούνται τεχνικές μηχανικής εκμάθησης συνόλων ή τεχνικές της συλλογικής μάθησης (*Ensemble Machine Learning*) για τον εντοπισμό των ιστοτόπων ηλεκτρονικού ψαρέματος. Οι ευφυείς αλγόριθμοι αυτής της μεθοδολογίας χρησιμοποιούν μια ποικιλία προσεγγίσεων εξόρυξης δεδομένων για να κατηγοριοποιήσουν τους ιστότοπους ως αυθεντικούς ή ως ψεύτικους. Ένα νέο μοντέλο ανίχνευσης *phishing* χρησιμοποιήθηκε στον αλγόριθμο *XGBOOST* από τους Musa. (2019), ενώ αλγόριθμοι αποθήκευσης και ενίσχυσης όπως οι *GradientBoosting* και *CatBoosting* προτάθηκαν από τους Deekshitha. (2022). Οι παραπάνω προτάσεις είχαν ως στόχο της αύξηση της ακρίβειας της αναγνώρισης εντοπισμού ενός ιστότοπου ηλεκτρονικού ψαρέματος. Ο γενετικός αλγόριθμος χρησιμοποιείται για τη βελτιστοποίηση των παραμέτρων πολλών τεχνικών μηχανικής εκμάθησης συνόλων και στη συνέχεια οι τρεις κορυφαίοι ταξινομητές

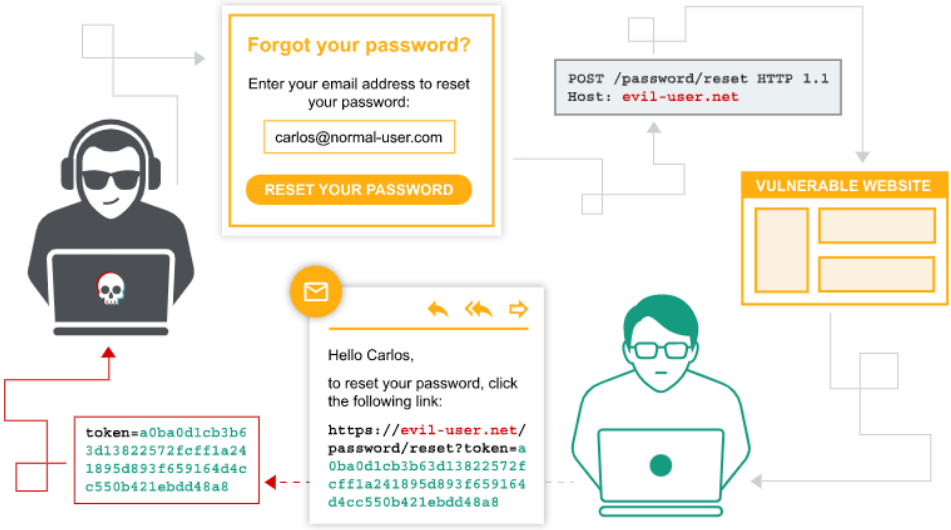
επιλέγονται ως βασικοί ταξινομητές σε μια προσέγγιση στοίβαξης συνόλων. Αυτό το βελτιστοποιημένο μοντέλο για τον εντοπισμό ενός ιστότοπου ηλεκτρονικού ψαρέματος προτάθηκε από τους Al-Sarem et al. (2021) σε μια πρόσφατη εργασία τους(Chinguwo&Dhanalakshmi, 2023).

### *5.2.2 Ανάκτηση και αρχικοποίηση κωδικού πρόσβασης (Password reset attack)*

*5.2.2.1 Περιγραφή επίθεσης*

Προκειμένου να ανασυνθέσουν τον κωδικό πρόσβασης από τα δεδομένα, οι εισβολείς πραγματοποιούν κάθε δυνατό συνδυασμό χαρακτήρων. Το γεγονός ότι το υλικό είναι κρυπτογραφημένο χάρη σε μια ισχυρή μέθοδο κρυπτογράφησης δεν αποκλείει και την επιτυχή εύρεσή του. Καταβάλλοντας περαιτέρω προσπάθεια και κάνοντας χρήση ισχυρών υπολογιστικών πόρων, εργαλείων και διαδικασιών, μπορεί να βρεθεί τελικά η τιμή του.

Ωστόσο, η επένδυση σε υπερυπολογιστές υψηλής απόδοσης για την αποκωδικοποίηση κρυπτογραφημένων δεδομένων δεν είναι μια έξυπνη κίνηση. Αυτά τα μηχανήματα μπορεί να είναι αποτελεσματικά για ένα περιορισμένο σύνολο εργασιών, αλλά είναι επίσης ακριβά όσον αφορά το οικονομικό βάρος. Αλλά με το υπολογιστικό νέφος, οι τελικοί χρήστες έχουν πρόσβαση σε εξαιρετικά ισχυρούς υπολογιστές που τους επιτρέπουν να εκτελούν τις απαιτητικές υπολογιστικές αυτές εργασίες, κάτι που είναι πολύ ανώτερο από τα μηχανήματα που λειτουργούν σε μια συμβατική υποδομή. Ένας κατάλληλος εικονικός υπολογιστής μπορεί να αγοραστεί ή να ενοικιαστεί από το *Amazon Cloud* για τη διεξαγωγή επιθέσεων ωμής βίας (Ristenpart et al., 2009).




***Εικόνα 20**: Εξαπόλυση επίθεσης τύπου «Password reset attack»*
**Πηγή**: PortSwigger

Τον Ιούλιο του 2012, η ομάδα χάκερ «*UGNazi*» εκμεταλλεύτηκε κρίσιμα τρωτά σημεία στον τηλεφωνητή και στις διαδικασίες ανάκτησης των κωδικών πρόσβασης της *AT&T* και της *Gmail*. Το αποτέλεσμα αυτής της επίθεσης ήταν ότι κατάφεραν να έχουν πρόσβαση στον προσωπικό λογαριασμό *Gmail* του Διευθύνοντα Συμβούλου της *CloudDare*. Με παρόμοιο τρόπο, ένα άλλο περιστατικό που αφορούσε την υπηρεσία αποθήκευσης *cloud* του *Dropbox* αποκαλύφθηκε τον Ιούλιο του 2012 (Barron et al., 2013). Σε αυτό το περιστατικό, οι χάκερ απέκτησαν ονόματα χρηστών και κωδικούς πρόσβασης από άλλους διακομιστές προκειμένου να έχουν πρόσβαση στους λογαριασμούς πελατών του *Dropbox*.

Υπάρχουν δύο κατηγορίες σε αυτό τον τύπο της επίθεσης:

- **Επίθεση Brute Force**

Το πιο τυπικό είδος επίθεσης ωμής βίας στοχεύει στα διαπιστευτήρια σύνδεσης των εφαρμογών Ιστού. Οι χρήστες συχνά επιλέγουν απλές λέξεις ή φράσεις ως *password* (κωδικός πρόσβασης). Αυτό καθιστά τις επιθέσεις ωμής βίας ως μια απλή διαδικασία. Τέτοιου τύπου επιθέσεις χρησιμοποιούν μια μακρά λίστα λέξεων και φράσεων ως πιθανούς κωδικούς πρόσβασης σε μια προσπάθεια να εισέλθουν στο σύστημα. Ο όρος «επίθεση λίστας λέξεων» ή «επίθεση λεξικού» αναφέρεται σε αυτήν την τεχνική.

- **Αναγνωριστικά συνεδρίας Brute Forcing**

Το *HTTP* είναι ένα πρωτόκολλο χωρίς κατάσταση (*stateless*). Οι εφαρμογές Ιστού διασφαλίζουν ότι προκειμένου να διατηρηθεί η κατάσταση, το αναγνωριστικό περιόδου λειτουργίας έχει παρασχεθεί από το πρόγραμμα περιήγησης σε κάθε αίτημα. Πιθανότατα, αυτή η αναγνώριση της περιόδου της σύνδεσης διατηρείται σε ένα *HTTP cookie* ή στην *URL* διεύθυνση. Σε ωμές επιθέσεις, ο εισβολέας προσπαθεί να καταλάβει την ταυτότητα της περιόδου σύνδεσης του χρήστη, επιχειρώντας κάθε πιθανό κωδικό πρόσβασης μέχρι να ανακαλύψει τον σωστό.

*5.2.2.2 Αντίμετρα*

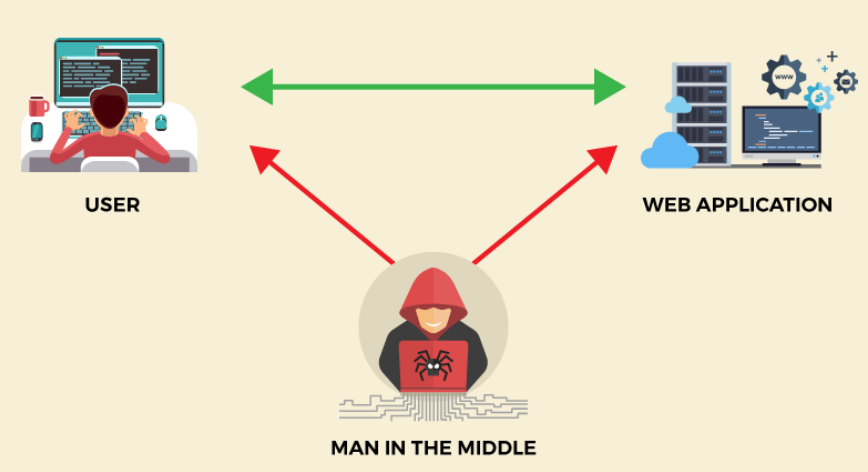
Τα αντίμετρα που μπορούν να πάρουν οι τελικοί χρήστες για την αποφυγή τέτοιου τύπου επιθέσεων είναι η επιλογή ισχυρών κωδικών πρόσβασης με ποικιλία αλφαριθμητικών και ειδικών χαρακτήρων, κεφαλαίων και μικρών γραμμάτων που θα εναλλάσσονται σε ένα μεγάλου μήκους κωδικό.

### *5.2.3 Man-in-the-Middle attack*

*5.2.3.1 Περιγραφή επίθεσης*

Σε αυτού του είδους την επίθεση οι εισβολείς πραγματοποιούν την υποκλοπή με το να «ακούν» τις συνομιλίες δύο συμμετεχόντων. Σε μια τυπική επικοινωνία μεταξύ δύο υπολογιστών που

βασίζεται στο διαδίκτυο, η κίνηση του δικτύου μετακινείται εμπρός και πίσω. Οι εισβολείς μπορούν να υποκλέψουν μηνύματα σε μια ανταλλαγή του δημόσιου κλειδιού που αποστέλλεται μεταξύ των δύο υπολογιστών και να τα επαναμεταδώσουν χρησιμοποιώντας τα δικά τους δημόσια κλειδιά ενώ οι αρχικοί χρήστες έχουν την εντύπωση ότι εξακολουθούν να επικοινωνούν μεταξύ τους. Μια άλλη πολύ γνωστή απεικόνιση αυτής της επίθεσης είναι όταν ο εισβολέας διαχωρίζει μια *TCP* διασύνδεση σε δύο νέα τμήματα, το ένα μεταξύ του πελάτη και του εισβολέα και το άλλο μεταξύ του εισβολέα και του διακομιστή, ενώ ο πελάτης και ο διακομιστής συμμετέχουν σε μια *http* κλήση.




***Εικόνα 21**: Man-in-the-Middle attack*
**Πηγή**: Threatcop, unkown

*5.2.3.2 Αντίμετρα*

Για την προστασία από αυτού του είδους των επιθέσεων έχει αναπτυχθεί ένας αριθμός εργαλείων με ισχυρούς μηχανισμούς κρυπτογράφησης (Bhadauria and Sanyal, 2012), συμπεριλαμβανομένων των *Dsniff*, *Cain*, *Ettercap*, *Wsniff*, *Airjack*, κ.λπ.

Το σχέδιο για την εξασφάλιση της ζωντανής μετανάστευσης *VM* προτάθηκε από τους συγγραφείς Zhang et al. (2008) για την προστασία από αυτού του τύπου τις επιθέσεις στο περιβάλλον του υπολογιστικού νέφους. Με τη χρήση αυτής της τεχνικής, το *VMM* θα είναι υπεύθυνο για όλες τις εργασίες που σχετίζονται με τη ζωντανή μετεγκατάσταση, συμπεριλαμβανομένης της εύρεσης και της αποκρυπτογράφησης όλων των σελίδων πηγής. Η προσέγγιση ξεκινά με την αποκρυπτογράφηση των κλειδιών και τον κατακερματισμό τους χρησιμοποιώντας το δημόσιο κλειδί της πλατφόρμας. Στη συνέχεια, και πριν από την αποκρυπτογράφηση, γίνεται η σύγκριση με τις τιμές κατακερματισμού των σελίδων πηγής.

Τα τείχη προστασίας, η κρυπτογράφηση και η απομόνωση δικτύου είναι μερικές από τις πολύ λίγες τεχνικές που προσφέρουν μηχανισμούς ασφαλείας σε επίπεδο δικτύου. Δίνοντας

έμφαση στα παραδοσιακά μέτρα ασφαλείας, όπως τα ασφαλή *API* και λαμβάνοντας συχνά αντίγραφα ασφαλείας, αυτές οι επιθέσεις μπορούν να αποφευχθούν (Zhang et al., 2011).

Επιπλέον, τόσο οι αξιόπιστοι κόμβοι όσο και οι εργαζόμενοι θα πρέπει να ελέγχονται και να επιτρέπεται η πρόσβασή τους σύμφωνα με τους κανόνες που έχουν τεθεί. Να σημειωθεί ότι όταν το πρωτόκολλο μετεγκατάστασης είναι κρυπτογραφημένο, είναι και αυτό ευάλωτο σε μια επίθεση τύπου Man-in-the-Middle (Bryan Williams, 2010), η οποία επιτρέπει την πραγματοποίηση αυθαίρετων αλλαγών στην κατάσταση της εικονικής μηχανής.

### *5.2.4 Επιθέσεις με εισχώρηση κακόβουλου λογισμικού στο νέφος (Cloud malware-injection attack)*

*5.2.4.1 Περιγραφή επίθεσης*

Η βασική ιδέα αυτής της επίθεσης είναι ότι ένας εισβολέας ανεβάζει ένα παραποιημένο αντίγραφο της υπηρεσίας του θύματος εισάγοντας τους δικούς του κακόβουλους κώδικες. Αυτή η επίθεση είναι ένας σημαντικός πρεσβευτής για την εκμετάλλευση του οικοσυστήματος των υπηρεσιών νέφους (Dey&Sen, 2017).

Ο στόχος αυτής της επίθεσης είναι ο επιτιθέμενος να αποκτήσει πρόσβαση στα δεδομένα χρήστη που είναι αποθηκευμένα στο νέφος. Οι χάκερ μπορούν να μεταδώσουν αιτήματα σε μολυσμένες μονάδες και να εκτελέσουν κακόβουλο κώδικα μολύνοντας τις *SaaS*, *PaaS* ή *IaaS* υποδομές. Το επικίνδυνο κακόβουλο λογισμικό έχει δύο στόχους: είτε να κλέψει δεδομένα είτε να «κρυφακούσει» τους καταναλωτές -πελάτες. Οι πιο συχνοί τύποι επιθέσεων έγχυσης κακόβουλου λογισμικού είναι «επιθέσεις δέσμης ενεργειών μεταξύ τοποθεσιών» και «επιθέσεις έγχυσης SQL» (Katrenko, 2020).

Οι επιθέσεις δέσμης ενεργειών μεταξύ τοποθεσιών καταχρώνται ευαίσθητες ιστοσελίδες εισάγοντας κακόβουλα σενάρια με προσθήκες όπως, για παράδειγμα, στο *Flash* ή στη *Javascript*. Τέτοιες επιθέσεις προσπαθούν να εξαπατήσουν το *cloud* ώστε ο επιτιθέμενος να θεωρείται ότι είναι γνήσιος χειριστής ενώ εισάγει στοιχεία σε δομές μηνυμάτων για την επικύρωση των υπογραφών που καλύπτουν το αίτημα μη εξουσιοδοτημένης υπηρεσίας του εισβολέα. Οι κυβερνοεγκληματίες μπορούν έπειτα να προβούν σε διοικητικές ενέργειες, συμπεριλαμβανομένης της αφαίρεσης και της προσθήκης των δεδομένων του πελάτη (Iqbal et al., 2016).

Η έγχυση *SQL* είναι ένα διαφορετικό είδος επίθεσης κακόβουλου λογισμικού που μπορεί να συμβεί σε μια ρύθμιση *cloud*. Αυτές οι επιθέσεις στοχεύουν σε μη προστατευμένες εφαρμογές βάσης δεδομένων διακομιστών *SQL*, όπως αναλύθηκαν σε προηγούμενη παράγραφο.

Οι εγκληματίες του κυβερνοχώρου που θέλουν να πραγματοποιήσουν κατανεμημένες επιθέσεις άρνησης υπηρεσίας και να στείλουν ανεπιθύμητα μηνύματα στοχεύουν σε ευάλωτες σελίδες με μεγάλους όγκους επισκεπτών. Το κακόβουλο λογισμικό αναπτύσσεται είτε σε μη προστατευμένες βάσεις δεδομένων είτε συνεργάζεται με άλλο επιβλαβές υλικό για τη λήψη του από σκοτεινούς ιστότοπους και την ενσωμάτωσή του στο *botnet* τους. Οι χρήστες θα πρέπει να αποφεύγουν να επισκέπτονται ιστότοπους που είναι γνωστό ότι έχουν παραβιαστεί, να αποφεύγουν τη χρήση προσθηκών όπως το *Flash* και να αποφεύγουν να κάνουν κλικ σε αναδυόμενα παράθυρα ανεξάρτητα από το τι φαίνεται ότι προσποιούνται ότι προσπαθούν να κάνουν (Iqbal et al., 2016).

Το Υπουργείο Οικονομικών των ΗΠΑ φέρεται να έκλεισε τέσσερις ιστοτόπους του *Bureau of Engraving and Printing* στους οποίους είχε πρόσβαση το κοινό τον Μάιο του 2009, αφού εντόπισαν κακόβουλο λογισμικό στον δικό τους ιστότοπο. Μεταγενέστερες έρευνες διαπίστωσαν ότι για το πρόβλημα ευθυνόταν μια άλλη οντότητα.

## 5.3Επιθέσεις που στοχεύουν στο IaaS μοντέλο διάθεσης

Οι εισβολείς αναλαμβάνουν αρχικά τον έλεγχο των δραστηριοτήτων μιας εικονικής μηχανής που φιλοξενείται σε αυτό το μοντέλο διάθεσης (*IaaS*), και με αυτό τον τρόπο αποκτούν πρόσβαση σε άλλα παραβιασμένα φιλοξενούμενα *VMs* ή στον *hypervisor*. Ενδεικτικά, το *DKSM*(*Direct Kernel Structure Manipulation*) είναι μια στρατηγική παράκαμψης διαφόρων μέτρων ασφαλείας που εξαρτώνται από το λειτουργικό σύστημα (*OS: Operating System*). Παρουσιάζονται δύο μοντέλα επίθεσης. Το ένα τροποποιεί τη σημασιολογία της δομής του πυρήνα, ενώ το άλλο τροποποιεί τη σύνταξη. Οι εισβολείς έλκονται από επιθέσεις σε πολυάριθμα παραβιασμένα *VMs* λόγω της ίδιας διαμόρφωσης στο υπολογιστικό νέφος, συμπεριλαμβανομένων των τεχνολογιών εικονοποίησης, του διαμοιρασμένου ευαίσθητου λογισμικού και των κοινών φυσικών πόρων (Ibrahim et al., 2011).

Όπως αναφέρθηκε ήδη, ο υπερπιστωτής είναι μια ευπάθεια που μπορεί να χρησιμοποιηθεί ως εφαλτήριο για περαιτέρω επιθέσεις, συμπεριλαμβανομένης της κακής χρήσης των υπολογιστικών πόρων (Turnbull and Shropshire, 2013). Η παράκαμψη οποιουδήποτε συστήματος ανίχνευσης εισβολής στην υποδομή δικτύου και η εκτέλεση του κακόβουλου *VM* ισοδυναμεί με τη μεταφορά του κακόβουλου κώδικα στο σύστημα δικτύου μέσω ενός ενιαίου φυσικού μηχανήματος. Για την εξυπηρέτηση μεγάλου αριθμού χρηστών, το εγκατεστημένο *VM* συνδέεται λογικά με ένα εικονικό δίκτυο. Το κοινό περιβάλλον της υποδομής *cloud* επιτρέπει τη δημιουργία διαφόρων μοντέλων επίθεσης στο εικονικό δίκτυο. Ως αποτέλεσμα, ελαττώματα ασφαλείας και επιθέσεις ενδέχεται να επηρεάσουν τόσο τις

εφαρμογές όσο και τα δεδομένα μαζί με την κατάστασή τους. Οι εισβολείς περιστασιακά χειρίζονται τους πίνακες σελίδων και στη συνέχεια να κάνουν κατάχρηση του τρέχοντος κώδικα. Με τη χρήση κακόβουλων παραμέτρων, οι επιτιθέμενοι μπορούν να διακόψουν και να αλλάξουν τη διαδικασία χειρισμού των αλλαγών του πίνακα σελίδων. Αφού ένας κυβερνοεγκληματίας ελέγχει με επιτυχία τις σελίδες μνήμης, η εικόνα ενός *VM* μπορεί να ανακατασκευαστεί. Η παραπάνω ενέργεια έχει ως αποτέλεσμα να μεταβάλλεται το περιεχόμενο του στόχου εξαπολύοντας με αυτό τον τρόπο επιθέσεις πλαστοπροσωπίας(*spoofing attacks*) (Wang and Jiang, 2010).

Μεταξύ των εικονικών μηχανών, υπάρχουν συνολικά δύο μορφές κίνησης:

- Η εσωτερική κίνηση: είναι η επικοινωνία που λαμβάνει χώρα μεταξύ των *VM* και της ομάδας χρηστών του. Οποιεσδήποτε ιδιωτικές πληροφορίες ενδέχεται να βρίσκονται στην εσωτερική αυτή ροή. Οι πάροχοι κακόβουλων υπηρεσιών υπολογιστικού νέφους και τα κακόβουλα άτομα θα πρέπει να αποτρέπονται από την πρόσβαση σε αυτές τις πληροφορίες. Σε αυτή την προσέγγιση, η ομάδα χρηστών θα πρέπει να αναπτύξει και να εφαρμόσει την πολιτική ασφάλειας, η οποία θα πρέπει να είναι ανεξάρτητη από τη διαχείριση ενός *cloud ISP*(*Independent Software Provider*). Παρομοίως, η ομάδα χρηστών, η οποία είναι ανεξάρτητη από τον *ISP*, θα πρέπει να είναι υπεύθυνη για την εσωτερική επικοινωνία.
- Εξωτερική επισκεψιμότητα: Κατά τη διάρκεια αυτής της μορφής επικοινωνίας, το *VM* συνδέεται με άλλες ομάδες χρηστών που φιλοξενούνται είτε από τον ίδιο πάροχο *cloud* είτε μέσω του διαδικτύου. Αυτός είναι ο τρόπος με τον οποίο οι ομάδες χρηστών επικοινωνούν μεταξύ τους. Η διαχείριση και ο έλεγχος της κίνησης μεταξύ των ομάδων χρηστών γίνεται από τον πάροχο του νέφους. Αυτός δημιουργεί και επιβάλλει μια πολιτική ασφαλείας που είναι υπεύθυνη για τυχόν ζητήματα με την ασφάλεια της εξωτερικής κυκλοφορίας.

Τα ζητήματα ασφαλείας σε επίπεδο εικονικοποίησης, όπως η ασφάλεια υπερεπόπτη, η ασφάλεια εικονικού δικτύου, η εικονική αποθήκευση κ.λπ., αποτελούν σημαντικές απειλές ασφαλείας για το υπολογιστικό σύστημα *IaaS*. Παρακάτω γίνεται μια περιγραφή διαφόρων σημαντικών απειλών για την ασφάλεια αυτού του μοντέλου διάθεσης.

### *5.3.1 Malicious insiders*

*5.3.1.1 Περιγραφή επίθεσης*

Άλλες οντότητες που μπορεί να βρεθούν στη θέση των κακόβουλων επιτιθέμενων είναι οι κακόβουλοι πελάτες, οι κακόβουλοι πάροχοι/μεσίτες *cloud*, οι κακόβουλοι διαμεσολαβητές

και οι κακόβουλοι χρήστες. Όταν ένα άτομο, ένας υπάλληλος ή ένα μέλος του προσωπικού που γνωρίζει πώς λειτουργεί το σύστημα εμφυτεύει επιβλαβές λογισμικό για να βλάψει οτιδήποτε εμπίπτει στο σύστημα υπολογιστικού νέφους μιας εταιρίας, αυτός ο τύπος επίθεσης συμβαίνει από κακόβουλους εσωτερικούς χρήστες και η επίθεση θεωρείται ότι εξαπολύεται εντός του οργανισμού.

Ο κίνδυνος επιθέσεων από εσωτερικούς χρήστες είναι ευρέως γνωστός στον τομέα του υπολογιστικού νέφους. Λόγω της δυνατότητας λήψης πολλών κρίσιμων πληροφοριών από τα δεδομένα που τηρούνται στο νέφος, αυτή η απειλή είναι πολύ πιο επικίνδυνη σε μια ρύθμιση *cloud*.Οι εσωτερικές απειλές εξακολουθούν να αποτελούν σοβαρή ανησυχία. Ωστόσο, επειδή οι επιχειρήσεις συχνά επικεντρώνονται στους εξωτερικούς κινδύνους και όχι στις εσωτερικές ανησυχίες, αυτού του είδους οι κίνδυνοι δεν λαμβάνουν ιδιαίτερης προσοχής. Οι επιθέσεις εκ των έσω είναι συχνά προσχεδιασμένες. Η μελέτη των *Eric* και *Shaw* αποκάλυψε ότι οι δράστες επιθέσεων από εσωτερικές πηγές δεν έχουν κοινά δημογραφικά χαρακτηριστικά, ωστόσο υπάρχουν αρκετοί δείκτες κινδύνου (Nkosi et al., 2013).

*5.3.1.2 Αντίμετρα*

Επειδή οι εικονικές μηχανές σε μια*IaaS*υποδομή είναι ελαστικές, συχνά μπορούν να ανακατανεμηθούν σε άλλες εικονικές μηχανές ή και σε φυσικό εξοπλισμό. Ένας παραβιασμένος*hypervisor*, εισάγει νέους κινδύνους και τρωτά σημεία κατά τη διάρκεια αυτής της κίνησης. Τόσο το λειτουργικό σύστημα του επισκέπτη όσο και του υπερπιστωτή μπορεί να αναγνωρίσουν τη δραστηριότητα μυστικών πληροφοριών. Η έρευνα που έγινε από τους Khorshed et al. (2011), η οποία κάνει χρήση της μάθησης βάσει κανόνων, ήταν επιτυχής στον εντοπισμό των συμπεριφορών των επιτιθέμενων.

Στη δημοσίευσή τους το 2013, οι Nkosi et al. παρείχαν μια μέθοδο για τον εντοπισμό κακόβουλων χρηστών σε περιβάλλον *cloud*. Οι συγγραφείς απέδειξαν πώς τα πρότυπα συμπεριφοράς των κακόβουλων χρηστών μπορούν επίσης να χρησιμοποιηθούν για την αναγνώρισή τους. Προκειμένου να εντοπιστεί οποιαδήποτε επιβλαβής συμπεριφορά προτύπων για ένα συγκεκριμένο προφίλ, η μεθοδολογία τους χρησιμοποιεί την προσέγγιση διαδοχικής χαρτογράφησης. Ωστόσο, ολόκληρο το περιβάλλον *cloud* δεν μπορεί να είναι πλήρως ασφαλισμένο χρησιμοποιώντας αυτήν την τεχνική.

Με τη δημιουργία ενός γραφήματος τροποποίησης των εσωτερικών πληροφοριών, έχει γίνει μια προσπάθεια παρακολούθησής τους, με τα δεδομένα να προέρχονται από μια σχεσιακή βάση δεδομένων. Στην εργασία τους οι Yaseen&Panda (2010) εξέτασαν με αυτό τον τρόπο τους κινδύνους κακόβουλης αλλαγής από εμπιστευτικούς χρήστες. Μέσω αυτού του

γραφήματος, κατέστη δυνατό να παρακολουθούνται οι τροποποιήσεις από εμπιστευτικές πληροφορίες ώστε να καθοριστεί εάν είναι εγκεκριμένες ή παράνομες.

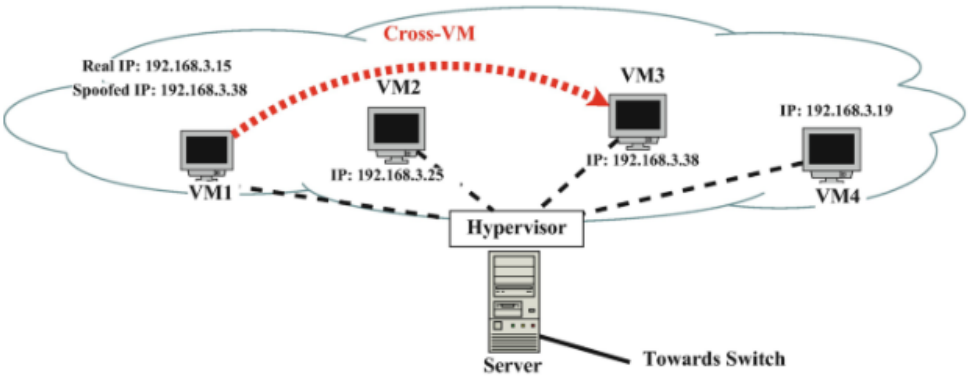
### *5.3.2 Επιθέσεων πλευρικών καναλιών (Cross VM Side-Channel Attacks)*

*5.3.2.1 Περιγραφή επίθεσης*

Οι επιθέσεις των πλευρικών καναλιών είναι μια απειλή που συχνά αγνοείται από το κρυπτογραφικό λογισμικό. Οι επιθέσεις αυτές χρησιμοποιούν πληροφορίες των πλευρικών καναλιών (*Cross VM Side-Channel*). Το ίδιο το κρυπτογραφικό πρόγραμμα χρησιμοποιείται για τη λήψη αυτών των δεδομένων, οι οποίες δεν είναι ούτε απλό (*plaintext*) ούτε κρυπτογραφημένο κείμενο (*ciphertext*). Ο κακός ενοικιαστής προσπαθεί να κλέψει τις πληροφορίες ζωτικής σημασίας των άλλων ενοικιαστών λόγω του κοινόχρηστου περιβάλλοντος στο υπολογιστικό νέφος. Οι επιθέσεις αυτές συχνά ακολουθούν τα παρακάτω δύο βήματα:

- **Τοποθέτηση**: ο επιτιθέμενος τοποθετείται στο ίδιο φυσικό μηχάνημα με το θύτη,
- **Εξαγωγή**: όταν το κακόβουλο λογισμικό εγκατασταθεί επιτυχώς στο εικονικό μηχάνημα /στόχος, εξάγονται από αυτό ιδιωτικά δεδομένα, αρχεία και έγγραφα.

Τα πλευρικά κανάλια είναι βασικά στοιχεία της ιδιότητας της πολλαπλής μίσθωσης (*multi-tenancy*)που χαρακτηρίζει το υπολογιστικό νέφος. Η εικονοποίηση επιτρέπει σε πολλές εικονικές μηχανές να συνυπάρχουν στον ίδιο φυσικό υπολογιστή (Xiao & Xiao, 2013) Λόγω της κοινόχρηστης υποδομής *cloud*, τα κανάλια χρονισμού ενδέχεται να τερματιστούν ανά πάσα στιγμή και οι κακοί χρήστες που βρίσκονται στην ίδια υποδομή ενδέχεται να μπορούν να κλέψουν ευαίσθητες πληροφορίες από άλλους νόμιμους χρήστες. Λόγω των κοινών εικονικών και φυσικών πόρων, οι προσεγγίσεις *VM* επιτρέπουν στους εισβολείς να αναλαμβάνουν επιθέσεις χρονισμού και επιθέσεις πλευρικών καναλιών εκμεταλλευόμενοι τον θεμελιώδη σχεδιασμό των εικονικών μηχανών (Xiao & Xiao, 2013).




***Εικόνα 22**: Επιθέσεις πλευρικών καναλιών*
**Πηγή**: Singh&Somani, 2018

Τα τρωτά σημεία που ανακαλύφθηκαν στα συστήματα *cloud* αποτέλεσαν αντικείμενο έρευνας από τους Godfrey&Zulkernine (2013). Η πιθανότητα παραβιάσεων των δεδομένων μιας εικονικής μηχανής μέσω ενός πλευρικού καναλιού είναι η πιο διαδεδομένη ευπάθεια σε ένα εικονικό περιβάλλον υπολογιστικού νέφους. Λόγω της ικανότητας του σύννεφου να διαμοιράζεται τους πόρους, αυτού του τύπου οι επιθέσεις είναι πολύ σοβαρές απειλές. Οι επιθέσεις που βασίζονται στην κρυφή μνήμη είναι οι πιο διαδεδομένες από αυτές. Σε αυτή την επίθεση τόσο ο κεντρικός υπολογιστής όσο και ο υπολογιστής επισκέπτη επηρεάζονται από τους κινδύνους του πλευρικού καναλιού. Το ζήτημα της βελτιωμένης χρήσης των πόρων προκύπτει από αυτή την επίθεση (Yu et al., 2013).

*5.3.2.2 Αντίμετρα*

Στην εργασία τους το 2011, οι Shi et al. ανέπτυξαν μια τεχνική που λάμβανε υπόψη το δυναμικό χρωματισμό της κρυφής μνήμης. Κατά την εκτέλεση των διαδικασιών που απαιτούν υψηλό επίπεδο ασφάλειας, το *VMM* χρησιμεύει ως σημείο για τη μεταφορά των δεδομένων σε μια πιο ασφαλή και απομονωμένη γραμμή. Ωστόσο, αυτές οι τεχνικές ενδέχεται να προσθέτουν επιβάρυνση και δεν είναι πρακτικές για εμπορικές εφαρμογές που βασίζονται στο νέφος. Επιπλέον, οι λύσεις τους πρέπει να ελέγχονται σε διαφορετικά εικονικά περιβάλλοντα, όπως πίνακες εκτεταμένων σελίδων και πίνακες στοιβαγμένων σελίδων.

Μια τεχνική για την καθιέρωση της απομόνωσης δικτύου μέσω μιας αρχιτεκτονικής φιλοξενίας υπολογιστικού νέφους ονομάζεται *SilverLine* (Mundada et al., 2011). Αυτή η στρατηγική επιδιώκει να ελέγξει και να σταματήσει τυχόν διαρροές δεδομένων. Οι συγγραφείς γνωρίζουν την αποτελεσματικότητα των τρεχόντων μηχανισμών ελέγχου ροής πληροφοριών που προκαλούνται από επιθέσεις πλευρικού καναλιού και σφάλματα διαμόρφωσης. Η ασφάλεια από την πλευρά του διακομιστή είναι η κύρια έμφαση αυτής της στρατηγικής ενώ η διαρροή του προγράμματος περιήγησης Ιστού δεν λαμβάνεται υπόψη.

Η αποκάλυψη μνήμης είναι ένα διαφορετικό είδος επίθεσης *Cross-VM* (Xiao and Xiao, 2013). Μέσω της αφαίρεσης της μνήμης, οι τεχνολογίες εικονικοποίησης επιτρέπουν τη χαμηλότερη κατανάλωση φυσικής μνήμης. Σε όλη αυτή τη λειτουργία ανταλλάσσονται σελίδες μνήμης με το ίδιο περιεχόμενο. Συγκρίνοντας τους χρόνους πρόσβασης των ίδιων σελίδων σε μια συνοικία εικονικών μηχανών, είναι δυνατό να εντοπιστεί η παρουσία μιας εφαρμογής ή αρχείων που έχουν προγραμματιστεί για να εξαπολύσουν μια τέτοια επίθεση (Harnik et al., 2010).

Η αφαίρεση της μνήμης είναι επίσης επιρρεπής σε επιθέσεις πλευρικών καναλιών (Suzaki, 2012). Για το ελάττωμα αυτό ευθύνεται η αφαίρεση της μνήμης *Copy-On-Write*. Το

*Copy-On-Write* είναι μια ευρέως χρησιμοποιούμενη μέθοδος ελέγχου κοινόχρηστων δεδομένων, ωστόσο αυτή η πρακτική έχει μετατραπεί σε κρυφό κανάλι διαρροής πληροφοριών. Η αφαίρεση της αφήνει ανοιχτές τις εικονικές μηχανές σε επιθέσεις πλευρικών καναλιών και διαρροών πληροφοριών Αυτές οι επιθέσεις θέτουν σε κίνδυνο και τα φυσικά χαρακτηριστικά του υλικού, όπως τα πρότυπα πρόσβασης της *CPU* και της μνήμης, στα οποία οι επιτιθέμενοι στοχεύουν προκειμένου να έχουν πρόσβαση και να ελέγχουν τις πληροφορίες όλου του διακομιστή. Για να ελαχιστοποιηθεί ο κίνδυνος επίθεσης πλευρικού καναλιού, το βασικότερο αντίμετρο θα ήταν να διαχωριστούν οι χρήστες σε διαφορετικούς φυσικούς υπολογιστές γεγονός που αυτοαναιρεί τον ορισμό του υπολογιστικού νέφους (Scarfone, 2011).

### *5.3.3 Επιθέσεις επαναφοράς εικονικής μηχανής (VM Roll back Attacks)*

*5.3.3.1 Περιγραφή επίθεσης*

Εάν παρουσιαστεί κάποιο πρόβλημα, τα *VM* είναι προγραμματισμένα να μπορούν να επανέλθουν στην αρχική τους κατάσταση. Δυστυχώς, αυτή η ενέργεια μπορεί για άλλη μια φορά να τα εκθέσει σε ελαττώματα ασφαλείας, καθιστώντας τους εισβολείς που στοχεύουν στον ευάλωτο υπερεπόπτη, σε πλεονεκτική θέση. Η προστασία δεδομένων είναι ζωτικής σημασίας κατά τη μεταφορά. Στην πραγματικότητα, αυτός είναι ο τρόπος με τον οποίο προστατεύεται το απόρρητο και η ακεραιότητα των δεδομένων κατά τη μετεγκατάστασή τους. Η πλαστογράφηση και οι επιθέσεις «*man-in-the-middle*» είναι μεταξύ των κινδύνων κατά τη μετανάστευση.

*5.3.3.2 Αντίμετρα*

Οι Xia et al. (2012) πρότειναν ένα σύστημα όπου οι χρήστες θα συνδέονται με ασφάλεια σε όλες τις λειτουργίες αναστολής/συνέχισης και μετεγκατάστασης εντός ενός αξιόπιστου τομέα υπολογιστών προκειμένου να επιτευχθεί μια ισορροπία μεταξύ της ασφάλειας και της λειτουργικότητας. Οι χρήστες έχουν έναν μηχανισμό ελέγχου του αρχείου καταγραφής προκειμένου να εντοπίζουν δόλιες επαναλήψεις και να περιορίζουν τις λειτουργίες στις εικονικές μηχανές. Αυτή η μέθοδος προσφέρει μια τεχνική για την αποτροπή της πρόσβασης ατόμων σε αυτές, μέσω των παραβιασμένων *hypervisors*.

Τα ξεπερασμένα συστήματα είναι επιρρεπή σε επιθέσεις επαναφοράς, καθώς είναι δύσκολο να γίνει διάκριση μεταξύ των δραστηριοτήτων επαναφοράς ρουτίνας/αναστολής και μετεγκατάστασης σε ξεπερασμένες πλατφόρμες *IaaS*. Στο παρελθόν, τα συστήματα απλώς απενεργοποιούσαν όλες αυτές τις λειτουργίες για να προστατευτούν από αυτού του τύπου τις επιθέσεις ή απαιτούσαν συνεχή ανατροφοδότηση από τον πελάτη σε κάθε βήμα της μετεγκατάστασης.

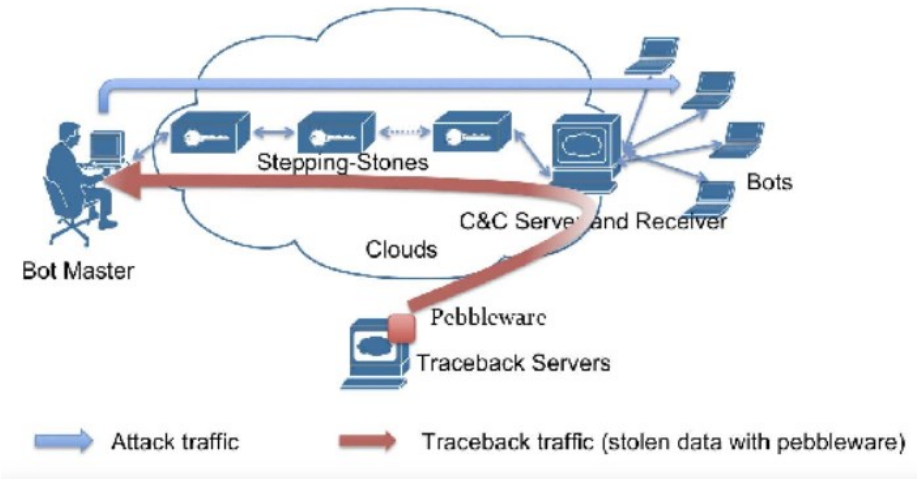
Η μελέτη των Fiebig et al. (2013) προσφέρει μια εναλλακτική μέθοδο για τον εντοπισμό της ζωντανής μετανάστευσης ενός *VM*. Η στρατηγική τους βασίζεται στην τεχνική υβριδικής ανίχνευσης, η οποία χρησιμοποιεί το πρωτόκολλο χρονισμού του δικτύου και το *ICMP*(*Internet Control Message Protocol*) πρωτόκολλο για την αξιολόγηση των καθυστερήσεων προκειμένου να προσδιοριστεί αν η ζωντανή μετανάστευση μιας εικονικής μηχανής αναπτύσσεται όπως αναμένεται. Ωστόσο, οι συγγραφείς δεν ολοκλήρωσαν τις ιδέες τους σε ρυθμίσεις ζωντανού υπολογιστικού νέφους, παρά μόνο προσέφεραν απλώς το πρωτότυπο. Για την ανάπτυξη πιο προηγμένων συστημάτων παρακολούθησης, είναι απαραίτητο να δοκιμαστεί το πρωτότυπό τους έναντι διαφόρων τύπων διακομιστών, όπως διακομιστές βίντεο ή διακομιστές εφαρμογών Ιστού.

### *5.3.4 Επιθέσεις από δίκτυο ρομπότ (Botnet Attacks / Stepping-Stone Attack)*

*5.3.4.1 Περιγραφή επίθεσης*

Οι χρήστες μπορούν να εγκαταστήσουν το δικό τους λειτουργικό σύστημα και τις εφαρμογές χρησιμοποιώντας τα *VM* που τους διαθέτει ο πάροχος. Λόγω δευτερευουσών επιδιορθώσεων ασφαλείας, οι εικονικές μηχανές ενδέχεται να περιέχουν ορισμένα ζητήματα. Οι επιτιθέμενοι χρησιμοποιούν προηγουμένως παραβιασμένα *VM*s,του *IaaS* μοντέλου διάθεσης, ως ενδιάμεσους κεντρικούς υπολογιστές αντί να επιτίθενται από τον δικό τους υπολογιστή σε αυτού του τύπου τις επιθέσεις. Οι επιθέσεις μπορούν να πραγματοποιηθούν εφόσον οι εικονικές μηχανές της *IaaS* πλατφόρμας έχουν μολυνθεί. Όταν ο εισβολέας χρησιμοποιεί μια ενδιάμεση επίθεση από έναν εσωτερικό οικοδεσπότη, οι πάροχοι υπηρεσιών είναι υπεύθυνοι και θύματα ταυτόχρονα. Στην υποδομή IaaS, οι ενδιάμεσες επιθέσεις που χρησιμοποιούν φιλοξενούμενα *VM* είναι ζωτικής σημασίας.

Αυτές οι επιθέσεις χρησιμοποιούν παραβιασμένες εικονικές μηχανές στοχεύοντας κυρίως εξωτερικούς κεντρικούς υπολογιστές. Υπό αυτή την έννοια, οι πάροχοι υπηρεσιών *IaaS* μπορεί επίσης να θεωρηθούν εισβολείς. Το σύννεφο *IaaS* θα πρέπει να προσφέρει μια προληπτική άμυνα έναντι αυτού του είδους των επιθέσεων, προκειμένου να διαφυλαχθεί αυτό το σενάριο. Τα τείχη προστασίας μπορούν μόνο να προστατεύσουν τα δεδομένα που περιλαμβάνονται στα πακέτα δικτύου, καθιστώντας εξαιρετικά δύσκολη την άμυνα έναντι ορισμένων μορφών επιθέσεων που τα χρησιμοποιούν (Kourai et al., 2012).




***Εικόνα 23**:Botnet attack*
**Πηγή**: Lin & Lee, 2012

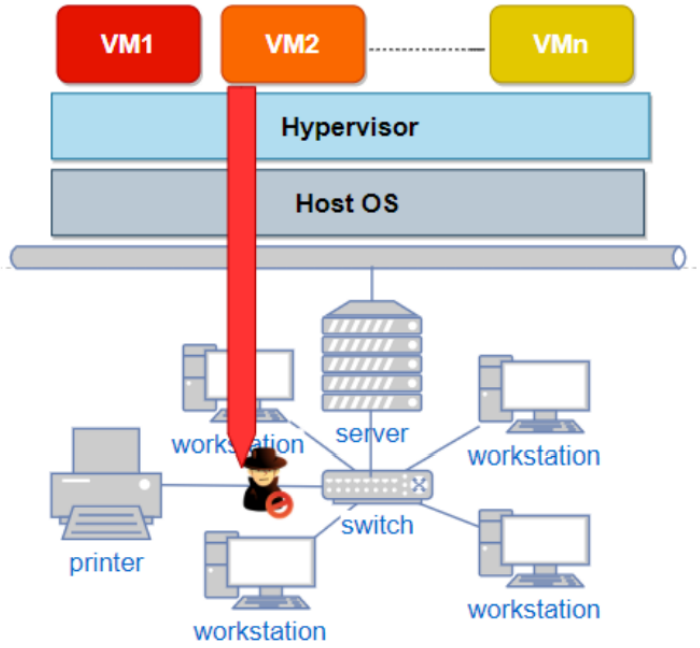
*5.3.4.2 Αντίμετρα*

Οι πάροχοι *cloud* θα πρέπει να θέσουν σε εφαρμογή κάποιου είδους ελέγχου για τον εντοπισμό των *botnets*, τη διακοπή τους και την παρακολούθηση του *bot master* (Kourai et al., 2012). Η τεχνική *Pebble trace* που προσδιορίζει τον *bot master* προτάθηκε στο έργο των Lin και Lee (2012). Προκειμένου να εντοπιστεί η *botnet* δραστηριότητα, αυτή η προσέγγιση βρίσκει πρώτα τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται για την *botnet* επικοινωνία πριν εντοπίσει αυτά τα κλειδιά πίσω στο *bot master*. Αυτή η καινοτόμος μέθοδος εντοπίζει τον *bot master* χωρίς την ανάγκη οθονών, αναβαθμίσεων δρομολογητή, βοήθειας από τον *ISP* σε όλες τις βάσεις ή τις διάφορες πλατφόρμες του υπολογιστικού νέφους.

### *5.3.5 Διαφυγή VM (VM escape)*

*5.3.5.1 Περιγραφή*

Υπάρχουν συχνά μερικές μη προνομιούχες εικονικές μηχανές και ένα προνομιακό *VM* στην αρχιτεκτονική εικονικοποίησης του νέφους. Μια επίθεση που αυξάνει τα προνόμια σε μια μη προνομιούχα εικονική μηχανή ονομάζεται *VMescape*. Σε αυτήν τη λειτουργία, η τιμή *Boolean* του *hypervisor* καθορίζει εάν παραχωρούνται ή όχι επιπλέον δικαιώματα στην εικονική μηχανή. Ο εισβολέας μπορεί να καταστρέψει το μολυσμένο *VM* αφού αυξήσει τα προνόμιά του για να εκτελέσει διάφορες άλλες κακόβουλες ενέργειες.




***Εικόνα 24**:VM escape*
**Πηγή**:Abusaimeh, 2020

*5.3.5.2 Αντίμετρα*

Οι λειτουργίες *libc* (Ding et al., 2012) περιορίζουν τις δυνατότητες αυτών των επιθέσεων. Σε αυτού του είδους τις επιθέσεις, οι δράστες καταβάλλουν προσπάθεια να παραβιάσουν το λειτουργικό σύστημα του επισκέπτη για να αποκτήσουν πρόσβαση στον υπερεπόπτη ή για να αποκτήσουν πρόσβαση στις περαιτέρω δυνατότητες των φιλοξενούμενων λειτουργικών συστημάτων και του υποκείμενου λειτουργικού συστήματος υποδοχής.

Escape είναι ο όρος που αναφέρεται σε αυτό το σπάσιμο μεταξύ του φιλοξενούμενου και του υποκείμενου λειτουργικού συστήματος (*guestOS*). Εάν οι επιτιθέμενοι καταφέρουν να αποκτήσουν παράνομη πρόσβαση στο λειτουργικό σύστημα του επισκέπτη αποκτώντας τον πλήρη έλεγχό του, ενδέχεται να θέσουν σε κίνδυνο τον *hypervisor*. Με αυτόν τον τρόπο, ένα μόνο τρωτό σημείο της ασφάλειας του υπερεπόπτη μπορεί να σταματήσει ολόκληρη την λειτουργία του (Scarfone, 2011). Η εικονική μηχανή που εκτελείται στο φυσικό μηχάνημα μπορεί να τροποποιηθεί με οποιονδήποτε τρόπο, εάν ο εισβολέας έχει τον έλεγχο του *hypervisor*. Ο κακόβουλος κώδικας που είναι γνωστός ως «*Escape the VM*»μπορεί να επηρεάσει όχι μόνο τον υπερεπόπτη αλλά και τις άλλες φιλοξενούμενες εικονικές μηχανές. Ως εκ τούτου, είναι σημαντικό να ερευνηθεί η καλύτερη στρατηγική για την άμυνα έναντι αυτών των επιθέσεων (You et al., 2012).

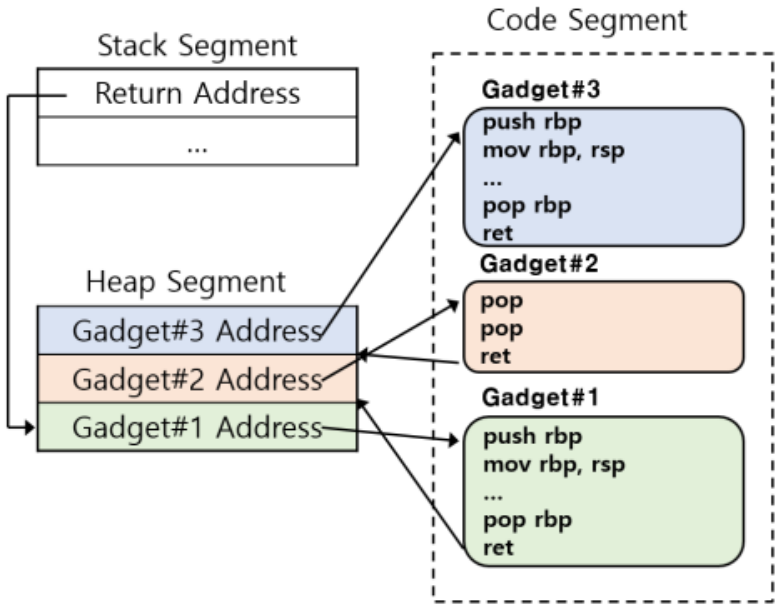
Ένα πρόγραμμα που εκτελείται σε μια εικονική μηχανή δεν μπορεί να παρατηρεί ή να παρεμβαίνει σε ένα πρόγραμμα που εκτελείται σε μια άλλη εικονική μηχανή ή στο κεντρικό

σύστημα. Ωστόσο, στην πράξη, οι εταιρείες υπονομεύουν την απομόνωση και εισάγουν νέα ελαττωματικά λογισμικά που κάνουν ακριβώς αυτό. Ως αποτέλεσμα αυτών των επιθέσεων, ολόκληρο το περιβάλλον είναι ευάλωτο. Η σωστή ρύθμιση των επισκεπτών υπολογιστών είναι απλώς μια προσέγγιση μετριασμού της επίθεσης.

### *5.3.6 Return oriented programming attack*

*5.3.6.1 Περιγραφή*

Οι υπερχειλίσεις *buffer* είναι μια καταστροφική στρατηγική επίθεσης με σοβαρές επιπτώσεις για την αξιοπιστία και τη συνεπή απόδοση μιας εφαρμογής. Αυτή η στρατηγική επεκτάθηκε στον προγραμματισμό προσανατολισμένο στην επιστροφή (*ROP: Return-Oriented Programming*)ο οποίος εκτελούσε διάφορες δραστηριότητες συνδέοντας μικρές ακολουθίες εντολών που καταλήγουν σε μια εντολή ret γνωστή ως gadgets. Με αυτήν την επίθεση, η ροή ελέγχου εκτρέπεται σε ένα εκτελέσιμο τμήμα κώδικα βιβλιοθήκης, το οποίο δεν ήταν ο επιδιωκόμενος προορισμός όπως απεικονίζεται στην παρακάτω εικόνα (Yun et al., 2020):




*Εικόνα 25: Επίθεση προγραμματισμού προσανατολισμένου στην επιστροφή*
**Πηγή**:Yun et al., 2020

Η επίθεση προγραμματισμού προσανατολισμένη στην επιστροφή ξεκίνησε να μελετάται από τους συγγραφείς Ding et al. το 2012. Αυτή η επίθεση χρησιμοποιεί τον υπάρχοντα κώδικα ενός *hypervisor* για την ενημέρωση του προνομιούχου πεδίου χωρίς την αλλαγή οποιουδήποτε άλλου κώδικα. Χρησιμοποιώντας προσεγγίσεις προγραμματισμού προσανατολισμένες στην επιστροφή, ο εισβολέας εξακολουθεί να τροποποιεί κακόβουλα τα δεδομένα ελέγχου του *hypervisor*(Iqbal et al., 2016).

*5.3.6.2 Αντίμετρα*

Έχουν προταθεί πολυάριθμες άμυνες έναντι επιθέσεων επαναχρησιμοποίησης κώδικα. Πρώτα απ 'όλα, η ακεραιότητα ροής ελέγχου (*CFI: Control-Flow Integrity*) διασφαλίζει ότι η ροή ελέγχου ενός προγράμματος ακολουθεί μια αναμενόμενη διαδρομή σύμφωνα με το γράφημα ροής ελέγχου της εφαρμογής. Οποιαδήποτε προσπάθεια από έναν εισβολέα να ελέγξει τη ροή ελέγχου κατά το χρόνο εκτέλεσης εντοπίζεται ως πειρατεία και διακόπτεται. Κάθε εντολή κλήσης και επιστροφής υλοποιείται στο χρόνο εκτέλεσης σε μια σκιώδη στοίβα, με τον τρόπο που υποδεικνύει το *CFI*. Αν και ο μηχανισμός αυτός προσφέρει μια ξεκάθαρη άμυνα και δεν απαιτεί τον πηγαίο κώδικα μιας εφαρμογής, έχει ορισμένα πρακτικά μειονεκτήματα, όπως μια μέση επιβάρυνση απόδοσης κατά 21%.

Σε άλλες προτάσεις η διάταξη της μνήμης μιας διεργασίας επανατυχαιοποιείται κατά τη σειρά των χιλιοστών του δευτερολέπτου χρησιμοποιώντας τεχνικές τυχαιοποίησης χρόνου εκτέλεσης όπως το *TASR* και το *Shuffler*, σε μια προσπάθεια να καταστούν αναχρονιστικές οι αποκαλύψεις της μνήμης.

Μια άλλη γραμμή άμυνας εστιάζει στην παρεμπόδιση της επαναλαμβανόμενης συγκομιδής εργαλείων. Ο πραγματικός προορισμός των εντολών κλήσης μπορεί να είναι κρυμμένος από έναν μη προσβάσιμο πίνακα, με τυχαιποιημένη τη σειρά με την οποία εκτελέστηκαν τα προγράμματα. Μια άλλη προστασία θα ήταν η χρήση μιας μνήμης μόνο για εκτέλεση, είτε μέσω εξομοίωσης λογισμικού είτε μέσω ενός προσαρμοσμένου υπερεπόπτη. Τέλος, μια άλλη λύση είναι να ξαναγράφονται δυνητικά ευαίσθητα δυαδικά αρχεία λογισμικού σε χρονομορφικά δυαδικά αρχεία χρησιμοποιώντας τεχνολογία αυτο-τροποποίησης κώδικα (*SMC: Self-Modifying Code*) (Yun et al., 2020).

### *5.3.7 Επίθεση κλοπής υπηρεσίας (Theft of Service Attacks)*

*5.3.7.1 Περιγραφή επίθεσης*

Αυτού του τύπου οι επιθέσεις εκμεταλλεύονται τα τρωτά σημεία στον προγραμματισμό ορισμένων υπερπιστωτών (Zhou et al., 2011). Η επίθεση καθίσταται δυνατή όταν ο αλγόριθμος του υπερεπόπτη δεν είναι σε θέση να αναγνωρίσει και να λάβει υπόψη τη χρήση της Κεντρικής Μονάδας Επεξεργασίας (*CPU: Central Processing Unit*) από απείθαρχες εικονικές μηχανές. Αυτό το σφάλμα θα μπορούσε να επιτρέψει σε κακούς χρήστες να αποκτήσουν υπηρεσίες *cloud* εις βάρος άλλων χρηστών. Αυτή η εκμετάλλευση είναι πιο συχνή στα δημόσια σύννεφα, επειδή οι χρήστες χρεώνονται με βάση τη διάρκεια λειτουργίας των εικονικών μηχανών τους και όχι με βάση τον χρόνο που καταναλώνουν *CPU* πόρους (Khalil et al, 2014).

Τα ελαττώματα που μπορεί να οδηγήσουν σε αυτή την ευπάθεια προκαλούνται κυρίως από τη χρήση ρολογιών χαμηλής ακρίβειας ή την περιοδική δειγματοληψία για την παρακολούθηση της χρήσης της *CPU*, η οποία στην επίθεση αυτή μοιάζει με επιβάτη τρένου που κρύβεται κάθε φορά που οι επιθεωρητές εισιτηρίων πλησιάζουν για να επαληθεύσουν τα εισιτήρια. Οι κυβερνοεγκληματίες διασφαλίζουν ότι η διαδικασία του ελέγχου δεν έχει προγραμματιστεί ποτέ όταν λαμβάνει χώρα μια επίθεση κλοπής υπηρεσίας. Τα πιο συχνά περιστατικά αυτής της επίθεσης περιλαμβάνουν (Khalil et al, 2014):

- Χρήση υπηρεσιών υπολογιστικού νέφους για μεγάλο χρονικό διάστημα, κρατώντας το κρυφό από τον πάροχο και
- Χρήση πόρων υπολογιστικού νέφους για παρατεταμένη χρονική περίοδο χωρίς να εμπεριέχεται σε κάποιον κύκλο τιμολόγησης.

*5.3.7.2 Αντίμετρα*

Οι Zhou et al. μελέτησαν και τεκμηρίωσαν μια άμυνα έναντι αυτής της επίθεσης (2011), με τροποποίηση του προγραμματιστή για να αποτραπεί η επίθεση χωρίς να θυσιαστεί η αποτελεσματικότητα, ή η απόκριση εισόδου/εξόδου(*Input*/*Output*). Οι θεμελιώδεις μέθοδοι για την ενίσχυση της πίστωσης και της προτεραιότητας δεν επηρεάζονται από αυτές τις αλλαγές. Υπάρχουν τέσσερις τροποποιημένοι χρονοπρογραμματιστές: ο ακριβής χρονοπρογραμματιστής, ο ομοιόμορφος χρονοπρογραμματιστής, ο προγραμματιστής πάθους και ο προγραμματιστής Bernoulli. Οι βασικές διακρίσεις μεταξύ αυτών των προγραμματισμών αφορούν στις στρατηγικές προγραμματισμού και παρακολούθησης καθώς και στους υπολογισμούς των χρονικών διαστημάτων. Το πείραμα που έτρεξαν οι συγγραφείς χρησιμοποιώντας τους επανασχεδιασμένους προγραμματιστές προσφέρει, εν τέλει, ακριβή και δίκαιο προγραμματισμό(Khalil et al, 2014).

Μια ακόμη θεωρητική προσέγγιση παρέχεται από τους Gruschka&Jensen(2010). Οι οποίοι προτείνουν τη χρήση μιας νέας διεπαφής στο μηχάνημα του θύματος για την παρακολούθηση του προγραμματισμού των παράλληλων παρουσιών. Στη συνέχεια, γίνεται σύγκριση των συνολικών αποτελεσμάτων και των νόμιμων περιπτώσεων. Μια σημαντική διαφορά στα αποτελέσματα αναφέρεται στις αρμόδιες αρχές ως επίθεση. Δεν υπάρχει καμία διαβεβαίωση ότι η χρήση αυτής της λύσης θα έχει θετικό αποτέλεσμα, επειδή δεν έχει ελεγχθεί ή επιβεβαιωθεί από τους συγγραφείς(Khalil et al, 2014).

### *5.3.8 Επιθέσεις ακουστικής στεγανογραφίας (Audio Steganography Attacks)*

*5.3.8.1 Περιγραφή επίθεσης*

Μία από τις πιο επικίνδυνες επιθέσεις σε συστήματα αποθήκευσης υπολογιστικού νέφους είναι η ακουστική στεγανογραφία[10]. Οι χρήστες μπορούν να χρησιμοποιήσουν στεγανογραφία ήχου για να αποκρύψουν ευαίσθητες πληροφορίες μέσα σε κοινά αρχεία ήχου. Ο επιτιθέμενος αποστέλλει αρχεία πολυμέσων που φαίνονται να είναι κανονικά αρχεία ήχου για να επικοινωνήσει τις κρυφές πληροφορίες. Εσωκλείοντας τον επιβλαβή κώδικά τους σε αρχεία ήχου και μεταφέροντάς τον στους διακομιστές των στόχων τους, οι κυβερνοεγκληματίες χρησιμοποιούν αυτή την εξελιγμένη τεχνική για να ξεπεράσουν τα τρέχοντα μέτρα ασφαλείας ή τα συμβατικά αντίμετρα, όπως η *Steganalysis*[11],που εφαρμόζεται για τη φύλαξη των συστημάτων αποθήκευσης στο υπολογιστικό νέφος(Khalil et al, 2014; Tupakula et al., 2011).


***Εικόνα 26**: Επίθεση ακουστικής στενογραφίας στο υπολογιστικό νέφος*
**Πηγή**: Shiu et al., 2017

*5.3.8.2 Αντίμετρα*

Μια διεξοδική διερεύνηση της επίθεσης ακουστικής στεναγογραφίας στα συστήματα αποθήκευσης του υπολογιστικού νέφους γίνεται από τους Liu et al. (Szefer and Lee, 2012). Για να καταπολεμήσουν τον κίνδυνο διαρροής δεδομένων που προκαλείται από επιθέσεις τέτοιου τύπου, ανέπτυξαν και εφάρμοσαν ένα σύστημα που ονομάζεται *StegAD* (*Steganography Active Defense*). Το αρχικό βήμα σε αυτήν την τεχνική είναι η χρήση του γνωστού αλγόριθμου ανάλυσης *steg* κλίμακας γκρι εικόνας *RS* για τον εντοπισμό των

[10]Η στεγανογραφία είναι μια από τις δημοφιλείς μεθόδους για την επίτευξη μυστικής επικοινωνίας μεταξύ αποστολέα και παραλήπτη με την απόκρυψη μηνύματος σε οποιαδήποτε μορφή μέσου κάλυψης όπως ήχος, βίντεο, κείμενο, εικόνες κ.λπ. (Gopalakrishnan Nair., 2012).

[11] Η στεγανάλυση είναι η μελέτη της ανίχνευσης μηνυμάτων που κρύβονται χρησιμοποιώντας στεγανογραφία. Είναι ανάλογη με την κρυπτοανάλυση που εφαρμόζεται στην κρυπτογραφία (Πηγή: https://en.wikipedia.org/wiki/Steganalysis).

κρυμμένων αρχείων ήχου μέσα στο σύστημα αποθήκευσης του νέφους. Οι συγγραφείς χρησιμοποιούν την προσέγγιση *SADI* (*Steganography Audio Dynamical Interference*) για να παρεμβαίνουν σε όλες τις πιθανές τοποθεσίες τέτοιων ύποπτων αρχείων μετά τη συλλογή τους. Οι συντάκτες χρησιμοποιούν μια στρατηγική που απαιτεί οι παρεμβολές να βρίσκονται σε πολλές κρυψώνες ή στις πιο σημαντικές τοποθεσίες σε μια προσπάθεια να αποτρέψουν την καταστροφή αθώων αρχείων, τα οποία έχουν επισημανθεί ως ύποπτα κατά τη διαδικασία της σάρωσης. Στην πρότασή τους, αντικαθιστούν πρώτα τις πιο σημαντικές πληροφορίες με τυχαίο θόρυβο πριν συγκρίνουν τις προηγουμένως αναλλοίωτες πληροφορίες με τις νέες πληροφορίες. Ανάλογα με τα αποτελέσματα της σύγκρισης, θα είναι δυνατό να διαπιστωθεί εάν το αρχείο ήχου περιέχει αθώο υλικό ή επιβλαβή κώδικα που μπορεί να βλάψει το σύστημα αποθήκευσης του νέφους(Khalil et al, 2014).

Ο στόχος της μελέτης των Gopalakrishnan Nair (2012) ήταν η ανάπτυξη μιας ασφαλούς προσέγγισης στεγανογραφίας με ένα μοντέλο υψηλής αντοχής που χρησιμοποιεί γενετικούς αλγόριθμους. Μία από τις πιο αξιόπιστες μεθόδους στεγανάλυσης η οποία αναλύει τα *pixels* της εικόνας με στατιστικό τρόπο προκειμένου να βρει το κρυφό μήνυμα είναι η *RS*. Ωστόσο, οι πληροφορίες στις φωτογραφίες σε κλίμακα του γκρι προστατεύονται από αυτή τη στεγανάλυση. Προκειμένου να αμυνθούν ενάντια της επίθεσης σε έγχρωμες φωτογραφίες, ο Gopalakrishnan Nair παρείχε μια τεχνική στεγανογραφίας που χρησιμοποιεί εξελικτικούς αλγόριθμους. Η εφαρμογή των εξελικτικών γενετικών αλγορίθμων επιτρέπει τη βελτιστοποίηση της ασφάλειας και της ποιότητας της εικόνας. Ωστόσο, η πιθανότητα ανακάλυψης ενός μυστικού μηνύματος μέσω της ανάλυσης *RS* αυξάνεται καθώς μεγαλώνει το μήκος του κρυφού μηνύματος (Gopalakrishnan Nair., 2012).

## 5.4 Συνέπειες των επιθέσεων στο υπολογιστικό νέφος και στους τελικούς χρήστες

Στον παρακάτω πίνακα παρουσιάζονται οι επιπτώσεις καθεμιάς από της παραπάνω επιθέσεις που αναλύθηκαν, τόσο στους τελικούς χρήστες των υπηρεσιών όσο και στους πόρους και την πλατφόρμα του υπολογιστικού νέφους:

***Πίνακας 7**: Κατηγοριοποίηση του τύπου των επιθέσεων στο υπολογιστικό νέφος και οι συνέπειες αυτών*

| **Attack Name**<br>(Ονομασία επίθεσης) | **Consequences**<br>(Συνέπειες / Επιπτώσεις) | **Category**<br>(Κατηγορία) |
|---|---|---|
| **Theft-of-service** | Χρήση υπηρεσιών *cloud* χωρίς χρέωση.<br>Κλοπή πόρων στο cloud με λιγότερο/χωρίς κόστος | Cloud<br>Infrastructure |
| **Denial of service**<br>**DDoS** | Μη διαθεσιμότητα υπηρεσιών και υλικού (*hardware*). | Network,<br>Cloud |

| | | |
|---|---|---|
| | | Infrastructure |
| **Cloud malware injection** | Διαρροή πληροφοριών διαπιστευτηρίων.<br>Διαρροή δεδομένων χρηστών.<br>Μη φυσιολογική συμπεριφορά των μηχανών του*cloud*. | Cloud Infrastructure |
| **Cross VM side channels** | Διαρροή δεδομένων χρηστών και πληροφοριών.<br>Διαρροή πληροφοριών πόρων της *cloud* υποδομής. | Cloud Infrastructure |
| **Targeted shared memory** | Διαρροή πληροφοριών των πόρων του *cloud*.<br>Διαρροή πληροφοριών των χρηστών και των δεδομένων τους.<br>Παροχή ευπάθειας για άλλες επιθέσεις, όπως πλευρικά κανάλια και έγχυση κακόβουλου λογισμικού στο *cloud*. | Cloud Infrastructure |
| **Phishing** | Μη εξουσιοδοτημένη πρόσβαση σε προσωπικά στοιχεία.<br>Εγκατάσταση κακόβουλου κώδικα στους υπολογιστές των χρηστών.<br>Πρόκληση ασυνήθιστης συμπεριφοράς στη δομή του υπολογιστικού νέφους.<br>Μη διαθεσιμότητα των διακομιστών στους τελικούς χρήστες. | Cloud Infrastructure, Network, Access |
| **Botnets Stepping Stone attack** | Μη εξουσιοδοτημένη πρόσβαση σε πόρους του*cloud*.<br>Πρόκληση ασυνήθιστης συμπεριφοράς στο σύστημα του υπολογιστικού νέφους.<br>Κλοπή ευαίσθητων πληροφοριών.<br>Κλοπή δεδομένων χρήστη. | Network, Cloud Infrastructure, Access |
| **Audio Steganography** | Μη διαθεσιμότητα του συστήματος αποθήκευσης στο *cloud*.<br>Παράνομη πρόσβαση σε δεδομένα χρηστών.<br>Διαγραφή δεδομένων χρηστών. | Cloud Infrastructure, Access |
| **VM rollback attack** | Εκκίνηση επίθεσης ωμής βίας.<br>Βλάβη υποδομής στο cloud.<br>Διαρροή ευαίσθητων πληροφοριών. | Cloud Infrastructure, Access |

# 6. ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

## 6.1 Μηχανισμοί για την εξασφάλιση της ασφάλειας στο νέφος

Η ασφάλεια αποτελεί μείζον μέλημα για τα έργα της πληροφορικής και τις εμπορικές σχέσεις μεταξύ των εταίρων που διαμοιράζονται πόρους και υπηρεσίες στο νέφος. Παρακάτω παρατίθενται οι διάφοροι μηχανισμοί ασφαλείας που μπορούν να αναπτυχθούν για κάθε τύπο προβλημάτων ασφαλείας και τα ζητήματα ασφάλειας που προκύπτουν, όπως προτάθηκαν από τους Murala&Panda (2019):

### *6.1.1 Ζητήματα ασφάλειας της ενσωματωμένης υποδομήςκαι της εικονικοποίησης*

Ένα από τα προηγμένα χαρακτηριστικά που προσφέρει το *cloud computing* είναι η εικονικοποίηση. Η υιοθέτηση του *CC* επηρεάζεται σε μεγάλο βαθμό από αυτή την τεχνολογία. Χάρη σε αυτή, οι χρήστες στα περιβάλλοντα του νέφους έχουν πρόσθετα οφέλη, όμως εξαιτίας της προκύπτουν αρκετά ζητήματα ασφάλειας. Οι επιτιθέμενοι στοχεύουν στο να βλάψουν την υπηρεσία εικονικοποίησης πραγματοποιώντας μια ποικιλία επιθέσεων στο *cloud*. Ο παρακάτω πίνακας παραθέτει τις κύριες ανησυχίες για την ασφάλεια της ενσωματωμένης υποδομής και της εικονικοποίησης.

***Πίνακας 8****:Ζητήματα ασφάλειας ενσωματωμένης υποδομής και εικονικοποίησης*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Ενσωματωμένη υποδομή και εικονικοποίηση** | Απομόνωση *VM* | Διαρροή δεδομένων, επίθεση μέσω άλλης εικονικής μηχανής |
| | Διακομιστής απλού πρωτοκόλλου διαχείρισης δικτύου (*SNMP*) | Επισφαλείς ρυθμίσεις, μη ενημερωμένη έκδοση κώδικα προμηθευτή |
| | Παρακολούθηση *VM* | Μη αξιόπιστα μέρη *hypervisor*, λανθασμένες κατατμήσεις, διαφυγή *VM*, εσφαλμένη δρομολόγηση των αιτημάτων ανάλογα με την κίνηση στον *hypervisor*. |
| | Προγραμματισμός *VM* | Διαφυγή*VM*, επιθέσεις μεταξύ εικονικών μηχανών, επιθέσεις πλευρικών καναλιών, έγχυση κακόβουλου λογισμικού, προγραμματισμός εντροπίας, ασυνέπεια, αδυναμία επαναχρησιμοποίησης και επαναφοράς του*VM*. |

- **Απομόνωση *VM*:** Η θεμελιώδης άποψη της εικονικοποίησης είναι ένας περιορισμός. Ένα από τα βασικά προβλήματα με τη λειτουργία του *cloud* είναι ότι ο φόρτος εργασίας

κατανέμεται μεταξύ των εικονικών μηχανών. Από την βασική αυτή ιδιότητα ενδέχεται να προκύψει διαρροή δεδομένων και επιθέσεις μεταξύ των *VMs*. Έτσι, ακόμη και κατά την παράδοση μιας εικονικής μηχανής πίσω στην αρχιτεκτονική, η διαδικασία της αποσύνδεσής της θα πρέπει να καθοριστεί προσεκτικά.

- **Διακομιστής *SNMP* (*Simple Network Management Protocol*):**Πρόκειται για ένα Απλό Πρωτόκολλο Διαχείρισης Δικτύου που έχει σχεδιαστεί για να παρέχει ένα στοιχείο χαμηλής επιβάρυνσης για την απόκτηση δεδομένων από συσκευές τακτοποίησης.
- **Παρακολούθηση VM:** Στον εικονικό κόσμο, ο υπερεπόπτης θεωρείται ως σημείο ελέγχου και υποτίθεται ότι παρακολουθεί τις εφαρμογές που χρησιμοποιούνται από τις εικονικές μηχανές. Σε μια οθόνη απεικονίζονται όλα τα στατιστικά στοιχεία ανάπτυξης.
- **Προγραμματισμός VM**: Σε ένα περιβάλλον *cloud*, οι επαγγελματικοί μεταγωγείς χρησιμοποιούν βοήθεια από τα προγραμματιζόμενα πακέτα επεξεργαστών σε κάθε θύρα που αφορούν τη λογιστική, τον αποκλεισμό και την αποκάλυψη παρατυπιών.

### *6.1.2 Θέματα εμπιστοσύνης, συμμόρφωσης και νομικών πτυχών*

Στο υπολογιστικό νέφος, η εμπιστοσύνη, ένα μη μετρήσιμο χαρακτηριστικό που παίζει πολύ σημαντικό ρόλο. Ο κρίσιμος ενδιάμεσος κρίκος μεταξύ του πελάτη και του παρόχου υπηρεσιών στο επιχειρηματικό περιβάλλον του *cloud* είναι η διασφάλιση. Ο ρόλος του *SLA* στο επιχειρηματικό μοντέλο cloud είναι σημαντικός και ουσιαστικός και βοηθάει στην ενίσχυση της επικοινωνίας μεταξύ του πελάτη και του παρόχου υπηρεσιών. Κατά τη διάρκεια της συμφωνίας ενός *SLA*, όλα τα μέρη υποχρεούνται να ακολουθούν τους κανόνες και τις προσαρμογές που περιλαμβάνονται σε αυτό. Ο παρακάτω πίνακας παρακάτω παραθέτει τα βασικά προβλήματα της εμπιστοσύνης, της συμμόρφωσης και της νομικής σχέσης.

***Πίνακας 9**:Εμπιστοσύνη, συμμόρφωση και νομικές πτυχές του Cloud Computing*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Εμπιστοσύνη, συμμόρφωση και νομικές πτυχές** | Αξιόπιστα τρίτα μέρη | Θέση δεδομένων, τερματισμός, προστασία αξιοπιστίας, συμφωνία επιπέδου υπηρεσιών. |
| | Ανθρώπινος παράγοντας | Κοινή χρήση διαπιστευτηρίων σύνδεσης, phishing. |
| | Δικαστική αξία | Κατάσχεση δεδομένων, αποκάλυψη δεδομένων. |
| | Διασφάλιση της φήμης | Συμπεριφορά πελατών και απομόνωση φήμης. |

- **Αξιόπιστα τρίτα μέρη (*TTP: Trusted Third Party*):** Επειδή οι ιδιοκτήτες φάρμας διακομιστών ενδέχεται να κάνουν κατάχρηση των δεδομένων των πελατών, μιας και

οι χρήστες *cloud* δεν γνωρίζουν τη συνολική θέση της ασφάλειας των δεδομένων τους, ανησυχούν σε πολλές περιπτώσεις για τον τρόπο με τον οποίο με τον οποίο αυτά χρησιμοποιούνται. Ένα αξιόπιστο τρίτο μέρος μπορεί να επαληθεύσει, να επιβεβαιώσει και να εγκρίνει τις απαιτούμενες ενέργειες για τα δεδομένα, ενώ παρέχει ακλόνητη προστασία ποιότητας από μη εξουσιοδοτημένες προσβάσεις.

- **Ανθρώπινος παράγοντας:** Για να φωτιστεί το κομμάτι της ανθρώπινης συνιστώσας σχετικά με την ασφάλεια στο σύννεφο, θα πρέπει να γίνει αρχικά κατανοητό ότι ο άνθρωπος είναι η πηγή για τη δημιουργία πολλών ζητημάτων, από την άλλη όμως είναι ικανός να διαχειριστεί ένα μεγάλο αριθμό θεμάτων.
- **Δικαστική Αξία**: Καθώς διευρύνεται η χρήση των διαδικτυακών εφαρμογών και των συστημάτων, οι προηγμένες παρανομίες και τα κυβερνοεγκλήματα επεκτείνονται επίσης με παρόμοιο τρόπο. Οι ηλεκτρονικές νομικές επιστήμες αναλαμβάνουν θεμελιώδες ρόλο σε αυτό πλαίσιο και αποδεικνύονται αρκετά κατατοπισμένες για την εξερεύνηση του εγκλήματος στον κυβερνοχώρο και της αδικοπραγίας την οποία υποβοηθούν τα σύγχρονα ηλεκτρονικά μέσα. Οι ανησυχίες εστιάζονται στην κατάσχεση, την αποκάλυψη και στην πώληση των απόρρητων ή ευαίσθητων πληροφοριών.
- **Φήμη:** Η ταχεία ανάπτυξη των κατανεμημένων υπολογιστών έχει προκαλέσει αρκετές ανησυχίες. Μερικές εικονικές μηχανές εισάγονται σε ένα κατανεμημένο υπολογιστικό περιβάλλον και διαμοιράζονται συγκρίσιμο υλικό. Είναι ένα ζήτημα όταν η συμπεριφορά ενός πελάτη αλληλοεπιδρά με την ποιότητα των υπηρεσιών των υπολοίπων προκαλώντας αποδέσμευση της φήμης (*notoriety disengagement*). Η συμπεριφορά των πελατών και κυρίως των τελικών χρηστών των περισσότερων οργανισμών θα πρέπει να παρακολουθείται μιας και τα επιχειρηματικά συμφέροντα και η φήμη ενδέχεται να επηρεαστούν μέσα στο νέφος.

### *6.1.3 Ζητήματα ασφάλειας της αποθήκευσης των δεδομένων*

Σε ένα περιβάλλον που αναπτύσσεται στο νέφος, τα προβλήματα όσον αφορά στην ασφάλεια των αποθηκευμένων δεδομένων βρίσκονται στην κορυφή της λίστας των εμποδίων για την υιοθέτηση της εν λόγω τεχνολογίας. Οι κάτοχοι των δεδομένων δεν γνωρίζουν πόσο συχνά τα δεδομένα τους αποθηκεύονται στα υπολογιστικά κέντρα δεδομένων του νέφους και τι είδους μέτρα ασφαλείας χρησιμοποιούνται για να διασφαλιστεί ότι αυτά είναι ασφαλή. Ο παρακάτω πίνακας περιλαμβάνει μια λίστα με τους κύριους κινδύνους ασφαλείας που ενέχει αυτή η αποθήκευση.

*Πίνακας 10*:*Ζητήματα ασφάλειας αποθήκευσης δεδομένων Cloud*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Αποθήκευση δεδομένων στο cloud** | Επιλογή τρόπου αποθήκευσης των δεδομένων | Απώλεια ελέγχου, διαρροή των πληροφοριών, διαθεσιμότητα σε τρίτους, επεξεργασία για άλλους σκοπούς |
| | Διαθεσιμότητα των δεδομένων | Επίθεση DoS/DDoS, φυσικές καταστροφές |
| | Κρυπτογράφηση | Κακή διαχείριση κλειδιού, λανθασμένοι υπολογισμοί κρυπτογράφησης, διακοπές των υπηρεσιών |
| | Αποτροπή παραβιάσεις δεδομένων | *Cloud blackouts*, πολλαπλές τοποθεσίες αποθήκευσης |
| | Διασφάλιση της ακεραιότητας και της εμπιστευτικότητας | Κακή διαχείριση κλειδιού, λανθασμένοι υπολογισμοί κρυπτογράφησης, |
| | Αποτροπή εγκατάστασης κακόβουλου λογισμικού και δούρειων ίππων | Επίθεση από αφάνεια, επίθεση εκ των έσω. |

- **Αποθήκευση δεδομένων:** Οι αποθήκες δεδομένων είναι αρκετά ικανές να οργανώνουν και να αναλύουν διάφορους πληθυσμούς χρηστών καθώς και τις απαιτήσεις ασφαλείας τους. Η ασφάλεια των δεδομένων και των πληροφοριών είναι μια κρίσιμη αξίωση που πρέπει να εκπληρωθεί και να διατηρηθεί για την ανάπτυξη του υπολογιστικού νέφους.
- **Προσβασιμότητα:** Ο κύριος στόχος και ένα από τα βασικά πλεονεκτήματα του νέφους είναι η παροχή υψηλής προσβασιμότητας στον τελικό καταναλωτή. Οι πάροχοι αυτής της τεχνολογίας τονίζουν ότι οι πελάτες μπορούν να ταξιδέψουν οπουδήποτε ανά πάσα στιγμή και να έχουν πρόσβαση στα δεδομένα τους από οπουδήποτε στον κόσμο. Το προϊόν, οι πληροφορίες και ο εξοπλισμός δεν είναι προσβάσιμα από κανέναν άλλον μέχρι αυτά να ζητηθούν από τους εξουσιοδοτημένους χρήστες.
- **Κρυπτογραφία:** Πολλές κρυπτογραφικές συνθήκες φαίνεται να αποτυγχάνουν όταν εφαρμόζεται η συνοδευτική προσπάθεια της ασφάλειας. Η κρυπτογραφία νέφους έχει μια σειρά από εμπόδια που πρέπει να ξεπεραστούν. Η κακή οργάνωση των κλειδιών, η ανεπαρκής ακρίβεια του σχήματος κρυπτογράφησης και η διαχείριση πολύ συγκεκριμένων δεδομένων που σχετίζονται με αυτή την πρακτική είναι προβλήματα που απαντώνται συχνά.

- **Παραβίαση δεδομένων:** Η διαρροή των πληροφοριών μπορεί να προκύψει ως αποτέλεσμα των πολλαπλών αντιγράφων σε πολλές και διαφορετικές τοποθεσίες. Έχει άμεση επίδραση στην προσέγγιση του *SLA* και οδηγεί σε απώλεια της ασφάλειας και της εμπιστοσύνης.
- **Ζητήματα ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας**: Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι οι τρεις κύριες προκλήσεις ενός κατανεμημένου χώρου αποθήκευσης. Η ειλικρίνεια είναι το πιο θεμελιώδες στοιχείο ενός πλαισίου δεδομένων που προστατεύει τις πληροφορίες από μη εξουσιοδοτημένες αλλαγές, ανακλήσεις ή αλλαγές. Ζητήματα ασφαλείας προκύπτουν όταν επιβλαβείς παράμετροι ασφαλείας χαρακτηρίζονται εσφαλμένα ως μη ή όταν εικονικές μηχανές ή υπερπιστωτές έχουν σχεδιαστεί με εσφαλμένο τρόπο.
- **Κακόβουλο λογισμικό και δούρειοι ίπποι:** Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν το ηλεκτρονικό ψάρεμα για να μολύνουν τις εικονικές μηχανές με κακόβουλο λογισμικό, μετατρέποντάς τες σε «ζόμπι» και στη συνέχεια στοχεύουν στους υπολογιστές μεγαλύτερων διακομιστών συστήματος που ονομάζονται *Botnets*.

### *6.1.4 Θέματα ασφάλειας υπολογιστικών συστάδων*

Ο όρος «*cluster* υπολογιστών» αναφέρεται σε μια συλλογή από διάφορα είδη διακομιστών, εικονικών μηχανών και υπολογιστών που συνδέονται στενά ή χαλαρά για να λειτουργούν ως ένα ενιαίο σύστημα. Ο παρακάτω πίνακας παραθέτει τα ζητήματα ασφάλειας που σχετίζονται με τους υπολογιστές συμπλέγματος.

***Πίνακας 11**:Ομαδοποίηση ζητημάτων ασφάλειας υπολογιστών*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Ασφάλεια υπολογιστών** | Φυσικό σύμπλεγμα | Επίθεση DoS, ωμή βία. |
| | Εικονικό σύμπλεγμα | Λανθασμένη διαμόρφωση |

- **Φυσικό σύμπλεγμα (*Physical Cluster*):** Για να έχουν οι καταναλωτές την καλύτερη δυνατή σύνδεση ταχύτητας ανταλλαγής, υπολογιστική ισχύ και τεράστιο αριθμό διαθέσιμων πόρων, το πακέτο προοδευτικής επέκτασης απαιτεί πληθώρα διαχειριζόμενων εικονικών μηχανών, διακομιστών και υπολογιστών. Μια περίληψη περίπτωσης έχει οριστεί να διαμοιράζεται σε όλη την ομάδα υπό το φως της καλύτερης συσχέτισης των ορίων της κοινής χρήσης των πληροφοριών, γεγονός που καθιστά εξαιρετική συνθήκη για τον κυβερνοεγκληματία που σκοπεύει να εξαπολύσει μια επίθεση τύπου *DoS*.

- **Εικονικό σύμπλεγμα (*Virtual Cluster*)**: Μπορεί να εκτελεστεί στο ομαδοποιημένο λειτουργικό σχέδιο της προαναφερθείσας φυσικής οντότητας. Μια λανθασμένη διαμόρφωσή της θέτει σε κίνδυνο την ασφάλεια όλου του φυσικού μηχανήματος.

### *6.1.5 Ζητήματα ασφάλειας που σχετίζονται με το διαδίκτυο και τις υπηρεσίες*

Το Διαδίκτυο μπορεί να χρησιμοποιηθεί για την αποστολή πληροφοριών από ένα σύστημα πηγής σε ένα σύστημα προορισμού που χρησιμοποιεί είτε ενσύρματα είτε ασύρματα μέσα μετάδοσης. Οι πληροφορίες μπορούν επίσης να αποσταλούν ως ακατέργαστα *bits* με τη μορφή πακέτων. Τα δεδομένα αποστέλλονται από την πηγή στον προορισμό μέσω των κόμβων που αποτελούν το Διαδίκτυο. Τα ζητήματα ασφάλειας που σχετίζονται με το Διαδίκτυο και τις υπηρεσίες παρατίθενται στον παρακάτω πίνακα:

***Πίνακας 12**:Ζητήματα που σχετίζονται με το Διαδίκτυο και τις Υπηρεσίες*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Διαδίκτυο και υπηρεσίες** | Διαθεσιμότητα υπηρεσίας | Εύρος ζώνης υπό παροχή, άμεση/έμμεση επίθεση *DoS*, *HTTP*πρωτόκολλο χωρίς κατάσταση, ακατάλληλα έγγραφα *WSDL*, έγχυση *XML*, πειρατεία συνεδρίας, κλοπή *cookie*, δηλητηρίαση *cookie*. |
| | Τεχνολογίες Ιστού | Ανοιχτή περίμετρος δικτύου, περιορισμοί των τειχών προστασίας και περιορισμένη σύνδεση των *Rooted* και *Jailbroken* συσκευών κινητής τηλεφωνίας. |
| | Υπηρεσίες Ιστού (Web Services) | Κακόβουλοι εσωτερικοί χρήστες και κακόβουλοι διαχειριστές του συστήματος, εξομάλυνση του υλικού, αρχαϊκός στατικός κωδικός πρόσβασης, επιθέσεις αναδίπλωσης *XML*, μέθοδοι αδύναμης επαναφοράς διαπιστευτηρίων. |
| | Πρωτόκολλα Διαδικτύου | Εύρος ζώνης υπό προμήθεια, άμεση/έμμεση επίθεση *DoS*, HTTPπρωτόκολλο χωρίς κατάσταση, παραβίαση περιόδων σύνδεσης, κλοπή cookie, δηλητηρίαση cookie. |

- **Διαθεσιμότητα υπηρεσίας:** Ένα πραγματικό όριο ανταλλαγής πληροφοριών και η καθορισμένη σε ένα πλαίσιο ασφάλεια είναι πλέον απαραίτητα για να βοηθήσουν σε σημαντικό βαθμό την ευημερία του υπολογιστικού νέφους.
- **Τεχνολογίες Ιστού:** Οι κυβερνοεγκληματίες που βασίζονται στον ιστό έχουν πρόσβαση στο μεγαλύτερο μέρος των εφαρμογών και των υπηρεσιών του *cloud*. Ο αριθμός των κακόβουλων ιστοσελίδων και των συνδέσμων στο Διαδίκτυο αυξάνεται

συνεχώς. Χρησιμοποιώντας αυτούς τους συνδέσμους για να προσελκύσουν χρήστες, οι εισβολείς μπορούν να εξαπολύσουν διάφορες επιθέσεις.

- **Υπηρεσίες Ιστού:** Η ορθότητα των πληροφοριών αποτελεί μείζον θέμα σε μια κατάσταση διάδοσης. Το ζήτημα της αξιοπιστίας των πληροφοριών στους κατανεμημένους υπολογιστές μπορεί να γίνει κατανοητό λόγω της προσανατολισμένης στην υπηρεσία αρχιτεκτονικής (*SOA: Service Oriented Architecture*).
- **Πρωτόκολλα Διαδικτύου**: Επειδή το περιβάλλον *cloud* βασίζεται στο Web το οποίο και χρησιμοποιεί μια ποικιλία πρωτοκόλλων σύνδεσης στο Διαδίκτυο, τελικά οι εισβολείς μπορεί να χρησιμοποιήσουν τις ευπάθειές τους για να επιχειρήσουν επιθέσεις που βασίζονται στο διαδίκτυο.

### *6.1.7 Θέματα ασφάλειας που βασίζονται σε δίκτυο*

Ένα από τα κύρια εμπόδια για την υιοθέτηση του *cloud computing* είναι η ασφάλεια του δικτύου. Λόγω της δυναμικής φύσης των δικτύων στο περιβάλλον *cloud*, εμφανίστηκε ένας μεγάλος αριθμός ζητημάτων ασφάλειας που σχετίζεται με αυτά.

Σε αυτό το πεδίο, αντιμετωπίζονται διάφορες ανησυχίες που σχετίζονται με το δίκτυο, όπως επιθέσεις άρνησης υπηρεσίας (*DoS*), Man-in-the-middle επιθέσεις, πειρατεία περιόδων σύνδεσης (*session hijacking*), προβλήματα χωρητικότητας δικτύου (*network bandwidth issues*), δυσκολίες δρομολόγησης και εξισορρόπησης φορτίου (*route and load balance*), αλλαγή πρωτοκόλλου δικτύου, ζητήματα που σχετίζονται με το τείχος προστασίας, απειλές ασφάλειας σύνδεσης, πλαστογράφηση IP (*IP spoofing*), επιθέσεις παγιδευτή πακέτων (*sniffer*), *jailbreaking* (αφαίρεση των περιορισμών ασφαλείας που έχουν ορισθεί από τον πωλητή μιας συσκευής). Ο παρακάτω πίνακας περιέχει μια λίστα με τα προβλήματα ασφάλειας που προκύπτουν από το δίκτυο.

***Πίνακας 13**: Ζητήματα ασφάλειας δικτύου υπολογιστών νέφους*

| Κατηγορία | Μηχανισμοί ασφάλειας | Ζητήματα ασφαλείας |
|---|---|---|
| **Δίκτυο** | Ασφάλεια περιφέρειας | Ανοιχτή περίμετρος δικτύου, περιορισμός τείχους προστασίας και περιορισμένη σύνδεση κινητής τηλεφωνίας. |
| | Κινητές πλατφόρμες | Κακόβουλο λογισμικό για κινητά, ευπάθειες κινητών, *rooting* και *jailbreaking*. |

- **Ασφάλεια περιφέρειας (*Circumference Security*):** Η ασφάλεια των άκρων σε περιβάλλον *cloud* είναι ένας συνδυασμός στατικών μέτρων ασφαλείας. Η δυναμική ασφάλεια ενός συστήματος κατασκευάζεται με τη χρήση συσκευών ασφαλείας που

είναι τοποθετημένες στην είσοδο και στα σημεία προώθησης. Δεδομένου του πόσο επικίνδυνα τείνουν να γίνονται τα πράγματα, αυτή η στρατηγική ασφάλειας προϋποθέτει ότι η δομική ρύθμιση είναι στατική.

- **Πλατφόρμες για φορητές συσκευές**: Η *BYOD* τάση μπορεί περιστασιακά να αποδειχθεί επικίνδυνη για τους οργανισμούς. Για να αποκτήσει πρόσβαση στις εφαρμογές ενός έργου στο οποίο συμμετέχει ένας εργαζόμενος χρησιμοποιεί τη δική του προσαρμοσμένη συσκευή. Αυτή η ιδέα είναι επωφελής από άποψη επάρκειας, αλλά εγκυμονεί κινδύνους για την ασφάλεια.

### *6.1.8 Ζητήματα σχετικά με τον έλεγχο πρόσβασης*

Πολλοί πελάτες χρησιμοποιούν το υπολογιστικό νέφος και κάθε ένας από αυτούς έχει μοναδικά δικαιώματα πρόσβασης για τη λήψη πληροφοριών από αυτό. Ο παρακάτω πίνακας περιγράφει τις βασικές προκλήσεις που σχετίζονται με τον έλεγχο πρόσβασης.

***Πίνακας 14**: Ζητήματα ελέγχου πρόσβασης στο υπολογιστικό νέφος*

| **Κατηγορία** | **Μηχανισμοί ασφάλειας** | **Ζητήματα ασφαλείας** |
|---|---|---|
| **Έλεγχος πρόσβασης** | Έλεγχος ταυτότητας οντότητας | Αρχαϊκός στατικός κωδικός πρόσβασης, επιθέσεις αναδίπλωσης *XML*, αδύναμες μέθοδοι επαναφοράς διαπιστευτηρίων. |
| | Διαπιστευτήρια χρήστη | Επίθεση *MITM*, επίθεση επανάληψης, εισβολή *TCP*, τύπου *network root* επιθέσεις. |

- **Έλεγχος ταυτότητας οντοτήτων**: Για να διασφαλιστεί η ασφαλής πρόσβαση σε εφαρμογές *cloud*, απαιτείται ένα πλαίσιο έγκρισης να έχει τεθεί σε λειτουργία. Οι επιθέσεις στο σύννεφο, είναι πολλές φορές ενέδρες αδύναμων κωδικών οι οποίοι υφίστανται λόγω αδύναμων πλαισίων επιβεβαίωσης.
- **Διαπιστευτήρια χρήστη:** Ο διακομιστής *cloud* της επιχείρησης μπορεί να αποθηκεύει όλα τα διαπιστευτήρια ενός χρήστη που απαιτούνται για την παροχή υπηρεσιών. Ο διακομιστής καθορίζει τον έλεγχο της ταυτότητας ενός χρήστη με βάση τα διαπιστευτήριά του. Χρησιμοποιώντας ένα τείχος προστασίας, αυτοί οι διακομιστές μπορούν να τοποθετηθούν είτε εντός είτε εκτός του συσχετισμού των παρόχων του νέφους. Το κόστος αφαίρεσης, αλλαγής, επιβολής κυρώσεων και απενεργοποίησης των λογαριασμών πελατών, καθώς και άλλων εργασιών, αυξάνεται σε μια αρκετά μεγάλη εταιρεία πελατών εφαρμογών.

### *6.1.9 Θέματα ασφάλειας λογισμικού*

Η ασφάλεια λογισμικού είναι επίσης ένα από τα θεμελιώδη ζήτημα όσον αφορά στο θέμα της ασφάλειας στο υπολογιστικό νέφος. Χρησιμοποιώντας τις δικές τους μοναδικές ιδέες και γλώσσες προγραμματισμού, οι ομάδες ανθρώπων παράγουν και τις δικές τους ιδιαίτερες σκέψεις, χρησιμοποιώντας μια εξατομικευμένη προγραμματιστική διάλεκτο. Ο εκάστοτε μηχανικός ακολουθεί το σχέδιο ελέγχου και επιβολής των κανόνων για τη διατήρηση των προγραμμάτων προϊόντων.

Η έκθεση της διεπαφής χρήστη, ο έλεγχος ταυτότητας και πρόσβασης, ο έλεγχος ροής, η τυπική επικύρωση, τα μειονεκτήματα μιας εφαρμογής, ο προγραμματισμός ανοιχτού κώδικα, η μεθοδολογία ανάπτυξης λογισμικού, η απομόνωση μεταξύ των επιπέδων, η ασφαλής κατάληξη συμβολοσειρών και η παρακολούθηση των στοιχείων είναι τα ζητήματα ασφάλειας αυτής της περιοχής. Ο παρακάτω πίνακας περιγράφει τις βασικές προκλήσεις ασφάλειας του λογισμικού.

***Πίνακας 15**: Ζητήματα ασφάλειας λογισμικού Cloud Computing*

| **Κατηγορία** | **Θέματα ασφαλείας** | **Επιπτώσεις** |
|---|---|---|
| **Λογισμικό** | Πλατφόρμες και πλαίσια | Αβέβαιες κλήσεις συστήματος, κακός μηχανισμός *SDLC* |
| | Διεπαφή χρήστη | Έκθεση διεπαφής |

- **Πλατφόρμες και πλαίσια:** Το *PaaS* προσφέρει τη δυνατότητα δημιουργίας μιας εφαρμογής *cloud* και υποστηρίζει διαφορετικές γλώσσες που είναι χρήσιμες για την ανάπτυξή της στο σύννεφο. Η μέτρηση των πόρων που καταναλώνει, η επίλυση των προβλημάτων διαμόρφωσης είναι μερικά μόνο από τα προβλήματα που σχετίζονται με την ασφάλεια.
- **Διεπαφή χρήστη**: Με τη χρήση μιας τυπικής διεπαφής χρήστη μέσω του Διαδικτύου, ένας πελάτης μπορεί να έχει πρόσβαση στα οφέλη των *IaaS* και των *PaaS* μοντέλων διάθεσης.

## 6.2 Μηχανισμοί για τη διασφάλιση του απορρήτου και της ιδιωτικότητας στο νέφος

Το απόρρητο δεδομένων αναφέρεται στον τρόπο χειρισμού μιας πληροφορίας δεδομένης της σημασίας της. Στην εποχή των υπολογιστών, χρησιμοποιείται συχνά την έννοια του απορρήτου δεδομένων για να περιγραφούν θεμελιώδεις ατομικές πληροφορίες, γνωστές και ως πληροφορίες προσωπικής ταυτοποίησης. Το απόρρητο δεδομένων για μια εταιρεία εκτείνεται πέρα από τις προσωπικές πληροφορίες ταυτοποίησης των πελατών και των εργαζομένων της. Για τον σκοπό της παροχής ελέγχου ταυτότητας χρήστη, εμπιστευτικότητας και ακεραιότητας

των μεταφερόμενων δεδομένων μεταξύ χρηστών και παρόχων υπηρεσιών *cloud* για τη μείωση των κινδύνων καταπάτησης της ιδιωτικότητας και της ασφάλειας, αρκετοί συγγραφείς παρουσίασαν μια νέα αρχιτεκτονική που χρησιμοποιεί μια υβριδική προσέγγιση με την τήρηση των παρακάτω αρχών:

- Παροχή πρόσβασης των δεδομένων τους στους χρήστες και προστασία τους από διάφορες απειλές και παράνομη πρόσβαση.
- Πολλαπλή αποθήκευση των δεδομένων σε πολλούς διακομιστές για την αποφυγή της οριστικής απώλειας και της μη διαθεσιμότητας και αποτροπή της διαρροής της αθέμιτης εκμετάλλευσης ή της αθέμιτης μεταβολής από μη εξουσιοδοτημένες πηγές.
- Καθορισμός του επιπέδου επεξεργασίας δεδομένων, επαλήθευσης και διασφάλισης στο οποίο εμπλέκονται οι υπεργολάβοι του *cloud*.
- Καθορισμός του υπεύθυνου για την παροχή νομικών απαιτήσεων για τα προσωπικά δεδομένα των καταναλωτών.

Οι πιο σημαντικές βασικές προκλήσεις που σχετίζονται με το απόρρητο στο *cloud computing* είναι:

- Η επιμονή και η πολυπλοκότητα της ενδελεχούς ανάλυσης κινδύνων και της αξιολόγησης της τρέχουσας κατάστασης του νέφους.
- Νέα σχέδια δράσης αναπτύσσονται συνεχώς, τα οποία σε πολλές περιπτώσεις επηρεάζουν αντίθετα το απόρρητο των πελατών του *cloud*.
- Η συμμόρφωση με τους σχετικούς νόμους και τα ρυθμιστικά πλαίσια.

# 7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Πολλά σοβαρά ζητήματα ασφάλειας και απορρήτου που εγείρονται στο περιβάλλον του υπολογιστικού νέφους σχετίζονται γενικά με το διαδίκτυο, αλλά επιδεινώνονται από το μοντέλο του υπολογιστικού νέφους, το οποίο έχει ως αποτέλεσμα την έλλειψη της εμπιστοσύνης των χρηστών. Ορισμένοι κίνδυνοι και ζητήματα ασφαλείας απαντώνται αποκλειστικά στο περιβάλλον του υπολογιστικού νέφους και όχι στο διαδίκτυο συνολικά Επίσης, φαίνεται να εκλείπει και η σαφής υιοθέτηση των ορίων ευθύνης του παρόχου έναντι του χρήστη καθώς και της σχετικής ανάληψης ευθύνης και της λογοδοσίας σε περίπτωση ζημίας (Alleweldt, 2012).

Είναι σημαντικό όταν εξετάζει κανείς το υπολογιστικό νέφος να κάνει ένα βήμα πίσω, ώστε να έχει κατά νου τη μεγαλύτερη εικόνα αυτού του νέου σχήματος διάθεσης υπολογιστικών πόρων. Τι ακριβώς έχει αλλάξει σε αυτό το νέο μοντέλο παροχής επεξεργαστικής ισχύος, χώρου αποθήκευσης, και λοιπών πόρων και πώς αυτό επηρεάζει την ασφάλεια και το απόρρητο; Θα πρέπει κανείς να έχει κατά νου ότι το *cloud computing* δεν είναι μια νέα τεχνολογία, αλλά μια επανάσταση στις επιχειρηματικές πρακτικές. Η χρήση κοινόχρηστων πόρων, ή πολυμίσθωση, είναι η μοναδική μεγαλύτερη αλλαγή που έχει επιφέρει το σύννεφο από την άποψη της ασφάλειας των πληροφοριών. Τα όρια εμπιστοσύνης έχουν μετατοπιστεί ως αποτέλεσμα του μετασχηματισμού αυτού.

Οι επαγγελματίες της ασφάλειας των πληροφοριών θα πρέπει να ανησυχούν περισσότερο για το γεγονός ότι αυτά τα όρια εμπιστοσύνης είναι επί του παρόντος ασαφή. Σε κάθε επίπεδο του μοντέλου διάθεσης, τα όρια εμπιστοσύνης είναι διαφορετικά. Ακόμη και για κάθε μοντέλο διάθεσης τα όρια εμπιστοσύνης αλλάζουν από πάροχο σε πάροχο. Είναι επίσης σημαντικό όταν εξετάζει κανείς την ασφάλεια που εγγυώνται οι πάροχοι να έχει κατά νου την τρέχουσα οπτική του. Για τους επαγγελματίες ασφάλειας πληροφοριών από μεγάλες επιχειρήσεις, μπορεί η ασφάλεια να φαίνεται κάλλιστα αδύναμη ή ακόμη και απαράδεκτη σε σύγκριση με την τρέχουσα στάση ασφαλείας εντός των οργανισμών τους. Ωστόσο, για πολλούς επαγγελματίες ασφάλειας πληροφοριών μικρομεσαίων επιχειρήσεων που εξετάζουν την ασφάλεια που παρέχουν οι εκάστοτε πάροχοι υπηρεσιών νέφους, αυτή μπορεί να φαίνεται αποδεκτή ή ακόμη και καλύτερη σε σύγκριση με την τρέχουσα στάση ασφαλείας του οργανισμού τους (Mather et al., 2009).

Μετά την ολοκλήρωση της εργασίας, είναι πλέον πολύ πιο σαφές πόσο σημαντικοί μπορεί να είναι οι έλεγχοι ασφάλειας και απορρήτου για τους πελάτες, ως ένα από τα πιο

σημαντικά εμπόδια για την υιοθέτηση του υπολογιστικού νέφους. Όλοι οι χρήστες πρέπει να γνωρίζουν καλύτερα τους κινδύνους ασφαλείας, τις επιθέσεις που εξαπολύονται και τις αδυναμίες που μπορεί να παρουσιάσει το νέφος. Επίσης, οι πάροχοι θα πρέπει να είναι πιο ανοιχτοί σχετικά με τις διαδικασίες ασφαλείας τους και να παρέχουν αρχεία ελέγχου των προσπαθειών τους προς όφελος των πελατών τους. Η επίγνωση των θεμάτων ασφάλειας στο σύννεφο θα βοηθήσει τους χρήστες να σταθμίσουν τα οφέλη και τα πλεονεκτήματα έναντι των κινδύνων και των μειονεκτημάτων των υπηρεσιών του νέφους (Khan et al., 2022).

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Ελληνική

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (2020). *ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ*.

## Ξένη

Abdulsalam, Y.S.A. and Hedabou, M. (2022). *Security and Privacy in Cloud Computing: Technical Review*. Future Internet. https://doi.org/10.3390/fi14010011.

Abusaimeh, H. (2020). *Virtual Machine Escape in Cloud Computing Services*. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 7.

Ahmed, M. andHossain, A.M. (2014). *Cloud Computing and Security Issues in the Cloud.* International Journal of Network Security & Its Applications 6(1):25-36. DOI: 10.5121/ijnsa.2014.6103.

Ahmed, M. andLitchfield, A. (2017). *Taxonomy for Identification of Security Issues in Cloud Computing Environments*. Journal of Computer Information Systems 58(1):79-88. DOI: 10.1080/08874417.2016.1192520.

Al-Sarem, M., Saeed, F., Al-Mekhlafi, Z.G., Mohammed, B.A., Al-Hadhrami, T., Alshammari, M. T., . . . Alshammari, T. S. (2021). *An Optimized Stacking Ensemble Model for Phishing Websites Detection*. Electronics 2021, 10, 1285., 1-18.

Alleweldt (Dr.), F., Kara (Dr.) S., Fielder, A., Brown, I., Weber, V. and McSpedden-Brown, N. (2012). *Cloud Computing*. Study. Policy Department Economic and Scientific Policy. European Parliament.

Bhatia, S. andMalhotra, J. (2018*). CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework*. International Journal of Electrical and Computer Engineering. DOI: 10.11591/ijece.v8i5.pp3756-3766.

Barron, C., Yu, H. and Zhan, J., (2013). *Cloud computing security case studies and research*. In: Proceedings of the World Congress on Engineering 2013, VOL II.

Basnet, R., Sung, A. H., and Liu, Q. (2012). *Rule-Based Phishing Attack Detection*.

Casalicchio, E. and Silvestri, L. (2013). *Mechanisms for SLA provisioning in cloud-based service providers*. Comput Networks.

Cheng, F. (2011). *Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm*. Mobile Networks Appl.

Chinguwo, R.M. and Dhanalakshmi, R. (2023). *Detecting Cloud Based Phishing Attacks Using Stacking Ensemble Machine Learning Technique*. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653. Volume 11 Issue III.

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E. and Song, Z. (2010). *Authentication in the Clouds: A Framework and Its Application to Mobile Users*. ACM, CCSW.

Deekshitha, B., Aswitha, C., Sundar, C.S. and Deepthi, A.K. (2022). *URL Based Phishing Website Detection by Using Gradient and Catboost Algorithms*. International Journal for Research in Applied Science &Engineering Technology (IJRAS), Volume 10 Issue VI.

Dey, S. and (Dr) Sen, K. S. (2017*). Four Dimensional Security and Vulnerability Matrix for Cloud (4-SVM)*. Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering. DOI: 10.15439/2017R41.

Duncan, A., Creese, S. and Goldsmith, M. (2012). *Insider attacks in cloud computing*. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

El-Sofany, F. H. and El-Seoud, A. S. (2019). *Performance Analysis of an Effective Approach to Protect Cloud Systems against Application Layer Based Attacks*. International Journal of Online and Biomedical Engineering. DOI: 10.3991/ijoe.v15i03.9931.

Emeakaroha, V. C., Netto, M. A. S., Calheiros, R. N., Brandic, I., Buyya, R.and Rose, C. A. F. D. (2012). *Towards autonomic detection of SLA violations in cloud infrastructures*. Future GenerComput Syst.

Fan, C. and Huang, S. (2013*). Controllable privacy preserving search based on symmetric predicate encryption in cloud storage*. Future GenerComput Syst.

Fazliya, M.H.F. and Naleer. H. (2019). *A Rule Based Prediction of Phishing Websites Using Data Mining Classification Techniques*. Journal of Technology and Value Addition Volume 1 (2).

Fernando, N., Loke, S. W.andRahayu, W. (2013). *Mobile cloud computing: A survey*. Future Gener Comput Syst.

Gonzalez, N., Miers, C., Redıgolo, F., Simplıcio, M., Carvalho, T., Naslund, M. and Pourzandi, M. (2012). *A quantitative analysis of current security concerns and solutions for cloud computing*. J Cloud Comput Adv Syst Appl.

Gopalakrishnan Nair, T.R., Suma, V. and Manas, S. (2012). *Genetic Algorithm to Make Persistent Security and Quality of Image in Steganography from RS Analysis*. Swarm Evolutionary and Memetric Computing Conference (SEMCCO), Vishakhapatnam.

Grobauer, B., Walloschek, T. and Stocker, E. (2011). *Understanding cloud computing vulnerabilities*. IEEE Security and Privacy.

Gruschka, N.and Jensen, M. (2010). *Attack surfaces: A taxonomy for attacks on cloud services. In Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing*. https://doi.org/10.1109/CLOUD.2010.23.

Guan, D. J., Chen, C.-M. and Lin, J.-B. (2022). *Anomaly Based Malicious URL Detection in Instant Messa*ging.

Gupta, S. and Kumar, P. (2013*). TAXONOMY OF CLOUD SECURITY*. International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.5. DOI : 10.5121/ijcsea.2013.3505 47.

Hassaan, M. (2022). *Security Issues in Cloud Computing*: A Study. DOI: 10.18280/rces.090404.

Hwang, K., Fox, G. andDongarra, J. (2010). *Cloud Architecture and Datacenter Design. Chapter 7 in Distributed Computing: Clusters, Grids and Clouds*.

Iqbal, S., Kiah (Miss), M.L., Dhaghighi, B., Hussain, M., Khan, S., Khan, K.M.and Choo, R.K-K. (2016).*On cloud security attacks: A taxonomy and intrusion detection and prevention as a service*. Journal of Network and Computer Applications 74 (2016) 98–120.

Issa, N. (2021). *Cloud Computing Security and Privacy Preservation: Using multi-level encryption*.

Jansen, W. andGrance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. NIST (National Institute of Standards and Technology) Special Publication 800-144.

Karnwal, T., Sivakumar, T. andAghila, G. (2012). *A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack*. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS). Bhopal, India.

Khalil, M. I., Khreishah, A.and Azeem, M. (2014). *Cloud Computing Security: A Survey*. doi:10.3390/computers3010001.

Khan, A., Abid, K. M.andFuzail, M. (2022). *An Analysis of Cloud Computing Security Problems*.

Krombholz, K. Hobel, H., Huber, M. and Weippl, E. (2013). *Social Engineering Attacks on the Knowledge Worker*.ACM SIN.

Krutz, L. R.andDean Vines, R. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, Inc.

Kulkarni, P. and Khanai, R. (2015). *Addressing mobile cloud computing security issues: a survey*, IEEE ICCSP 2015 conference. Bangalore, India.

Lin, W. and Lee, D. (2012). *Traceback Attacks in Cloud -- Pebbletrace Botnet*. 32nd International Conference on Distributed Computing Systems Workshops. DOI:10.1109/ICDCSW.2012.61.

Mell, P. andGrance, T. (2011) *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology.https://doi.org/10.6028/NIST.SP.800-145.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. andRajarajan, M. (2013). *A survey of intrusion detection techniques in Cloud*. J Network Comput Appl.

Mohammad, R. M., Thabtah, F., and McCluskey, L. (2014). *Intelligent rule-based phishing websites classification*.

Murala, K. D. and Panda, K. S. (2019). *A Survey on Cloud Computing Security and Privacy Issues and Challenges*. Jour of Adv Research in Dynamical & Control Systems, Vol. 11, 06-Special Issue.

Musa, H., Gital, A., Zambuk, F.U., Umar, A., Umar, A.Y. and Wazir, J.U. (2019). *A Comparative Analysis of Phishing Website Detection Using XGBoost Algorithm*. Journal of Theoretical and Applied Information Technology, Vol.97. No 5.

Neumann, J. A., Statland, N. and Webb, D. R. (1977). *Post-processing audit tools and techniques*. US Department of Commerce, National Bureau of Standards. pp. 11-3--11-4.

Nickerson, R. C., Varshney, U. and Muntermann, J. (2013). *A method for taxonomy development and its application in information systems*. Eur J Inf Syst.

Pan, Y. and Ding, X. (2006). *Anomaly Based Web Phishing Page Detection*. 2006 22nd Annual Computer Security Applications Conference (ACSAC'06).

Panda, R., D., Behera, K. S. and Jena, D. (2021). *A Survey on Cloud Computing Security Issues, Attacks and Countermeasures.*

Perez-Botero, D., Szefer, J. and Lee, R. B. (2013). *Characterizing hypervisor vulnerabilities in cloud computing servers*. ACM. Cloud Computing.

Qaisar, S. and Khawaja, K.F. (2012). *Cloud computing: network/security threats and countermeasures*. Interdiscip. J. Contemp. Res. Bus. 3 (9).

Reuben, J.S. (2007). *A Survey on Virtual Machine Security*. Helsinki University of Technology.

Riquet, D., Grimaud, G. and Hauspie, M. (2012). *Large-scale coordinated attacks: Impact on the cloud security*. In Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). Palermo, Italy.

Roberts, J. C. and Al-Hamdani, W. (2011). *Who can you Trust in the Cloud? a Review of Security Issues within Cloud Computing*. ACM. Information Security Curriculum Development Conference.

Rodero-Merino, L., Vaquero, L., Caron, E., Muresan, A. and Desprez, F. (2012). *Building safe PaaS clouds: a survey on security in multitenant software platforms*. Comput. Secur. 31 (1). DOI: 10.1016/j.cose.2011.10.006.

Sabahi, F. (2011). *Virtualization-level security in cloud computing*. In: Proceedings of the Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference. IEEE.

Sawesi, K.G.A., Saudi, M.M. and Jali, M.Z. (2013). *Designing a new E-Commerce authentication framework for a cloud-based environment*. In: Proceedings of the Control and System Graduate Research Colloquium (ICSGRC). IEEE.

Scarfone, K. (2011). *Guide to Security For Full Virtualization Technologies*. DIANE Publishing.

Sen, J. (2015). *Security and Privacy Issues in Cloud Computing*. DOI: 10.4018/978-1-4666-6539-2.ch074. In book: Cloud Technology.

Shiu, H.-J., Lin, B.-S., Cheng, C.-W., Huang, C.-H. and Lei, C.-L. (2017). *High-Capacity Data-Hiding Scheme on Synthesized Pitches Using Amplitude Enhancement - A New Vision of Non-Blind Audio Steganography*. https://doi.org/10.3390/sym9060092.

Singh, K.G. &Somani, G. (2018). *Cross-VM Attacks: Attack Taxonomy, Defense Mechanisms, and New Directions*. Springer. https://doi.org/10.1007/978-3-319-97643-3_8.

Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, S.M. andRevathy, P. (2012). *State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment*. ACM ICACCI.

Sosinsky, B. (2011). *Cloud Computing Bible*. Wiley Publishing.

Sun, L., Singh, J.and Hussain, O. K. (2012*). Service Level Agreement (SLA) Assurance for Cloud Services: A Survey from a Transactional Risk Perspective*. ACM MoMM. Bali, Indonesia.

Sun, Y. and He., D. (2012). *Model checking for the defense against cross-site scripting attacks*. In: Proceedings of the Computer Science & Service System (CSSS). International Conference. IEEE.

Sureshkumar, V. and Baranidharan, B. (2021). *A study of the cloud security attacks and threats*.

Tong, J., Xiong, G., Zhao, Y. and Guo, L. (2013). *A Research on the vulnerability in popular P2P protocols*. 8th International Conference on Communications.

Tupakula, U., Varadharajan, V. and Akku, N. (2011). *Intrusion detection techniques for infrastructure as a service cloud*. In Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia.

Turnbull, L.and Shropshire, J. (2013*). Breakpoints: an analysis of potential hypervisor attack vectors. In: Proceedings of the Southeastcon*. IEEE.

Vaquero, L. M., Rodero-Merino, L. andMorán, D. (2011). *Locking the sky: a survey on IaaS cloud security*.

Wakelyn, C.C. (1976*). Bank Recordkeeping and the Customer's Expectation of Confidentiality*. Catholic University Law Review. Volume 26, Issue 1, Article 8.

Xiao, Z. and Xiao, Y. (2013). *Security and Privacy in Cloud Computing*. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2.

Yun, J., Park, K.-W., Koo, D. and Shin, Y. (2020). *Lightweight and Seamless Memory Randomization for Mission-Critical Services in a Cloud Platform*. MDPI.

Zhou, F., Goel, M. andDesnoyers, P. (2011). *Scheduler Vulnerabilities and Attacks in Cloud Computing.*

## Ιστοσελίδες

Audenard, J-F. (2011). *Comprendre les attaques de "XML Signature Wrapping" contre Amazon et Eucalyptus*. https://www.orange-business.com/fr/blogs/securite/cloud-computing/comprendre-les-attaques-de-xml-signature-wrapping-contre-amazon-et-eucalyptus.

CertMike.com (2023). *Confidentiality, Integrity and Availability – The CIA Triad*. https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/.

Content Team. (2021). *What is The CIA TRIAD & its Importance for Cybersecurity*. https://websitesecuritystore.com/blog/what-is-the-cia-triad/.

Guardian News & Media. (2016). *Dropbox hack leads to leaking of 68m user passwords on the internet*. https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach.

HACKERNOON. (2023). *Cloud Phishing: New Tricks and the Crown Jewel*. https://hackernoon.com/cloud-phishing-new-tricks-and-the-crown-jewel.

IBM. (2023). *What is cloud security? A Complete Guide to Securing Your Cloud Environment*. https://www.ibm.com/topics/cloud-security.

ICO, Information Commissioner's Office (2023*). Security: Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/.

Koshkin, D. (2022). *Cloud Deployment Models: Advantages and Disadvantages*. SaM Solutions USA, Inc. https://sam-solutions.us/advantages-and-disadvantages-of-cloud-deployment-models/.

Krzyzanowski, P. (2022). *Computer Security: Introduction to Computer Security Thinking about Security*. https://people.cs.rutgers.edu/~pxk/419/notes/intro.html.

Microsoft. (2023). *Define cloud models*. https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/5-define-cloud-models.

Munson, L. (2015). *Stolen Uber login credentials for sale on the dark web*. https://nakedsecurity.sophos.com/2015/03/30/stolen-uber-login-credentials-for-sale-on-the-dark-web/.

Office of Information Security. (2023). *Confidentiality, Integrity, and Availability: The CIA Triad. Washington University in St. Louis*. https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/.

PortSwigger. (unkown). *Password reset poisoning*. https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning.

PortSwigger. (unkown).*SQL injection*. https://portswigger.net/web-security/sql-injection.

Reed, J. (2023). *50 Million Password Heist Shows Info-stealing is on the Rise.* https://securityintelligence.com/news/info-stealing-on-the-rise/.

Siemons, F. (2018). *SQL Injection Protection in Cloud Systems*. https://resources.infosecinstitute.com/topic/sql-injection-protection-cloud-systems/.

Theastrologypage. (2023). *Τι είναι μια στρατηγική πολλαπλών σύννεφων; - ορισμός από την τεχνολογία*. https://el.theastrologypage.com/multi-cloud-strategy.

Threatcop. (unkown). *Man in the Middle Attack: A Havoc to Network Security*. https://threatcop.com/blog/man-in-the-middle-attack/.

Toth, P. - NIST (2022). *Cybersecurity – A Critical Component of Industry 4.0 Implementation*. https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation.

Tozzi, C. (2023).*Cross-Site Scripting Attacks: How to Protect Your Website*. https://www.itprotoday.com/development-techniques-and-management/cross-site-scripting-attacks-how-protect-your-website.

UBIKA (2022). *Cross-Site Scripting (XSS).*https://www.cloudprotector.com/cross-site-scripting-xss/.

WebBazar India (2021). *What Is Cloud Deployment Model? Type of Cloud Deployment models*. https://webbazar.co.in/what-is-cloud-deployment-model-type-of-cloud-deployment-models/.

Wikipedia. (2023). *Information security*. https://en.wikipedia.org/wiki/Information_security.

Zhang, F., Huang, Y., Wang, H., Chen, H. and Zang, B. (2008). *PALM: security preserving VM live migration for systems with VMM-enforced protection*. DOI: 10.1109/APTC.2008.15.