ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Δ.Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΝΕΦΟΣ»

ΚΟΡΩΝΑΙΟΣ ΙΟΡΔΑΝΗΣ ΡΑΦΑΗΛ

ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ

CSCYB22011

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΔΡ. ΣΤΕΦΑΝΟΣ ΓΚΡΙΤΖΑΛΗΣ

ΑΘΗΝΑ, ΑΠΡΙΛΙΟΣ 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

UNIVERSITY OF WEST ATTICA

SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING

MSc "CYBERSECURITY"

DIPLOMA THESIS

"CLOUD SECURITY AND PRIVACY"

KORONAIOS IORDANIS RAFAIL

REGISTRATION NUMBER

CSCYB22011

SUPERVISOR

Dr. STEFANOS GKRITZALIS

ATHENS, APRIL 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Δ.Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ»

«ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΝΕΦΟΣ»

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι εξεταστική επιτροπή:

Α/α	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	ΕΠΙΒΛΕΠΩΝ ΔΡ. ΣΤΕΦΑΝΟΣ ΓΚΡΙΤΖΑΛΗΣ		STEFANOS GKRITZALIS 08/05/2024 17:44
2	ΜΕΛΟΣ Ι ΔΡ. ΠΑΝΑΓΙΩΤΗΣ ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ		Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2024.05.08 19:45:00 +03'00'
3	ΜΕΛΟΣ ΙΙ ΔΡ. ΕΜΜΑΝΟΥΗΛ ΜΙΧΑΗΛΙΔΗΣ		EMMANOUIL MICHAILIDIS Digitally signed by EMMANOUIL MICHAILIDIS Date: 2024.05.08 18:15:06 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ιορδάνης Ραφαήλ Κορωναίος του Ιωάννη, με αριθμό μητρώου cscyb22011 φοιτητής του ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας της παρούσας μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένης και αναφέρεται στην εργασία. Επιπλέον, 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, οι οποίες ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Ακόμα, βεβαιώνω ότι η εργασία αυτή έχει συγγραφεί από εμένα 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

Ιορδάνης Ραφαήλ Κορωναίος

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντα καθηγητή κύριο Γκρίτζαλη, για τη δυνατότητα που μου έδωσε να υλοποιήσω τη διπλωματική μου εργασία. Οι σημαντικές υποδείξεις αλλά και συμβουλές του με κατεύθυναν σε έναν ορθό τρόπο σκέψης, μα πάνω από όλα μου πρόσφεραν σημαντικά εφόδια για την μετέπειτα ανέλιξη μου.

Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του Δ.Π.Μ.Σ. «Κυβερνοασφάλεια» του Πανεπιστημίου Δυτικής Αττικής για τις πολύτιμες γνώσεις που μου μεταλαμπάδευσαν όλο αυτό το χρονικό διάστημα της συνεργασίας μας.

Εν κατακλείδι, θα επιθυμούσα να εκφράσω ένα τεράστιο ευχαριστώ στους γονείς και στην αδερφή μου για την αμέριστη συμπαράσταση τους, τη στήριξη, την εμπιστοσύνη και την υπομονή που κατέδειξαν όλο αυτό το διάστημα για την αποπεράτωση του Μεταπτυχιακού μου.

Περιεχόμενα

Συντομογραφίες

ABE	Attribute-based encryption
ABKS	Attribute-Based Encryption with Dynamic Keyword Search
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
CAMM	Cybersecurity Assessment and Management Methodology
CCAK	Certificate of Cloud Auditing Knowledge
CCM	Cloud Control Matrix
CoT	Cloud of Things
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CSA	Cloud Security Alliance
DBDH	Decision Bilinear Diffie-Hellman
DDoS	Distributed Denial of Service
DIZK	Distributed Zero Knowledge Proofs
DMaaS	DDoS Mitigation as a Service
DNS	Domain Name System
DoS	Denial of Service
EAP	Electronic Administrative Procedures
ECC	Elliptic Curve Cryptography
EHR	Electronic Health Records
FWaaS	Firewall-as-a-Service
HCS	Hybrid Cryptographic System
HIBE	Hierarchical Identity-Based Encryption
IaaS	Infrastructure as a Service
IBE	Identity-Based Encryption
IDPS	Intrusion Detection and Prevention System

IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPS	Intrusion Prevention Systems
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
KP-ABE	Key-Policy Attribute-Based Encryption
MAC	Mandatory Access Control
MNS	Mobile Network Services
NIST	National Institute of Standards and Technology
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a Service
PDC	Personal Data Cloud
PDP	Provable Data Possession
PEKS	Public Key Encryption with keyword Search
POR	Proofs of Retrievability
PRKS	Proxy Re-encryption with Keyword Search
RBAC	Role-based access control
RSA	Rivest–Shamir–Adleman
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SE	Searchable Encryption
SEFSCITY	Secure Framework for Future Smart City
SET	Searchable Encryption Techniques
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SSE	Searchable Symmetric Encryption
SSL	Secure Sockets Layer
STAR	Safety, Trust, Assurance and Risk
TLS	Transport Layer Security

TPAs	Third-Party Auditors
UI	User Interface
WfMS	Work flow Management System
XML	Extensible Markup Language
ZKPs	Zero Knowledge Proofs

Περίληψη

Το υπολογιστικό νέφος αφορά ένα δίκτυο ή διαδίκτυο, το οποίο μπορεί να χαρακτηριστεί ως μία αυτούσια τεχνολογία, μία συλλογή τεχνολογιών, ένα λειτουργικό μοντέλο ή ένα επιχειρηματικό μοντέλο.

Στόχος της παρούσας εργασίας ήταν η μελέτη της ασφάλειας και του απορρήτου των δεδομένων στο υπολογιστικό νέφος.

Οι βάσεις δεδομένων, οι οποίες χρησιμοποιήθηκαν για τη διεξαγωγή της παρούσας εργασίας είναι το Google Scholar, το ACM και το IEEE. Η γλώσσα αναζήτησης ήταν η αγγλική. Στην τελική βιβλιογραφία συμπεριλήφθηκαν μελέτες, οι οποίες είχαν δημοσιευτεί κατά το χρονικό διάστημα από το Σεπτεμβρίου του 2009 έως το Δεκέμβριο του 2023. Σε κάθε βάση δεδομένων ξεχωριστά εισήχθησαν οι ακόλουθες λέξεις κλειδιά “cloud security”, “data privacy”, “cloud storage security”, “IoT security” και “cloud security and privacy”. Στο σύνολό τους μελετήθηκαν 42 βιβλιογραφικές αναφορές, οι οποίες περιλάμβαναν βιβλία, άρθρα και δημοσιεύσεις διεθνών οργανισμών σχετικά με την ασφάλεια και το απόρρητο στο υπολογιστικό νέφος.

Η τεχνολογία υπολογιστικών νεφών γίνεται όλο και πιο διαδεδομένη λύση για την παροχή υπηρεσιών μέσω του διαδικτύου. Η υιοθέτηση της παρέχει τη δυνατότητα στους χρήστες να έχουν πρόσβαση σε μία ποικιλία από πλεονεκτήματα, όπως το μειωμένο κόστος, η υψηλή επεκτασιμότητα, η ευελιξία υπηρεσιών και η παροχή πόρων κατά απαίτηση.

Παρόλα αυτά, η ασφάλεια και το απόρρητο των δεδομένων έχουν γίνει ένα από τα σημαντικότερα εμπόδια στην υιοθέτηση υπηρεσιών υπολογιστικών νεφών. Οι βασικοί τομές της ασφάλειας στα περιβάλλοντα υπολογιστικών νεφών είναι η ασφάλεια υποδομής, η ασφάλεια εφαρμογών και η ασφάλεια δεδομένων.

Η ασφάλεια σε περιβάλλοντα υπολογιστικών νεφών επηρεάζει πολλές άλλες τεχνολογίες όπως είναι το Διαδίκτυο των Πραγμάτων, τα κοινωνικά δίκτυα, το blockchain, η αποθήκευση δεδομένων και άλλες.

Έχουν αναπτυχθεί αρκετά αντίμετρα, τα οποία στοχεύουν στον μετριασμό των προκλήσεων, οι οποίες εγκυμονούν έναντι των συστημάτων υπολογιστικών νεφών. Ωστόσο, είναι αναγκαία η συνεχής έρευνα για τον εντοπισμό νέων κινδύνων και τη διασφάλιση δημιουργίας στρατηγικών και αρχιτεκτονικών ασφαλείας.

Λέξεις κλειδιά: ασφάλεια υπολογιστικών νεφών, απόρρητο δεδομένων, ασφάλεια υπολογιστικών νεφών και απόρρητο

Abstract

Cloud computing refers to a network or internet, which can be characterized as a single technology, a collection of technologies, an operating model or a business model.

The aim of this thesis was to study the security and privacy of data in cloud computing.

The databases used to carry out this thesis are Google Scholar, ACM and IEEE. The search language was English.

The final bibliography included studies published between September 2009 and December 2023. The following keywords “cloud security”, “data privacy”, “cloud storage security”, “IoT security” and “cloud security and privacy” were entered into each database separately. A total of 42 bibliographic references were studied, which included books, articles and publications of international organizations regarding the security and privacy in cloud computing.

Cloud computing technology is becoming an increasingly popular solution for providing services over the Internet. Its adoption enables users to access a variety of benefits, such as reduced cost, high scalability, service flexibility, and on-demand resource provisioning.

However, data security and privacy have become one of the major barriers to the adoption of cloud computing services. The key intersections of security in cloud computing environments are infrastructure security, application security and data security.

Security in cloud computing environments affects many other technologies such as the Internet of Things, social networks, blockchain, data storage and others.

Several countermeasures have been developed that aim to mitigate the challenges facing cloud computing systems. However, continuous research is needed to identify new risks and ensure security strategies and architectures are in place.

Key words: cloud security, data privacy, cloud security and privacy

Εισαγωγή

Με τον όρο υπολογιστικό νέφος (ή ευρέως γνωστό ως Cloud Computing) γίνεται αναφορά σε ένα δίκτυο ή διαδίκτυο. Υπάρχουν πολλοί διαφορετικοί τρόποι αναφοράς στον όρο υπολογιστικό νέφος. Πιο συγκεκριμένα, μπορεί για παράδειγμα να χαρακτηριστεί ως μία αυτούσια τεχνολογία, μία συλλογή τεχνολογιών, ένα λειτουργικό μοντέλο ή ακόμη και ένα επιχειρηματικό μοντέλο. Μπορεί να θεωρηθεί, ουσιαστικά, μεταμορφωτικό και ανατρεπτικό. Επιπλέον, το υπολογιστικό νέφος αναπτύσσεται με πάρα πολύ γρήγορους ρυθμούς και δε δείχνει σημάδια επιβράδυνσης.

Η τεχνολογία υπολογιστικών νεφών γίνεται όλο και πιο μαγική σαν λύση, την στιγμή που αποτελεί μία ευρέως υιοθετημένη τεχνολογία για την παροχή υπηρεσιών μέσω του διαδικτύου χάρη στα ποικίλα οφέλη του. Σε αυτά συμπεριλαμβάνονται οι υπηρεσίες κατά απαίτηση, η μείωση του κόστους, η κοινή χρήση και διαμόρφωση υπολογιστών πόρων, η υψηλή επεκτασιμότητα και η ευελιξία των υπηρεσιών, οι οποίες μπορούν να παρασχεθούν.

Ωστόσο, με την εμφάνιση αυτής της τεχνολογίας, η έννοια της ασφάλειας και το απόρρητο των δεδομένων έχουν γίνει ένα από τα σημαντικότερα εμπόδια στην υιοθέτηση υπηρεσιών υπολογιστικών νεφών. Πράγματι, έχουν διεξαχθεί πολλές έρευνες για τον εντοπισμό ζητημάτων ασφάλειας και απορρήτου σε περιβάλλοντα υπολογιστικών νεφών.

Στην παρούσα εργασία, γίνεται μελέτη της έννοιας της τεχνολογίας υπολογιστικού νέφους, αναλύονται οι κίνδυνοι, οι οποίοι διαδραματίζουν σημαντικό ρόλο στα συστήματα υπολογιστικών νεφών και προτείνονται μέτρα για τον περιορισμό της απειλής. Τέλος, παρουσιάζεται ο συσχετισμός της ασφάλειας και του απορρήτου σε περιβάλλοντα υπολογιστικών νεφών με αρκετές σύγχρονες τεχνολογίες.

Σκοπός της παρούσας εργασίας ήταν η μελέτη της ασφάλειας και του απορρήτου των δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλοντα υπολογιστικών νεφών και ο συσχετισμός της ασφάλειας της τεχνολογίας των υπολογιστικών νεφών με άλλες σύγχρονες τεχνολογίες.

Μεθοδολογία

Οι βάσεις δεδομένων, οι οποίες χρησιμοποιήθηκαν για τη διεξαγωγή της παρούσας εργασίας είναι το Google Scholar, ACM και IEEE. Η γλώσσα αναζήτησης ήταν η αγγλική. Στην τελική βιβλιογραφία συμπεριλήφθηκαν μελέτες, οι οποίες είχαν δημοσιευτεί κατά το χρονικό διάστημα από το Σεπτεμβρίου του 2009 έως το Δεκέμβριο του 2023. Σε κάθε βάση δεδομένων ξεχωριστά εισήχθησαν οι ακόλουθες λέξεις κλειδιά “cloud security”, “data privacy”, “cloud storage security”, “IoT security” και “cloud security and privacy”.

Τα άρθρα αξιολογήθηκαν με βάση τη συνάφεια του τίτλου τους, προς τα αντικείμενο μελέτης και τους δείκτες επισκεψιμότητας, οι οποίοι αναφέρονταν στην κάθε βάση δεδομένων. Στο σύνολό τους μελετήθηκαν 42 βιβλιογραφικές αναφορές, οι οποίες περιλάμβαναν βιβλία, άρθρα και δημοσιεύσεις διεθνών οργανισμών σχετικά με το φαινόμενο της ασφάλειας και του απορρήτου στο υπολογιστικό νέφος.

1. Υπολογιστικά Νέφη (Cloud Computing)

1.1. Υπολογιστικά Νέφη

Το υπολογιστικό νέφος είναι ένα λειτουργικό μοντέλο, το οποίο αποτελείται από ένα σύνολο τεχνολογιών και έχει στόχο τη διαχείριση δεξαμενών υπολογιστικών πόρων, είναι μία τεχνολογία, η οποία έχει τη δυνατότητα να βελτιώσει τη συνεργασία, την ευελιξία, την κλιμάκωση και τη διαθεσιμότητα, καθώς επίσης να παρέχει ευκαιρίες για την μείωση του κόστους. Το υπολογιστικό νέφος έχει αλλάξει εντελώς την τοπογραφία των υπολογιστών, των υπηρεσιών, της αποθήκευσης και των επικοινωνιακών υποδομών. Υπάρχει η δυνατότητα, λοιπόν, να επιτραπεί η κατ' απαίτηση διαθεσιμότητα υπολογιστικών και αποθηκευτικών πόρων. Έχει σχεδιαστεί με τέτοιο τρόπο ώστε τα στοιχεία να μπορούν να ενορχηστρωθούν γρήγορα, να σχεδιαστούν, να υλοποιηθούν και να κλιμακωθούν προς τα πάνω ή προς τα κάτω έτσι ώστε να παρέχουν ένα μοντέλο κατανομής και κατανάλωσης κατά παραγγελία.

Για τον ορισμό του υπολογισμού νέφους μπορούν να δοθούν πολλοί ορισμοί, αλλά οι δύο πιο αξιοσημείωτοι είναι από δύο οργανισμούς. Αναλυτικότερα, με βάση το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST), το υπολογιστικό νέφος ορίζεται ως εξής, *«Το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την απεριόριστη, βολική, κατ' απαίτηση πρόσβαση δικτύου σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικός χώρος, εφαρμογές και υπηρεσίες) που μπορεί να παρασχεθεί και να κυκλοφορήσει γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση παρόχου υπηρεσιών»*.

Την ίδια στιγμή, ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization – ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission – IEC) παρουσιάζει το δικό του ορισμό για το υπολογιστικό νέφος, *«Παράδειγμα για τη δυνατότητα πρόσβασης σε ένα κλιμακούμενο και ελαστικό αποθεματικό κοινόχρηστων φυσικών ή εικονικών πόρων με αυτόνομη παροχή και διαχείριση κατά απαίτηση»*.

Ένα υπολογιστικό νέφος αποτελείται από υπολογιστικούς πόρους, οι οποίοι είναι παρόμοιοι με τα «υπολογιστικά» παραδείγματα επεξεργαστών και μνήμης, δίκτυα, δομές αποθήκευση και πόρους υψηλότερου επιπέδου, όπως για παράδειγμα βάσεις δεδομένων και εφαρμογές.

Τα υπολογιστικά νέφη είναι από τη φύση τους πολυενοικιαζόμενα. Διαφορετικές ομάδες χρηστών – καταναλωτών μοιράζονται τους ίδιους πόρους, αλλά είναι διαχωρισμένες και απομονωμένες μεταξύ τους. Ο διαχωρισμός επιτρέπει στον πάροχο υπηρεσιών υπολογιστικού νέφους να διαμοιράζει τους πόρους στις διαφορετικές ομάδες και η απομόνωση διασφαλίζει την ακεραιότητα των δεδομένων, δηλαδή ότι δεν μπορούν να δουν ή να τροποποιήσουν ο ένας τα δεδομένα του άλλου. Η πολυμίσθωση δεν ισχύει μόνο για διαφορετικούς οργανισμούς. Χρησιμοποιείται επίσης για τη διανομή πόρων μεταξύ διαφορετικών μονάδων σε ένα μεμονωμένο οργανισμό.

1.2. Μοντέλα Ανάπτυξης Υπολογιστικών Νεφών

Τόσο το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) όσο και ο Διεθνής Οργανισμός Τυποποίησης μαζί με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (ISO/IEC) χρησιμοποιούν τα ίδια τέσσερα μοντέλα ανάπτυξης υπολογιστικών νεφών. Τα μοντέλα ανάπτυξης, λοιπόν, είναι το δημόσιο (public), το ιδιωτικό (private), το κοινοτικό (community) και το υβριδικό (hybrid). Αυτά τα μοντέλα χρησιμοποιούνται από εταιρείες με στόχο την παροχή εφαρμογών και επιχειρηματικών υπηρεσιών σε αποτελεσματικό επίπεδο.

Το δημόσιο υπολογιστικό νέφος (public cloud) είναι ένας τύπος υπολογιστικού νέφους, ο οποίος επιτρέπει στα συστήματα και τις υπηρεσίες να είναι εύκολα προσβάσιμα στο ευρύ κοινό. Το δημόσιο υπολογιστικό νέφος ανήκει σε έναν οργανισμό, αλλά αποτελεί τον λιγότερο ασφαλή τύπο υπολογιστικού νέφους.

Το ιδιωτικό υπολογιστικό νέφος (private cloud) επιτρέπει στα συστήματα και τις υπηρεσίες να είναι αποκλειστικά και να λειτουργούν μόνο για έναν οργανισμό. Με αυτό τρόπο μπορεί να θεωρηθεί ότι προσφέρει αυξημένη ασφάλεια σε σχέση με τα υπόλοιπα μοντέλα ανάπτυξης υπολογιστικών νεφών λόγω του ιδιωτικού του χαρακτήρα.

Το κοινοτικό υπολογιστικό νέφος (community cloud) είναι ένα μοντέλο ανάπτυξης υπολογιστικού νέφους, το οποίο διαχειρίζεται από μία συγκεκριμένη κοινότητα και υποστηρίζει μία ομάδα υπηρεσιών. Σαν μοντέλο ανάπτυξης υπηρεσιών μπορεί να διαχειρίζεται από έναν συγκεκριμένο οργανισμό ή από κάποιο τρίτο μέρος.

Το υβριδικό υπολογιστικό νέφος (hybrid cloud) αποτελείται από τον συνδυασμό δύο ή περισσοτέρων διαφορετικών μοντέλων ανάπτυξης υπολογιστικού νέφους (δημόσια, ιδιωτικά, κοινοτικά). Τα μοντέλα ανάπτυξης παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με στόχο τη μεταφορά δεδομένων.

1.3. Μοντέλα υπηρεσιών υπολογιστικών νεφών

Τα μοντέλα υπηρεσιών είναι τα μοντέλα αναφοράς στα οποία βασίζεται η τεχνολογία των υπολογιστικών νεφών. Αυτά μπορούν να κατηγοριοποιηθούν σε τρία βασικά μοντέλα υπηρεσιών όπως προτείνονται και πάλι τόσο από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) όσο και από το Διεθνή Οργανισμό Τυποποίησης μαζί με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (ISO/IEC) και τα οποία παρατίθενται παρακάτω:

1. Υποδομή ως υπηρεσία (Infrastructure as a Service – IaaS)
2. Πλατφόρμα ως υπηρεσία (Platform as a Service – PaaS)
3. Λογισμικό ως υπηρεσία (Software as a Service – SaaS)

Υπάρχουν πολλά άλλα μοντέλα υπηρεσιών, τα οποία μπορούν να λάβουν τη μορφή κάποιας υπηρεσία. Μερικά παραδείγματα αυτών θα μπορούσαν να είναι το δίκτυο ως υπηρεσία, η επιχείρηση ως υπηρεσία, η αυθεντικοποίηση ως υπηρεσία, η βάση δεδομένων ως υπηρεσία ή η στρατηγική ως υπηρεσία.

Ένας τρόπος μελέτης του υπολογιστικού νέφους είναι ως στοίβα όπου το Λογισμικό ως Υπηρεσία είναι χτισμένο στην Πλατφόρμα ως Υπηρεσία και η οποία με τη σειρά της βασίζεται στην Υποδομή ως Υπηρεσία. Αυτό δεν είναι αντιπροσωπευτικό όλων των μοντέλων ανάπτυξης των υπολογιστικών νεφών, αλλά μπορεί να θεωρηθεί ένα μοντέλο, το οποίο κυριαρχεί.

Αξιοσημείωτο είναι ότι η υποδομή ως υπηρεσία (IaaS) είναι το πιο βασικό επίπεδο υπηρεσίας. Ακόμη, αξίζει να σημειωθεί ότι καθένα από τα μοντέλα υπηρεσιών χρησιμοποιεί το υποκείμενο του μοντέλο υπηρεσίας, δηλαδή, το κάθε μοντέλο υπηρεσίας κληρονομεί τον μηχανισμό ασφάλειας και διαχείρισης από το υποκείμενο μοντέλο.

Η υποδομή ως υπηρεσία είναι ένας τύπος υπηρεσίας στην οποία οι πάροχοι προσφέρουν πρόσβαση σε θεμελιώδεις πόρους όπως η υπολογιστική ισχύ (φυσικές μηχανές, εικονικές μηχανές) και σε χώρο αποθήκευσης (εικονική αποθήκευση) κατόπιν ζήτησης.

Η πλατφόρμα ως υπηρεσία (PaaS) είναι ένας τύπος λογισμικού, ο οποίος παρέχει μία πλατφόρμα – περιβάλλον στο υπολογιστικό νέφος, πάνω στο οποίο μπορούν να εκτελεστούν εφαρμογές και εργαλεία ανάπτυξης.

Το μοντέλο του λογισμικού ως υπηρεσία (SaaS) ένας τύπος λογισμικού, ο οποίος επιτρέπει τη χρήση εφαρμογών λογισμικού ως υπηρεσία στους τελικούς χρήστες.

1.4. Χρήσεις των υπολογιστικών νεφών

Οι καταναλωτές υπηρεσιών είναι τελικοί χρήστες ή οργανισμοί, οι οποίοι χρησιμοποιούν τα μοντέλα ανάπτυξης Λογισμικό, Πλατφόρμα ή Υποδομή ως Υπηρεσία. Αλληλεπιδρούν με διαφορετικές διεπαφές χρήστη (User Interfaces – UIs) και διεπαφές προγραμματισμού (Application Programming Interfaces – APIs) ανάλογα με τον τύπο της υπηρεσίας και τον ρόλο τους. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους, από τη μεριά τους, παρέχουν την υπηρεσία στον καταναλωτή, με τα καθήκοντα να ποικίλλουν ανάλογα με τον τύπο της υπηρεσίας.

Τα σενάρια χρήσης της τεχνολογίας υπολογιστικού νέφους είναι αρκετά. Στο παρόν έγγραφο παρουσιάζονται τα κυριότερα. Αρχικά, το σενάριο περίπτωσης χρήσης «Τελικός χρήστης στο υπολογιστικό νέφος (End User to Cloud)», περιλαμβάνει έναν τελικό χρήστη, ο οποίος έχει απευθείας πρόσβαση σε κάποια υπηρεσία υπολογιστικού νέφους, όπως είναι μία εφαρμογή λογισμικού, μέσω του προγράμματος περιήγησής του στον ιστό ή μέσω μίας κινητής συσκευής. Ακόμη, το σενάριο «επιχείρηση στο υπολογιστικό νέφος (Enterprise to Cloud)», το οποίο εστιάζει σε μία επιχείρηση, η οποία αξιοποιεί υπηρεσίες υπολογιστικού νέφους για κάποιες επιχειρηματικές ανάγκες, όπως είναι η αποθήκευση δεδομένων, η φιλοξενία (hosting) εφαρμογών ή η παροχή υποδομής. Ένα άλλο σενάριο είναι το σενάριο «Επιχείρηση στο Υπολογιστικό Νέφος στον Τελικό Χρήστη (Enterprise to Cloud to End User)». Στο παρόν σενάριο, μία επιχείρηση χρησιμοποιεί μία υπηρεσία υπολογιστικού νέφους, με στόχο να παραδώσει ένα προϊόν ή μία υπηρεσία σε έναν τελικό χρήστη, όπως μία εταιρεία, η οποία παρέχει στους υπαλλήλους της ένα σύστημα ηλεκτρονικού ταχυδρομείου, το οποίο βασίζεται σε υπολογιστικό νέφος. Επιπλέον, το

σενάριο «Επιχείρηση στο Υπολογιστικό Νέφος στην Επιχείρηση (Enterprise to Cloud to Enterprise)», το οποίο περιλαμβάνει πολλές επιχειρήσεις, οι οποίες χρησιμοποιούν μία υπηρεσία υπολογιστικού νέφους για συνεργασία, κοινή χρήση πόρων ή ανταλλαγή δεδομένων. Ένα ακόμη σενάριο χρήσης είναι η «Αλλαγή προμηθευτών υπολογιστικού νέφους (Changing Cloud Vendors)», όπου εδώ διερευνάται η διαδικασία μετάβασης από έναν προμηθευτή υπηρεσιών υπολογιστικού νέφους σε έναν άλλο, υπογραμμίζοντας με αυτό τον τρόπο τη σημασία της διαλειτουργικότητας και της φορητότητας των δεδομένων. Επιπλέον, το σενάριο «Ιδιωτικού Υπολογιστικού Νέφους (Private Cloud)». Αυτό το σενάριο περίπτωσης χρήσης ασχολείται με την ανάπτυξη ενός ιδιωτικού υπολογιστικού νέφους σε έναν οργανισμό, επιτρέποντας μεγαλύτερο έλεγχο των πόρων και της ασφάλειας. Τέλος, το σενάριο «Υβριδικό Υπολογιστικό Νέφος (Hybrid Cloud)», το οποίο συνδυάζει δημόσιες και ιδιωτικές υπηρεσίες υπολογιστικού νέφους, επιτρέποντας έτσι ευέλικτη κατανομή πόρων και βελτιστοποίηση του κόστους.

Τα παραπάνω σενάρια περιπτώσεων χρήσης καταδεικνύουν την ευελιξία και τα οφέλη του υπολογιστικού νέφους, όπως είναι η ταχεία παροχή, η επεκτασιμότητα και η εξοικονόμηση κόστους. Την ίδια στιγμή όμως, είναι εμφανής η ανάγκη για ανοιχτά πρότυπα και διαλειτουργικότητα προκειμένου να διασφαλιστεί η απρόσκοπτη ενσωμάτωση και φορητότητα σε διαφορετικά περιβάλλοντα υπολογιστικού νέφους.

2. Ασφαλή Υπολογιστικά Νέφη και Κρίσιμες Υποδομές

2.1. Ασφαλή Υπολογιστικά Νέφη

Οι υπηρεσίες, οι οποίες ποροσφέρονται από τα υπολογιστικά νέφη γίνονται ολοένα και περισσότερο μία ευρέως υιοθετημένη τεχνολογία, καθώς αποτελούν μία «μαγική» λύση για την παροχή υπηρεσιών μέσω του Διαδικτύου, αφού έχουν αρκετά πλεονεκτήματα, όπως η υψηλή επεκτασιμότητα, η ευελιξία υπηρεσιών, η κοινή χρήση και διαμόρφωση υπολογιστικών πόρων, αλλά και φυσικά η μείωση του κόστους. Όλα αυτά τα πλεονεκτήματα έχουν ενθαρρύνει μεγάλους οργανισμούς να αναθέσουν σε τρίτους την υποδομή πληροφορικής τους σε περιβάλλον υπολογιστικού νέφους, το οποίο προσφέρεται από τους παρόχους αυτών των υπηρεσιών. Ωστόσο, ταυτόχρονα με τα πλεονεκτήματά της αυτή η τεχνολογία, εμφανίζει και μειονεκτήματα. Ένα από τα σημαντικότερα μειονεκτήματα είναι ο τομέας της ασφάλειας και της ιδιωτικότητας, ο οποίος αποτελεί ένα σημαντικό εμπόδιο για την υιοθέτηση των υπηρεσιών υπολογιστικών νεφών.

Οι ανησυχίες, λοιπόν, οι οποίες διεγείρονται σχετικά με την ασφάλεια και το απόρρητο έχουν γίνει σημαντικό εμπόδιο για την υιοθέτηση υπηρεσιών υπολογιστικού νέφους. Είναι κοινώς γνωστό ότι το περιβάλλον στο οποίο είναι ανεπτυγμένες οι υπηρεσίες υπολογιστικών νεφών, είναι ευρέως κατανεμημένο και ιδιαίτερα δυναμικό. Ως εκ τούτου, πολλές απειλές και επιθέσεις σε υποδομές υπολογιστικών νεφών, όπως είναι τα δίκτυα ή η πρόσβαση σε υπηρεσίες είναι ικανές να απειλήσουν και να δημιουργήσουν προβλήματα τόσο στη διαθεσιμότητα όσο και στην ασφάλεια των υπηρεσιών υπολογιστικών νεφών. Αυτές οι επιθέσεις μπορεί να προέρχονται είτε από εξωτερικούς είτε από εσωτερικούς παράγοντες στο υπολογιστικό νέφος. Οι επιθέσεις, οι οποίες προέρχονται από εσωτερικό παράγοντα στο υπολογιστικό νέφος χωρίζονται σε δύο κατηγορίες. Πιο αναλυτικά, ο επιτιθέμενος μπορεί να είναι ένας κακόβουλος χρήστης, ο οποίος εργάζεται για τον πάροχο υπηρεσιών υπολογιστικών νεφών, ή ο επιτιθέμενος να είναι ένας «εσωτερικός» χρήστης, ο οποίος εργάζεται για τον οργανισμό που αναθέτει σε τρίτους την υποδομή πληροφορικής του, δηλαδή σε παρόχους υπηρεσιών υπολογιστικών νεφών.

Σε περίπτωση επιθέσεων στο υπολογιστικό νέφος, κρίνεται ευκολότερη η διασφάλιση εκ νέου της διαθεσιμότητας και η απόδοση των υπηρεσιών υπολογιστικών νεφών σε αντίθεση με τη διασφάλιση εκ νέου της διαθεσιμότητας των δεδομένων με απόλυτη ακεραιότητα, αρά και εμπιστευτικότητα. Σε ένα γενικότερο πλαίσιο, οι πάροχοι υπηρεσιών υπολογιστικών νεφών είναι

υπεύθυνοι για τη διασφάλιση της διαθεσιμότητας των υπηρεσιών, τις οποίες παρέχουν. Ωστόσο, η ευθύνη για τη διασφάλιση της γενικότερης ασφάλειας μοιράζεται μεταξύ των παρόχων υπηρεσιών υπολογιστικών νεφών και των οργανισμών – καταναλωτών των υπηρεσιών, με διαφορετικά ποσοστά ανάλογα με τους τύπους των υπηρεσιών υπολογιστικών νεφών, έχουν ζητήσει οι καταναλωτές. Πράγματι, σε ένα ανασφαλές περιβάλλον όπως είναι τα υπολογιστικά νέφη, τα ευαίσθητα δεδομένα είναι απαραίτητο να ελέγχονται. Αυτό έχει ως αποτέλεσμα, οι πάροχοι να είναι αναγκαίο να υιοθετήσουν τους απαραίτητους μηχανισμούς ασφαλείας και τα αντίμετρα, τα οποία θα έχουν ως αποτέλεσμα να μετριάσουν αυτές τις ανησυχίες, αλλά και να ενισχύσουν την εμπιστοσύνη για τις υπηρεσίες υπολογιστικών νεφών τις οποίες παρέχουν.

Ταυτόχρονα, τα δύο στοιχεία, τα οποία αναφέρθηκαν παραπάνω και είναι σημαντικό να μελετηθούν είναι η εμπιστευτικότητα και η ακεραιότητα των δεδομένων. Στην εμπιστευτικότητα, είναι απαραίτητο να διασφαλιστεί ότι τα δεδομένα παραμένουν εμπιστευτικά και αόρατα, όχι μόνο από τη δημοσιότητα αλλά ακόμη και στον πάροχο των υπηρεσιών υπολογιστικών νεφών. Πιο συγκεκριμένα, ακόμη και αν το κέντρο δεδομένων του παρόχου δεχθεί επίθεση, τα δεδομένα των καταναλωτών θα πρέπει να ελαχιστοποιηθεί η πιθανότητα είτε να κλαπούν είτε να επαναχρησιμοποιηθούν. Όσον αφορά την ακεραιότητα των δεδομένων, δηλαδή τη διατήρηση των δεδομένων στη σωστή αρχική τους μορφή. Αυτό σημαίνει ότι το σύστημα κρίνεται αναγκαίο να αποτρέπει την αδικαιολόγητη τροποποίηση των πληροφοριών και συγκεκριμένα την τροποποίηση από μη εξουσιοδοτημένους χρήστες, όπως και την εσφαλμένη τροποποίηση από εξουσιοδοτημένους χρήστες.

Συνολικά, επί του παρόντος, υπάρχουν πολλές απειλές και επιθέσεις στον κόσμο της πληροφορικής. Πράγματι, το περιβάλλον των υπολογιστικών νεφών είναι ευρέως διαδεδομένο και μπορεί, δυσκολότερα, να παρέχει τις υπηρεσίες σε χρήστες, οι οποίοι έχουν κακόβουλους σκοπούς. Επομένως, παρακάτω θα αναλυθούν αυτοί οι παράμετροι, οι οποίοι θα καθορίσουν αν το περιβάλλον υπολογιστικών νεφών είναι πιο ασφαλές σε σχέση με άλλα περιβάλλοντα.

2.2. Κρίσιμες υποδομές στα υπολογιστικά νέφη

Το υπολογιστικό νέφος λαμβάνει όλο και πιο αυξανόμενη κεντρική θέση στη σύγχρονη ψηφιακή υποδομή, αφού έχει οφέλη, όπως το χαμηλό κόστος και η επεκτασιμότητα. Ωστόσο,

αντιμετωπίζει προβλήματα ως προς την ανάπτυξη πολιτικής σχετικά με τον ουσιαστικό ρόλο του υπολογιστικού νέφους σε κρίσιμα συστήματα και την ανάγκη για κατάλληλες δομές εποπτείας.

Έχουν καταγραφεί αρκετά αξιοσημείωτα περιστατικά, τα οποία μπορούν να υπογραμμίσουν τους κινδύνους, οι οποίοι σχετίζονται με την υποδομή υπολογιστικού νέφους. Οι κυριότεροι τομείς, στους οποίους εστιάζεται η υιοθέτηση των υπηρεσιών υπολογιστικού νέφους σε τομείς ζωτικής σημασίας υποδομής είναι η υγειονομική περίθαλψη, οι μεταφορές, η ενέργεια, η άμυνα και οι χρηματοοικονομικές υπηρεσίες, δίνοντας έμφαση σε παράγοντες όπως η αποθήκευση δεδομένων, η επεκτασιμότητα και οι απαιτήσεις συνεχούς διαθεσιμότητας.

Ως αποτέλεσμα των παραπάνω, στη διαχείριση του κινδύνου στο υπολογιστικό νέφος, οι υπεύθυνοι χάραξης πολιτικής είναι αναγκαίο να εξετάσουν την ασφάλεια και την ανθεκτικότητα ως βασικές ανησυχίες. Δύο διακριτά χαρακτηριστικά του υπολογιστικού νέφους, τα οποία μπορούν να εξεταστούν είναι η σύνθετη εξάρτηση και ανάθεση ελέγχου και ορατότητας, τα οποία θέτουν προκλήσεις στις παραδοσιακές προσεγγίσεις διαχείρισης κινδύνου.

Συμπερασματικά, καλό είναι να παρασχεθούν συστάσεις πολιτικής για την ενίσχυση της ορατότητας των κινδύνων στο ευρύτερο περιβάλλον του υπολογιστικού νέφους για τομείς ζωτικής σημασίας υποδομών, προτείνοντας βελτιώσεις στα υπάρχοντα πλαίσια και τη δημιουργία διατομεακών δομών διαχείρισης κινδύνων. Είναι απαραίτητο να δοθεί σημασία στην αναγνώριση των ευρύτερων επιπτώσεων της ασφάλειας στο υπολογιστικό νέφος πέρα από μεμονωμένες υπηρεσίες, προτρέποντας τους υπεύθυνους χάραξης πολιτικής να δώσουν επειγόντως προτεραιότητα σε αυτό το ζήτημα.

Συνολικά, υπάρχει ανάγκη προσαρμογής των υπευθύνων χάραξης πολιτικής στο εξελισσόμενο περιβάλλον του υπολογιστικού νέφους, καθώς στη σύγχρονη τεχνολογική ζωή διαδραματίζει σημαντικό ρόλο στην υποστήριξη θεμελιωδών οικονομικών και πολιτικών δραστηριοτήτων.

2.3. Προκλήσεις απορρήτου στα υπολογιστικά νέφη

Η τεχνολογία υπολογιστικών νεφών έχει εξελιχθεί σε βασικό στοιχείο της βιομηχανίας πληροφορικής, προσφέροντας υπολογιστικούς πόρους, λογισμικό αλλά και υπηρεσίες μέσω του διαδικτύου. Ταυτόχρονα με τα οφέλη που παρέχει, οι ανησυχίες για την ασφάλεια και το απόρρητο

εξακολουθούν να υφίστανται, εμποδίζοντας με αυτό τον τρόπο την ευρεία υιοθέτηση της τεχνολογίας. Οι προκλήσεις, οι οποίες εμφανίζονται, περιλαμβάνουν μεταξύ άλλων απώλεια δεδομένων και παραβιάσεις απορρήτου. Διάφορα μοντέλα υπολογιστικών νεφών στοχεύουν στη βελτίωση της απόδοσης του οργανισμού, ωστόσο τα ζητήματα απορρήτου και ασφάλειας εξακολουθούν να υφίστανται, αφού δεδομένα χρηστών ανατίθενται σε τρίτους. Η αντιμετώπιση αυτών των ανησυχιών είναι πολύ σημαντική για την ενίσχυση της εμπιστοσύνης και τη διευκόλυνση της υιοθέτησης των υπηρεσιών υπολογιστικών νεφών.

Δύο σημαντικές ανησυχίες είναι η ασφάλεια και το απόρρητο στο περιβάλλον του υπολογιστικού νέφους, επηρεάζοντας έτσι την αξιοπιστία και την αποτελεσματικότητά του. Τα θέματα απορρήτου περιστρέφονται γύρω από την προστασία των προσωπικών δεδομένων, την αποθήκευση, τον έλεγχο πρόσβασης, τη διαγραφή δεδομένων, τη συμμόρφωση με τους νόμους αλλά και τις πολιτικές απορρήτου. Η δημοτικότητα, την οποία φέρει το υπολογιστικό νέφος μεταξύ των οργανισμών, ιδιαίτερα από τους μικρομεσαίους, έχει επιταχυνθεί λόγω της προσβασιμότητας και της οικονομικής του αποδοτικότητας. Ωστόσο, η αυξανόμενη υιοθέτηση εγείρει επίσης κινδύνους για την ασφάλεια και την ιδιωτικότητα, απειλώντας την πνευματική ιδιοκτησία και την προστασία των προσωπικών πληροφοριών.

Οι παραβιάσεις του απορρήτου και η μη εξουσιοδοτημένη πρόσβαση ενέχουν σοβαρούς κινδύνους για τους χρήστες των υπηρεσιών υπολογιστικού νέφους, τονίζοντας έτσι την ανάγκη για αυστηρά μέτρα ασφαλείας. Πιο συγκεκριμένα, καλό είναι να δίνεται έμφαση στην ασφάλεια των συστημάτων Διαδικτύου των Πραγμάτων (Internet of Things – IoT) για την προστασία κρίσιμων προσωπικών πληροφοριών. Ακόμη, μεγάλη σημασία κρίνεται αναγκαίο να δίνεται στα μεγάλα δεδομένα για την ενημέρωση των εταιρικών πολιτικών και την αντιμετώπιση κοινωνικών ζητημάτων, αλλά και γενικότερα στο εξελισσόμενο τοπίο του υπολογιστικού νέφους.

Όπως αποτυπώνεται και παραπάνω, μεγάλη σημασία είναι απαραίτητο να δίνεται στη προστασία ευαίσθητων δεδομένων σε περιβάλλοντα υπολογιστικού νέφους, συστημάτων διαδικτύου των πραγμάτων και μεγάλων δεδομένων. Υπογραμμίζεται, ακόμη, η ανάγκη προστασίας των μεταδιδόμενων δεδομένων από παθητικές επιθέσεις για τη διασφάλιση του απορρήτου των καταναλωτών του υπολογιστικού νέφους. Η τεχνολογία των συστημάτων διαδικτύου των Πραγμάτων μπορεί να παρέχει διευκόλυνση στην επικοινωνία αλλά παρουσιάζει και ευπάθεια σε επιθέσεις που διακυβεύουν τα δεδομένα των χρηστών. Επιπλέον, τεράστιες

δυνατότητες και εφαρμογές έχουν τα μεγάλα δεδομένα, ιδιαίτερα στις βιολογικές επιστήμες, ενώ υπογραμμίζονται οι προκλήσεις της διαχείρισης μεγάλου όγκου δεδομένων, τα οποία παράγονται γρήγορα. Παρά την αυξανόμενη δημοτικότητα του περιβάλλοντος των υπολογιστικών νεφών, οι ανησυχίες για την ασφάλεια και το απόρρητο εξακολουθούν να υφίστανται, εμποδίζοντας την ευρεία υιοθέτησή του. Ωστόσο, η προώθηση αμυντικών μέτρων είναι ζωτικής σημασίας για τη διασφάλιση ενός ασφαλούς περιβάλλοντος υπολογιστικού νέφους.

Η τεχνολογία υπολογιστικών νεφών παρουσιάζει ευκαιρίες και προκλήσεις, ιδιαίτερα όσον αφορά την ιδιωτικότητα και την ασφάλεια. Η απεριόριστη πρόσβαση στο δίκτυο και την αποθήκευση που προσφέρεται από τους παρόχους, συχνά με χαμηλό κόστος ή με δωρεάν δοκιμές, μπορεί να οδηγήσει σε κακή χρήση ευαίσθητων δεδομένων που επιδεινώνεται από την έλλειψη ελέγχου που έχουν οι χρήστες σχετικά με τον πολλαπλασιασμό των δεδομένων τους και τα αντίγραφα ασφαλείας. Οι κυβερνητικοί κανονισμοί (νόμοι) και οι συμβατικές υποχρεώσεις στοχεύουν στην προστασία των δεδομένων, αλλά εξακολουθούν να υπάρχουν προκλήσεις, όπως τα κυβερνητικά αιτήματα για πρόσβαση σε δεδομένα. Άλλα περιστατικά όπως η επίθεση στον πάροχο υπηρεσιών υπολογιστικού νέφους Google υπογραμμίζουν την ευπάθεια των δεδομένων οργανισμών και χρηστών που είναι αποθηκευμένα στο υπολογιστικό νέφος. Επιπλέον, δημιουργούνται ανησυχίες όταν τα δεδομένα αποθηκεύονται σε δευτερεύουσα μνήμη για τη μείωση του κόστους.

Την ίδια στιγμή, οι κακόβουλοι εμπιστευτικοί παράγοντες αποτελούν σημαντική απειλή, καθώς οι πάροχοι υπηρεσιών υπολογιστικού νέφους ενδέχεται να μην αποκαλύπτουν την πρόσβαση των εργαζομένων σε περιουσιακά στοιχεία, επιτρέποντας εσωτερικές απειλές. Οι χρήστες συχνά στερούνται λογοδοσίας για την ασφάλεια των δεδομένων τους, τα οποία είναι αποθηκευμένα στο υπολογιστικό νέφος, κάτι που απαιτεί δυναμική παροχή δεδομένων και διαφάνεια σχετικά με τις τοποθεσίες αποθήκευσης δεδομένων και τις πολιτικές διατήρησης τους. Το γεγονός αυτό είναι ζωτικής σημασίας για την αντιμετώπιση των προβλημάτων απορρήτου. Για τους χρήστες των υπολογιστικών νεφών είναι επιτακτική ανάγκη να λαμβάνουν επιβεβαίωση διαγραφής δεδομένων και να εφαρμόζουν επαρκή μέτρα ελέγχου πρόσβασης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και κακής χρήσης δεδομένων. Τέλος, ο πολλαπλασιασμός πολλαπλών αντιγράφων δεδομένων εγείρει επίσης ανησυχίες για απώλεια ή διαρροή δεδομένων, υπογραμμίζοντας τη σημασία των τακτικών διαδικασιών εκκαθάρισης δεδομένων.

Η ασφάλεια είναι πρωταρχικής σημασίας στην τεχνολογία υπολογιστικού νέφους, με στόχο την προστασία ευαίσθητων δεδομένων από διάφορα τρωτά σημεία και επιθέσεις. Το τοπίο του υπολογιστικού νέφους θέτει διάφορους παράγοντες κινδύνου. Αρχικά, η πολυμίσθωση εισάγει τρωτά σημεία στην υποδομή υπολογιστικού νέφους εκτελώντας ένα πρόγραμμα σε πολλά μηχανήματα ταυτόχρονα και μοιράζοντας πόρους μεταξύ διαφορετικών χρηστών. Ταυτόχρονα, η πρόσβαση σε ευαίσθητες πληροφορίες στο υπολογιστικό νέφος είναι επιρρεπής σε επιθέσεις, επιτρέποντας στους εισβολείς να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα για πιθανή κακή χρήση. Η διαθεσιμότητα δεδομένων στο υπολογιστικό νέφος είναι απαραίτητη, ωστόσο προκύπτουν προκλήσεις στην ανάκτηση αντιγράφων ασφαλείας σε περίπτωση αποτυχίας, με αποτέλεσμα την απώλεια της εμπιστοσύνης των καταναλωτών. Η εμπιστοσύνη παραμένει μία σημαντική ανησυχία, με τους οργανισμούς – καταναλωτές να διστάζουν, ακόμα, να εμπιστευτούν πλήρως τους παρόχους υπολογιστικών νεφών με τα προσωπικά τους δεδομένα, υπογραμμίζοντας την ανάγκη για ισχυρά μέτρα ασφαλείας. Παράλληλα, οι μηχανισμοί ελέγχου είναι ζωτικής σημασίας για την παρακολούθηση και τη διασφάλιση της ακεραιότητας των δεδομένων, αλλά αυτή τη στιγμή τα τρέχοντα συστήματα υπολογιστικών νεφών αγωνίζονται να παρέχουν εξωτερικό έλεγχο χωρίς να διακυβεύεται η ακεραιότητα των δεδομένων. Τέλος, η αντιμετώπιση αυτών των θεμάτων ασφάλειας είναι απαραίτητη για την ενίσχυση της εμπιστοσύνης μεταξύ των χρηστών των υπηρεσιών υπολογιστικού νέφους και για τη βελτίωση της συνολικής στάσης ασφαλείας των περιβαλλόντων υπολογιστικού νέφους.

Για την αντιμετώπιση των προβλημάτων απορρήτου στο υπολογιστικό νέφος, τόσο οι χρήστες υπηρεσιών υπολογιστικού νέφους όσο και οι πάροχοι μπορούν να λάβουν προληπτικά μέτρα. Οι χρήστες υπηρεσιών υπολογιστικού νέφους καλό είναι να εξετάζουν προσεκτικά τις πολιτικές απορρήτου των παρόχων υπηρεσιών προτού αποθηκεύσουν δεδομένα, εξετάζοντας εναλλακτικούς παρόχους εάν είναι απαραίτητο. Κρίνεται αναγκαίο να γνωρίζουν τα δικαιώματά τους σχετικά με τις πληροφορίες των χρηστών του δημόσιου υπολογιστικού νέφοπυς και να διασφαλίζουν τη δυνατότητα να ζητούν αφαίρεση δεδομένων από το υπολογιστικό νέφος. Η αποφυγή της αποθήκευσης ευαίσθητων δεδομένων που θα μπορούσαν να είναι επωφελείς για ανταγωνιστές ή κρατικούς φορείς είναι πολύ σημαντική. Τέλος, η διαβούλευση με τις ομάδες τεχνικής υποστήριξης μπορεί να βοηθήσει στη διασφάλιση της ασφάλειας των δεδομένων.

Από την μεριά τους οι πάροχοι υπηρεσιών υπολογιστικού νέφους είναι απαραίτητο να διασφαλίζουν τη συμμόρφωση με τους νόμους, τις πολιτικές και τις δεσμεύσεις, αποκαλύπτοντας τη φυσική τοποθεσία των δεδομένων των χρηστών και διατηρώντας αυστηρή απομόνωση δεδομένων. Η εκπαίδευση των χρηστών σχετικά με τους μηχανισμούς προστασίας, η κατάρτιση σχεδίων ταχείας αποκατάστασης για καταστροφές ή παραβιάσεις και η ενημέρωση των χρηστών σχετικά με τους σχετικούς νόμους και κανονισμούς είναι αναγκαία. Οι πάροχοι θα πρέπει επίσης να ενημερώνουν εκ των προτέρων τις αλλαγές της πολιτικής απορρήτου και να διατηρούν λεπτομερή αρχεία καταγραφής δεδομένων χρηστών για λόγους διαφάνειας. Με την εφαρμογή αυτών και άλλων μέτρων, τόσο οι χρήστες όσο και οι πάροχοι μπορούν να ενισχύσουν την προστασία του απορρήτου και την εμπιστοσύνη σε περιβάλλοντα υπολογιστικού νέφους.

Συμπερασματικά, η ταχεία επέκταση του περιβάλλοντος του υπολογιστικού νέφους έχει προκαλέσει σημαντικές ανησυχίες για την ασφάλεια και το απόρρητο, συμπεριλαμβανομένων των παραβιάσεων του απορρήτου και της παράνομης πρόσβασης. Οι ειδικοί έχουν προτείνει διάφορες λύσεις απορρήτου των δεδομένων για την αντιμετώπιση αυτών των ζητημάτων. Η εμπιστοσύνη είναι απαραίτητη μεταξύ των εταιρειών, των χρηστών και των παρόχων υπηρεσιών υπολογιστικού νέφους, καθώς οι οργανισμοί θα μεταφέρουν τα δεδομένα τους στο υπολογιστικό νέφος μόνο εάν εδραιωθεί εμπιστοσύνη. Παρά τις προσπάθειες για βελτίωση της εμπιστοσύνης, εξακολουθούν να υπάρχουν κενά στο υπολογιστικό νέφος, τα οποία είναι αναγκαίο να αντιμετωπιστούν από τους παρόχους. Με τις εξελίξεις στην τεχνολογία υπολογιστικού νέφους, υπάρχει μεγαλύτερη προσβασιμότητα στις υπηρεσίες υπολογιστικού νέφους τόσο για τους δημόσιους όσο και για ιδιωτικούς οργανισμούς. Η εκπαίδευση του κοινού σχετικά με το απόρρητο των δεδομένων είναι απαραίτητη για την ανάπτυξη του υπολογιστικού νέφους, την προώθηση πρακτικών υπεύθυνης διαχείρισης δεδομένων και την αύξηση της ευαισθητοποίησης σχετικά με την ασφάλεια του Διαδικτύου. Τέλος, η ενίσχυση της ευαισθητοποίησης για το απόρρητο των δεδομένων μπορεί να βοηθήσει στον μετριασμό των κινδύνων ακούσιας διαρροής ευαίσθητων πληροφοριών.

2.4. Απόρρητο των Υπολογιστικών Νεφών για προσωπικά δεδομένα

Τα Νέφη Προσωπικών Δεδομένων (Personal Data Cloud – PDC) είναι λύσεις διαχείρισης δεδομένων, τα οποία έχουν σχεδιαστεί για να παρέχουν στους χρήστες τον έλεγχο των δεδομένων τους, παρέχοντας παράλληλα τις δυνατότητες της συλλογής και της αποθήκευσης δεδομένων. Τα

νέφη προσωπικών δεδομένων δίνουν προτεραιότητα στα στοιχεία που βελτιώνουν το απόρρητο, επιτρέποντας όμως στους χρήστες να διαχειρίζονται τα δεδομένα τους και να αποφασίζουν με ποιον θα τα μοιραστούν. Κρίνεται αναγκαίο να προσδιοριστούν τα βασικά αρχιτεκτονικά στοιχεία των νεφών προσωπικών δεδομένων και να αξιολογηθούν τα χαρακτηριστικά ιδιωτικότητας και ασφάλειας, ιδιαίτερα στο πλαίσιο των εφαρμογών υγείας για κινητά. Τα νέφη προσωπικών δεδομένων προσφέρουν πολλά υποσχόμενα χαρακτηριστικά, όπως η επικέντρωση στο χρήστη και το απόρρητο από το σχεδιασμό, την ίδια στιγμή όμως υπάρχουν σημαντικά κενά στην εφαρμογή, όπως περιορισμένες πρακτικές ελαχιστοποίησης δεδομένων και κρυπτογράφησης. Παρατηρούνται προκλήσεις όσον αφορά την εξισορρόπηση της ευαισθησίας και της χρηστικότητας, την επιβολή των δικαιωμάτων των χρηστών, τη θέσπιση προτύπων φορητότητας δεδομένων αλλά και τη βελτίωση της κρυπτογραφίας. Συστάσεις που μπορούν να δοθούν, περιλαμβάνουν την προώθηση τεχνολογιών, οι οποίες βελτιώνουν το απόρρητο, τη βελτίωση των διεπαφών ελέγχου χρήστη, την εφαρμογή μηχανισμών διαχείρισης των δικαιωμάτων, την προώθηση προτύπων φορητότητας δεδομένων και την ενίσχυση των μέτρων ασφαλείας μέσω ασφαλούς κωδικοποίησης και τακτικών ελέγχων. Συνολικά, καλό είναι να δοθεί σημασία στην αντιμετώπιση των προκλήσεων της ιδιωτικής ζωής και της ασφάλειας για τη διευκόλυνση της ευρύτερης υιοθέτησης και εμπιστοσύνης των νεφών προσωπικών δεδομένων.

2.5. Ασφάλεια και απόρρητο επιχειρηματικών ροών εργασιών

Η αυξανόμενη επικράτηση της τεχνολογίας από ιδιώτες και δημόσιους ή ιδιωτικούς οργανισμούς έχει κάνει το περιβάλλον του υπολογιστικού νέφους δημοφιλές λόγω της δυνατότητας που μπορεί να προσφέρει υπολογιστικούς πόρους κατά απαίτηση. Ωστόσο, οι ανησυχίες για το απόρρητο και την ασφάλεια εμποδίζουν την ευρεία υιοθέτηση του, ιδιαίτερα για ροές εργασιών οργανισμών, οι οποίοι ασχολούνται με ευαίσθητα δεδομένα. Πιο συγκεκριμένα, παρατηροούνται λύσεις αφαλείας κατά τις φάσεις μοντελοποίησης και εκτέλεσης των ροών εργασίας αλλά ανεπαρκής κάλυψη των φάσεων παρακολούθησης και προσαρμογής. Επομένως, το κενό, το οποίο προκύπτει, αφήνει μία σημαντική ανάγκη για έρευνα όσον αφορά τον εντοπισμό, την πρόληψη και την αντίδραση σε παραβιάσεις ασφαλείας κατά τις φάσεις ροών εργασιών, οι οποίες βασίζονται στην τεχνολογία υπολογιστικού νέφους.

Οι ροές εργασίας, οι οποίες περιλαμβάνουν υπολογιστικές εργασίες και οι οποίες συνδέονται με ροές δεδομένων και ελέγχου, χρησιμοποιούνται συνήθως σε επιστημονικά και επιχειρηματικά πλαίσια. Οι επιστημονικές ροές εργασίας περιλαμβάνουν εκτεταμένη επεξεργασία δεδομένων, σε σύγκριση με τις επιχειρηματικές ροές εργασίας, οι οποίες δίνουν έμφαση και προτεραιότητα στην αυτοματοποίηση διαδικασιών στα πληροφοριακά συστήματα. Η τεχνολογία υπολογιστικών νεφών διαδραματίζει πολύ σημαντικό ρόλο στη διαχείριση ροής εργασιών. Αυτό συμβαίνει, καθώς, μπορεί να προσφέρει υπολογιστικούς πόρους κατά απαίτηση, μειώνοντας με αυτό τον τρόπο το κόστος και βελτιώνοντας παράλληλα την ποιότητα της υπηρεσίας. Ταυτόχρονα όμως με τα πλεονεκτήματα της τεχνολογίας αυτής, παρουσιάζονται και ανησυχίες για την ασφάλεια, ειδικότερα όσον αφορά το χειρισμό ευαίσθητων δεδομένων και τις κακόβουλες επιθέσεις. Ένα σημαντικό κενό υφίσταται στην αντιμετώπιση της ασφάλειας σε όλη τη διάρκεια της ζωής των ροών εργασίας, οι οποίες βασίζονται σε τεχνολογία υπολογιστικών νεφών κατά τη φάση της μοντελοποίησης των ιδιοτήτων ασφάλειας των ροών εργασίας.

Στη φάση της μοντελοποίησης, λοιπόν, κρίσιμη θεωρείται η αυτοματοποίηση των απαιτήσεων ασφαλείας. Μία σημαντική προσέγγιση είναι η δημιουργία ενός τυπικού μοντέλου ροής εργασιών, το οποίο πληροί όλες τις απαιτήσεις ασφαλείας και ταυτόχρονα επιτρέπει την διευκόλυνση της αυτοματοποίησης. Παρόλα αυτά, οι υφιστάμενες γλώσσες μοντελοποίησης, οι οποίες δίνουν έμφαση στην ασφάλεια προτείνουν συνήθως τα δικά τους μοντέλα, γεγονός που περιορίζει την ευρύτερη υιοθέτηση. Παράλληλα, ένα άλλο πρόβλημα, το οποίο παρατηρείται, είναι η έλλειψη αυτοματοποιημένου ελέγχου μοντέλου, προκειμένου να διασφαλιστεί ότι πληρούνται οι απαιτήσεις ασφάλειας της ροής εργασιών.

Για τη φάση ανάπτυξης και εκτέλεσης, οι προκλήσεις ασφαλείας στις υποδομές υπολογιστικών νεφών συνήθως οφείλονται στην τεχνολογία εικονικοποίησης (Virtualization Technology), για τον λόγο αυτό απαιτείται η εξέταση της σχέσης μεταξύ της τεχνολογίας εικονικοποίησης και των ιδιοτήτων ασφάλειας. Την ίδια στιγμή, υπάρχει ανάγκη για μία μέθοδο προγραμματισμού με επίγνωση της ασφάλειας για την επιλογή της κατάλληλης τεχνολογίας εικονικοποίησης σε επίπεδα εργασιών και ροής εργασίας με βάση τα χαρακτηριστικά και τις απαιτήσεις των χρηστών.

Κατά τη φάση παρακολούθησης, ανάλυσης και προσαρμογής, παρατηρείται αξιοσημείωτο κενό. Δεν εντοπίζεται αξιόπιστη και επεκτάσιμη στρατηγική για τον εντοπισμό όλων των πιθανών

επιθέσεων κατά την εκτέλεση της ροής εργασίας. Επιπλέον, υφίστατι έλλειψη προσεγγίσεων για την πρόληψη και την αντίδραση σε παραβιάσεις ασφάλειας και απορρήτου, ειδικά για τις επιχειρηματικές ροές εργασίας. Τα τρέχοντα συστήματα δεν θεωρούν την τεχνολογία υπολογιστικών νεφών ή τους κακόβουλους χρήστες ως πιθανές απειλές, την στιγμή που υπάρχει ανάγκη για ένα σύστημα διαχείρισης ροής εργασιών, το οποίο βασίζεται σε περιβάλλοντα υπολογιστικών νεφών με πολλαπλές μονάδες προσαρμογής.

Οι μελλοντικές κατευθύνσεις έρευνας περιλαμβάνουν τη δημιουργία ενός τυπικού μοντέλου ροής εργασίας που καταγράφει θεμελιώδεις αρχές ασφάλειας, ενσωματώνοντας στρατηγικές προσαρμογής για κάθε εργασία, ανάπτυξη μηχανισμών για τη λήψη βέλτιστων επιλογών σε περιβάλλοντα cloud, ενίσχυση των δυνατοτήτων παρακολούθησης για τον εντοπισμό παραβιάσεων ασφαλείας και ενσωμάτωση πολλαπλών μονάδων προσαρμογής στην αρχιτεκτονική του συστήματος διαχείρισης ροής εργασιών (Work flow Management System – WfMS) εξασφαλίζουν ασφάλεια και προσαρμοστικότητα.

3. Ασφάλεια και Απόρρητο Υπολογιστικών Νεφών

3.1. Ασφάλεια Δεδομένων και Προστασία του Απόρρητο σε Περιβάλλοντα Υπολογιστικών Νεφών

Η ραγδαία εξέλιξη σε επίπεδο τεχνολογικών επιτευγμάτων, όπως είναι το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT), οι έξυπνες πόλεις (smart citites), ο ψηφιακός μετασχηματισμός σε δημόσιους και ιδιωτικούς οργανισμούς αλλά και η αναπτυσσόμενη ψηφιακή οικονομία, έχει οδηγήσει σε μαζική παραγωγή και συλλογή δεδομένων. Αυτή η αύξηση στην κυκλοφορία των δεδομένων έχει φέρει δυσκολίες στις λύσεις αποθήκευσης, κάτι το οποίο έχει σαν αποτέλεσμα την ταχεία ανάπτυξη στον τομέα αποθήκευσης και ιδιαιτέρως στα συστήματα αποθήκευσης σε περιβάλλοντα υπολογιστικού νέφους. Μεγάλη κινητικότητα μεταφοράς δεδομένων σε περιβάλλοντα υπολογιστικού νέφους από κυβερνήσεις, δημόσιους και ιδιωτικούς οργανισμούς αλλά ακόμη και από μεμονωμένους χρήστες ιδιώτες, αναγνωρίζοντας τον πολύ κρίσιμο ρόλο του στη σύγχρονη ζωή. Παρόλο που αυτή η μεταφορά προσφέρει ευκαιρίες για δημιουργία πλούτου, ενέχει όμως την ίδια στιγμή σημαντικές ανησυχίες όπως είναι οι παραβιάσεις της ιδιωτικής ζωής, η παράνομη πρόσβαση και η διαρροή δεδομένων.

Η ταχεία ανάπτυξη της τεχνολογίας υπολογιστικών νεφών έχει προσελκύσει μεγάλες εταιρείες όπως η Amazon, η Google και η Microsoft, οι οποίες εξελίσσουν και βελτιστοποιούν συνεχώς τις υπηρεσίες τους προκειμένου να φιλοξενήσουν περισσότερους χρήστες. Ωστόσο, οι ανησυχίες γύρω από την ασφάλεια και το απόρρητο των δεδομένων παραμένουν σημαντικά εμπόδια στην ευρεία υιοθέτηση, καθώς από τους παρόχους υπηρεσιών υπολογιστικών νεφών απουσιάζουν βασικοί τομείς, όπως η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, ο έλεγχος (audit) και ο έλεγχος από ρυθμιστικές αρχές. Οι υφιστάμενοι νόμοι περί απορρήτου δεν κρίνονται ικανοί να στηρίξουν τη νέα δυναμική των σχέσεων που αναπτύσσονται γύρω από τα περιβάλλοντα υπολογιστικών νεφών, στις οποίες εμπλέκονται πολλά μέρη. Ο πολλαπλασιασμός της αποθήκευσης δεδομένων σε πολλές τοποθεσίες και των υπηρεσιών επιδεινώνει τα ζητήματα απορρήτου. Η ενημέρωση των κανονισμών απορρήτου για την αντιμετώπιση κενών στα περιβάλλοντα υπολογιστικών νεφών θα μπορούσε να ενθαρρύνει περισσότερους χρήστες να αγκαλιάσουν την τεχνολογία, οδηγώντας τελικά στην ευρεία υιοθέτηση της.

Η τεχνολογία υπολογιστικών νεφών προσφέρει κλιμακούμενες, αξιόπιστες και γρήγορα προσβάσιμες υπηρεσίες, αλλά ταυτόχρονα εγκυμονεί προκλήσεις ασφάλειας και απορρήτου. Οι βασικές πτυχές ασφάλειας που παρέχουν τα περιβάλλοντα υπολογιστικών νεφών είναι η διαθεσιμότητα, κατά την οποία τα συστήματα είναι απαραίτητο να διασφαλίζουν την αδιάλειπτη πρόσβαση για τους χρήστες. Η εμπιστευτικότητα, η οποία αφορά την διατήρηση της αφάλειας για τα δεδομένα των χρηστών. Ακόμη, η ακεραιότητα των δεδομένων, η οποία διασφαλίζει την ακεραιότητα των δεδομένων των χρηστών στα συστήματα. Ο αποκεντρωμένος έλεγχος ροής πληροφοριών διασφαλίζει την ασφάλεια και το απόρρητο των δεδομένων και ρυθμίζει την χρήση συστημάτων και εφαρμογών. Τέλος, ο έλεγχος μέσω της παρακολούθησης των δραστηριοτήτων σε περιβάλλοντα υπολογιστικών νεφών είναι πολύ σημαντικός για σκοπούς ασφάλειας και συμμόρφωσης.

Στο τομέα της ασφάλειας στα περιβάλλοντα υπολογιστικών νεφών παρουσιάζονται αρκετές απειλές, τα οποία μπορεί να εκμεταλλευτούν τρωτά σημεία και να δημιουργήσουν ζητήματα ασφάλειας ή απορρήτου των δεδομένων. Ενδεικτικά, πιθανές απειλές είναι οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service – DDoS) και οι επιθέσεις man-in-the-middle. Ακόμη, απειλές μπορεί να προκύψουν από ευπάθειες όπως είναι οι ευάλωτες διεπαφές προγραμματισμού ή η διαρροή και απώλεια δεδομένων και η πειρατεία λογαριασμών.

Η υιοθέτηση της τεχνολογίας υπολογιστικών νεφών εγείρει αξιοσημείωτες ανησυχίες για το απόρρητο λόγω της αποθήκευσης και διαχείρισης των ευαίσθητων πληροφοριών των χρηστών από τους παρόχους υπηρεσιών υπολογιστικών νεφών. Οι υφιστάμενοι νόμοι περί απορρήτου δεν επαρκούν ώστε να αντιμετωπίσουν αποτελεσματικά την πολυπλοκότητα του περιβάλλοντος υπολογιστικών νεφών, το οποίο περιλαμβάνει μία νέα σχέση μεταξύ χρηστών και παρόχων υπηρεσιών υπολογιστικού νέφους.

Τα νομικά ζητήματα αποτελούν σημαντικό παράγοντα ανησυχίας, καθώς οι υφιστάμενες πρακτικές περί απορρήτου κρίνονται ανεπαρκείς για την προστασία των δεδομένων των χρηστών στα περιβάλλοντα υπολογιστικών νεφών. Ακόμη, η αποθήκευση δεδομένων σε πολλαπλές τοποθεσίες δημιουργεί διάφορους κινδύνους και προκλήσεις.

Η αντιμετώπιση των ανησυχιών και ο μετριασμός των ζητημάτων ασφαλείας θα βοηθήσουν στη διασφάλιση του απορρήτου, στην ακεραιότητα των δεδομένων αλλά και παράλληλα στην προσαρμοστικότητα και την ευελιξία στο μετριασμό μελλοντικών απειλών.

Ακόμη, θα βοηθήσουν στην οικοδόμηση εμπιστοσύνης και στη διασφάλιση της λογοδοσίας για τους παρόχους υπηρεσιών υπολογιστικών νεφών και τους χρήστες τους. Για την αντιμετώπιση, λοιπόν, των ζητημάτων καλό είναι να θεσπιστεί ένα σύνολο ελέγχων κυβερνοασφάλειας για τους παρόχους υπηρεσιών υπολογιστικών νεφών και για τους χρήστες. Επιπλέον, κρίνεται αναγκαίο να γίνεται χρήση ισχυρών αμυντικών μηχανισμών, όπως είναι οι μηχανισμοί άμυνας επιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS) και η υιοθέτηση λύσεων όπως Zero Knowledge Proofs (ZKPs), Distributed Zero Knowledge Proofs (DIZK), Third-Party Auditors (TPAs). Άλλες πτυχές ασφάλειας είναι ο έλεγχος πρόσβασης και η διαχείριση ταυτότητας. Η προστασία συστημάτων πληροφοριών και εγκαταστάσεων επεξεργασίας δεδομένων, η διαχείριση ασφάλειας δικτύων και η ασφάλεια φορητών συσκευών. Ακόμη, η προστασία δεδομένων και πληροφοριών, η κρυπτογραφία και η διαχείριση περιστατικών και απειλών στον κυβερνοχώρο αποτελούν βοηθητικά συστατικά για τα ζητήματα ασφάλειας. Την ίδια στιγμή, η φυσική ασφάλεια, η ασφάλεια διαδικτυακών εφαρμογών, η διαχείριση κλειδιών συμπληρώνουν μία σειρά από προτάσεις. Τέλος, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST) προτείνει τη θέσπιση σαφών όρων για συμφωνίες υπηρεσιών υπολογιστικού νέφους, οι οποίοι μπορεί να περιλαμβάνουν πολιτικές απορρήτου, πολιτικές αποδεκτής χρήσης, όρους χρήσης και συμφωνία επιπέδου υπηρεσίας (Service Level Agreement – SLA).

Συμπερασματικά, οι σημαντικές ανησυχίες για την ασφάλεια και το απόρρητο λειτουργούν σαν εμπόδια στην ευρεία υιοθέτηση της τεχνολογίας υπολογιστικού νέφους. Η κατανόηση αλλά και η αντιμετώπιση των ζητημάτων ασφαλείας και απορρήτου είναι ζωτικής σημασίας για τους χρήστες και για την προστασία των ευαίσθητων πληροφοριών τους σε περιβάλλοντα υπολογιστικών νεφών. Ορισμένοι πάροχοι υπηρεσιών υπολογιστικών νεφών αντιμετωπίζουν αυτές τις ανησυχίες, αλλά οι υπάρχουσες στρατηγικές κρίνονται ανεπαρκείς. Η ανάπτυξη πιο ισχυρών μέτρων ασφαλείας σε περιβάλλοντα υπολογιστικών νεφών για την επίτευξη των στόχων ασφαλείας θα οδηγήσει στην ευρεία υιοθέτηση του.

3.2. Απειλές για την ασφάλεια και ζητήματα απορρήτου

Οι κύριοι τομείς της ασφάλεια στα περιβάλλοντα υπολογιστικών νεφών είναι τρεις και αφορούν την ασφάλεια υποδομής, την ασφάλεια εφαρμογών και την ασφάλεια δεδομένων. Η

ασφάλεια της υποδομής περιλαμβάνει τη φυσική προστασία δικτύου, της αποθήκευσης και του διακομιστή. Την ίδια στιγμή, η ασφάλεια εφαρμογών εστιάζει στην ασφάλεια διαδικτυακών εφαρμογών και εφαρμογών API. Η ασφάλεια δεδομένων συνεπάγεται την προστασία ευαίσθητων δεδομένων χρηστών, οικονομικών πληροφοριών και πνευματικής ιδιοκτησίας, τα οποία αποθηκεύονται και τελούν υπό επεξεργασία σε περιβάλλοντα υπολογιστικών νεφών.

Η οικοδόμηση ενός ασφαλούς υπολογιστικού νέφους και η αξιολόγηση των κινδύνων ασφαλείας, των απειλών και των υφιστάμενων αμυντικών μηχανισμών σε επίπεδο οργανισμών είναι ζωτικής σημασίας για την προστασία ευαίσθητων δεδομένων, τη συμμόρφωση με τις κανονιστικές απαιτήσεις, τον μετριασμό των τρωτών σημείων και απειλών στον κυβερνοχώρο και ένα πλάνο διασφάλισης της επιχειρηματικής συνέχειας. Στη συνέχεια, αναλύονται οι κυριότερες απειλές και τρωτά σημεία, τα οποία συναντώνται και σχετίζονται με την τεχνολογία των υπολογιστικών νεφών και στα οποία συμπεριλαμβάνονται οι παραβιάσεις και απώλειες δεδομένων, οι επιθέσεις άρνησης υπηρεσίας, τα ευάλωτα συστήματα και API, ο ελλιπής έλεγχος ταυτότητας και οι παραβιάσεις λογαριασμών.

Γενικά, οι απειλές, οι οποίες παρατηρούνται σε περιβάλλοντα υπολογιστικών νεφών μπορούν να χωριστούν σε κατηγορίες όπως είναι οι ευπάθειες σε επίπεδο εφαρμογής και διεπαφής, στην οποία οι απειλές αφορούν τρωτά σημεία στο επίπεδο εφαρμογής και διεπαφής και τα οποία μπορεί να περιλαμβάνουν ζητήματα όπως ανασφαλή API και ελλιπή έλεγχο ταυτότητας. Σε ευπάθειες σε επίπεδο πλατφόρμας, οι οποίες σχετίζονται με το επίπεδο πλατφόρμας του υπολογιστικού νέφους, όπως ανασφαλείς διαμορφώσεις, αδύναμους μηχανισμούς κρυπτογράφησης ή ανεπαρκής παρακολούθηση ασφάλειας. Επιπλέον, οι ευπάθειες σε επίπεδο υποδομής είτε σε επίπεδο εικονικοποίησης, οι οποίες μπορεί να περιλαμβάνουν ευπάθειες στη διαφυγή εικονικής μηχανής, κλιμάκωση των προνομίων hypervisor και ανεπαρκή απομόνωση μεταξύ εικονικών μηχανών. Τρωτά σημεία σε επίπεδο δικτύου, τρωτά σημεία σε επίπεδο αποθήκευσης, τα οποία περιλαμβάνουν παραβιάσεις δεδομένων, μη εξουσιοδοτημένη πρόσβαση σε αποθηκευμένα δεδομένα ή μεταδεδομένα και έλλειψη κρυπτογράφησης δεδομένων σε κατάσταση ηρεμίας. Οι ευπάθειες σε επίπεδο υλικού, όπως φυσικές επιθέσεις σε στοιχεία υλικού, παραβιάσεις υλικού και επιθέσεις στην αλυσίδα εφοδιασμού. Ακόμη, ευπάθειες σε εγκαταστάσεις περιβαλλόντων υπολογιστικών νεφών, οι οποίες περιλαμβάνουν παραβιάσεις φυσικής ασφάλειας, περιβαλλοντικούς κινδύνους, οι οποίοι επηρεάζουν τις λειτουργίες των κέντρων δεδομένων και

μη εξουσιοδοτημένη πρόσβαση σε κέντρα δεδομένων. Τέλος, τρωτά σημεία σε επίπεδο συμμόρφωσης σε περιβάλλοντα υπολογιστικών νεφών, όπως μη συμμόρφωση με κανονισμούς, ανεπαρκείς διαδρομές ελέγχου και έλλειψη διαφάνειας στα μέτρα συμμόρφωσης.

Μία βασική προσέγγιση για την εξέταση των ζητημάτων ασφαλείας και του απορρήτου των δεδομένων στα περιβάλλοντα υπολογιστικών νεφών κατά τους Abdulsalam και Hedabou (2022), είναι η προσέγγιση STRIDE. Η συγκεκριμένη προσέγγιση περιλαμβάνει το Spoofing, δηλαδή την πλαστογραφία, το Tampering, δηλαδή την παραβίαση, το Repudiation, δηλαδή την αποποίηση, το Information Disclosure, δηλαδή την αποκάλυψη πληροφοριών, το Denial of Service, πιο συγκεκριμένα τις επιθέσεις άρνησης υπηρεσίας και το Elevation of Privilege, δηλαδή οι απειλές, οι οποίες προέρχονται από τα αυξημένα προνόμια.

Η πλαστογραφία (Spoofing) αφορά τη συγκάλυψη μίας επικοινωνίας, η οποία προκύπτει από άγνωστη πηγή και συμπεριφέρεται ως γνωστή αξιόπιστη πηγή, η οποία μπορεί να οδηγήσει σε κλοπή ή καταστροφή δεδομένων. Η αποποίηση (Repudiation) ως απειλή ασχολείται με την παραποίηση της εμφάνισης μίας επικοινωνίας ή μίας συναλλαγής, η οποία υπάρχει η πιθανότητα να οδηγήσει σε ζητήματα λογοδοσίας. Τα αυξημένα προνόμια (Elevation of Privilege) δίνουν την ευκαιρία απόκτησης μη εξουσιοδοτημένης πρόσβασης σε προνομιούχους πόρους, η οποία μπορεί να οδηγήσει σε παραβίαση δεδομένων. Την ίδια στιγμή, υφίσταται και η επίθεση πλαστογραφία μεταδεδομένων από εισβολείς.

Η παραβίαση δεδομένων ασχολείται με τη μη εξουσιοδοτημένη τροποποίηση δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλον υπολογιστικού νέφους. Είναι μία πολύ σημαντική ανησυχία τόσο για τους παρόχους υπηρεσιών υπολογιστικού νέφους όσο και για τους χρήστες, καθώς μπορεί να οδηγήσει σε καταστροφή ή και απώλεια δεδομένων, οικονομική ζημιά, προβλήματα σχετικά με τη φήμη του κάθε οργανισμού και νομική ευθύνη. Το γεγονός αυτό μπορεί να συμβεί λόγω στοχευμένων επιθέσεων, ανθρώπινου λάθους, τρωτών σημείων σε εφαρμογές ή ανεπαρκών διαδικασιών ασφαλείας.

Οι μη ασφαλείς διεπαφές προγραμματισμού εφαρμογών (API) σε περιβάλλοντα υπολογιστικών νεφών εγκυμονούν κινδύνους, οι οποίοι μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις δεδομένων. Οι ευάλωτες διεπαφές προγραμματισμού εφαρμογών μπορούν να παρέχουν ένα εύκολο σημείο εισόδου για τους επιτιθέμενους. Για τον λόγο αυτό, οι διεπαφές προγραμματισμού εφαρμογών, οι οποίες

φιλοξενούνται σε περιβάλλοντα υπολογιστικών νεφών είναι απαραίτητο να αναπτυχθούν ώστε να αντέχουν τόσο ακούσιες όσο και σκόπιμες προσπάθειες εκμετάλλευσής τους. Αυτή η απειλή μπορεί να οδηγήσει σε επιθέσεις, όπως phishing του προγράμματος περιήγησης, και κακόβουλοι χρήστες μπορούν να ξεκινήσουν πλαστογράφηση πιστοποιητικών SSL.

Η απειλή παραβίασης λογαριασμού συμβαίνει όταν ένας εισβολέας κλέβει τα διαπιστευτήρια σύνδεσης ενός εξουσιοδωτημένου χρήστη, με στόχο να εκμεταλλευτεί αυτά τα διαπιστευτήρια για ανήθικους σκοπούς. Το γεγονός αυτό μπορεί να έχει ως αποτέλεσμα την απώλεια ευαίσθητων πληροφοριών, την οικονομική ζημιά και προβλήματα σχετικά με τη φήμη.

Ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης ή τα τρωτά σημεία στους μηχανισμούς ελέγχου ταυτότητας μπορεί να επιτρέψουν μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς χρηστών ή ευαίσθητα δεδομένα, υπάρχει πιθανότητα να οδηγήσει σε κλοπή δεδομένων, χειραγώγηση ή κακή χρήση της υπηρεσιών, οι οποίες παρέχονται από συστήματα υπολγιστικών νεφών. Η έκθεση ευαίσθητων δεδομένων λόγω αδύναμων ελέγχων ασφαλείας ενδέχεται να οδηγήσουν σε διαρροές δεδομένων ή παραβιάσεις απορρήτου.

Η διαρροή δεδομένων αναφέρεται στη μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλοντα υπολογιστικών νεφών. Είναι μία σημαντική ανησυχία για τους οργανισμούς, οι οποίοι αποθηκεύουν εμπιστευτικά δεδομένα σε συστήματα, τα οποία φιλοξενούνται σε συστήματα υπολογιστικών νεφών, καθώς μπορεί να οδηγήσει σε παραβιάσεις δεδομένων και απορρήτου.

Η απώλεια δεδομένων σε συστήματα υπολογιστικών νεφών οφείλεται σε παράγόντες όπως είανι το ανθρώπινο λάθος, οι εσφαλμένες διαμορφώσεις, οι διακοπές ρεύματος, το κακόβουλο λογισμικό, οι κυβερνοεπιθέσεις ή οι αστοχίες, τις οποίες μπορεί να εμφανίσει ένα σύστημα.

Η αποθήκευση δεδομένων σε συστήματα υπολογιστικών νεφών εμπεριέχει κινδύνους όπως απώλεια δεδομένων λόγω αστοχιών υλικού, παραβιάσεις δεδομένων λόγω πειρατείας καταστροφή δεδομένων λόγω σφαλμάτων λογισμικού, ή μη κρυπτογραφημένων ευαίσθητων δεδομένων. Ένας άλλος τύπος επίθεσης είναι το Dumpster Diving κατά το οποίο λαμβάνονται πληροφορίες από εγκαταλελειμμένα δεδομένα από ένα άτομο ή κάποιο οργανισμό και οδηγεί σε προβλήματα διαθεσιμότητας.

Η απειλή των επιθέσεων άρνησης υπηρεσίας (Denial of Service – DoS) μπορεί να διαταράξει τις υπηρεσίες υπολογιστικών νεφών, καθιστώντας με αυτό τον τρόπο τις υπηρεσίες μη διαθέσιμες σε νόμιμους και εξουσιοδοτημένους χρήστες. Τέτοιου είδους επιθέσεις μπορεί να έχουν αρνητικές επιπτώσεις στη διαθεσιμότητα ενός συστήματος. Σε μία επίθεση άρνησης υπηρεσίας, ο επιτιθέμενος στέλνει μεγάλο όγκο κίνησης σε ένα σύστημα ή δίκτυο, συνήθως και με επιθέσεις botnet, κατακλύζοντάς το και καθιστώντας το με αυτό τον τρόπο μη διαθέσιμο για τους εξουσιοδοτημένους χρήστες.

Ο κίνδυνος των κακόβουλων insiders από εσωτερικούς χρήστες με κακόβουλη πρόθεση αποτελεί σημαντική απειλή για την ασφάλεια συστημάτων υπολογιστικών νεφών. Οι κακόβουλοι εσωτερικοί ενδέχεται να κάνουν κατάχρηση των προνομίων, τα οποία τους παραχωρηθεί και να παραβιάσουν δεδομένα ή να διαταράξουν τις υπηρεσίες, οι οποίες προσφέρονται από συστήματα υπολογιστικών νεφών. Παραδείγματα τέτοιων χρηστών είναι πρώην εργαζόμενοι, διαχειριστές συστημάτων, τρίτοι εργολάβοι ή επιχειρηματικοί εταίροι.

Ακόμη, η απειλή της κακής ή ανήθικης χρήσης και κατάχρησης των υπηρεσιών υπολογιστικών νεφών. Η χρήση των υπηρεσιών υπολογιστικών νεφών για κακόβουλες δραστηριότητες, όπως η φιλοξενία κακόβουλου λογισμικού, η δημιουργία επιθέσεων ή η εμπλοκή σε παράνομες δραστηριότητες. Η υποδομή υπολογιστικών νεφών δεν έχει πλήρη έλεγχο της χρήσης των πόρων, παρέχοντας στους κακόβουλους χρήστες τη δυνατότητα να εκμεταλλευτούν αυτές τις αδυναμίες. Αυτές οι απειλές επηρεάζουν κυρίως τα επίπεδα PaaS και IaaS κυρίως λόγω του υψηλού επιπέδου αλληλεπίδρασης με το χρήστη.

Η εξωτερική ανάθεση δεδομένων αφορά τις προκλήσεις, οι οποίες σχετίζονται με την εξωτερική ανάθεση αποθήκευσης δεδομένων σε παρόχους υπηρεσιών υπολογιστικών νεφών και περιλαμβάνουν ζητήματα όπως το απόρρητο δεδομένων, η ασφάλεια των δεδομένων και η ιδιοκτησία δεδομένων. Αυτό μπορεί να οδηγήσει σε διαδοχικές αποτυχίες, οι οποίες με την σειρά τους επηρεάζουν τη διαθεσιμότητα της υπηρεσίας.

Η εξελιγμένη και επίμονη φύση των APT. Τα APT είναι ένας τύπος επίθεσεις στον κυβερνοχώρο κατά την οποία ο εισβολέας διεισδύει σε δίκτυα, με στόχο να εισχωρήσει σε περιβάλλοντα υπολογιστρικών νεφών ενός οργανισμού, προκειμένου να καταφέρουν την κλοπή ευαίσθητων δεδομένων ή τη διακοπή λειτουργίας των υπηρεσιών. Τα APT επιτίθενται στους

στόχους τους κρυφά για μεγάλες χρονικές περιόδους, συχνά αλλάζοντας τους μηχανισμούς ασφαλείας, οι οποίοι προστατεύουν τα συστήματα.

Ο κίνδυνος επιθέσεων injection, όπως η επίθεση SQL injection και άλλες τεχνικές injection κώδικα, όπως η επίθεση Cross-Site Scripting (XSS), οι οποίες έχουν την ικανότητα να χειριστούν βάσεις δεδομένων ή να εκτελέσουν μη εξουσιοδοτημένες εντολές ή και scripts. Τα τρωτά σημεία επίθεσης αυτών των επιθέσεων χρησιμοποιούνται για την αποκάλυψη λειτουργικών σημείων εφαρμογών.

Ταυτόχρονα, έντονο κίνδυνο μπορεί να προκαλέσουν επιθέσεις Man-in-the-Middle, κατά τις οποίες ο επιτιθέμενος δημιουργεί ξεχωριστές συνδέσεις με τα θύματα του και περνά επικοινωνίες μεταξύ τους, οδηγώντας σε ζητήματα διαθεσιμότητας, μη απόρριψης και ακεραιότητας.

Η απειλή της επίθεσης αναδίπλωσης υπογραφών XML είναι μία αρκετά γνωστή επίθεση στις υπογραφές XML, οι οποίες και χρησιμοποιούνται για τη διασφάλιση του ελέγχου ταυτότητας και της ακεραιότητας των μηνυμάτων SOAP.

Ο κίνδυνος ασφαλείας, ο οποίος προκαλείται από την εκχώρηση εικονικών μηχανών, οι οποίες έχουν την ικανότητα να εξαντλήσουν τους πόρους του συστήματος και κατά επέκταση να προκαλέσουν κατάρρευση της απόδοσης του συστήματος. Αλλά και η απειλή ασφαλείας της επίθεσης μέσω VM Side-Channel, κατά την οποία ένας επιτιθέμενος τοποθετεί μία κακόβουλη εικονική μηχανή μεταξύ άλλων εικονικών μηχανών στο ίδιο φυσικό μηχάνημα, αποκτώντας έτσι πρόσβαση σε κοινόχρηστο υλικό και τοποθετώντας κρυφές μνήμες για να παραβιάσει ευαίσθητες πληροφορίες από τις νόμιμες εικονικές μηχανές.

Η απειλή της πλαστογραφίας του πρωτοκόλλου ARP. Αυτό είναι ένα από τα κύρια τρωτά σημεία στη στοίβα πρωτοκόλλου IP. Με την εκμετάλλευση αυτής της ευπάθειας, οι κακόβουλοι χρήστες υπάρχει η δυνατότητα να ανακατευθύνουν την εξερχόμενη και την εισερχόμενη κυκλοφορία νόμιμων και εξουσιοδοτημένων χρηστών. Ακόμη, επιθέσεις πλαστογράφησης DNS, αποκάλυψη πακέτων, σάρωση θυρών για εκμετάλλευση τρωτών σημείων ή μη χρήση συστημάτων ανίχνευσης και πρόληψης εισβολής (IDPS) μπορεί να εκθέσουν τα δίκτυα σε κινδύνους. Την στιγμή κατά την οποία υφίστανται επιθέσεις TCP Hijacking, όπου ο υπολογιστής εισβολέα

αντικαθιστά τη διεύθυνση IP του αξιόπιστου πελάτη με τη δική του, οδηγώντας με αυτό τον τρόπο σε ζητήματα εμπιστευτικότητας και ακεραιότητας.

Ένας σημαντικός κίνδυνος είναι αυτός της ανεπαρκούς καταγραφής για την παρακολούθηση δραστηριοτήτων, τον εντοπισμό περιστατικών ασφαλείας και τη διερεύνηση παραβιάσεων.

Ακόμη, η μη ασφαλής ή ελλιπής διαγραφή δεδομένων είναι μία απειλή ασφαλείας, η οποία προκύπτει όταν τα δεδομένα δεν διαγράφονται με ασφάλεια από τον χώρο αποθήκευσης στα περιβάλλοντα υπολογιστικών νεφών, καθιστώντας τα προσβάσιμα σε δεύτερο χρόνο.

Τέλος, το ανθρώπινο σφάλμα, το οποίο μπορεί να αποτελέσει σημαντικό τρωτό σημείο σε περιβάλλοντα υπολογιστικών νεφών, μέσω κάποιας τυχαίας εσφαλμένης διαμόρφωσης, λάθους χειρισμού δεδομένων, επιθέσεων phishing ή γενικότερα επιθέσεων social engineering κατά τις οποίες χρησιμοποιούνται κοινωνικές δεξιότητες για την απόκτηση πληροφοριών, όπως διαπιστευτήρια σύνδεσης, όπου μπορεί να οδηγήσουν σε διαρροή δεδομένων ή μη εξουσιοδοτημένη πρόσβαση.

Οι παραπάνω απειλές υπογραμμίζουν το ποικίλο φάσμα των προκλήσεων ασφαλείας, τις οποίες αντιμετωπίζει η τεχνολογία υπολογιστικών νεφών σε διαφορετικά επίπεδα δικτύου και μοντέλα υπηρεσιών, σε τεχνολογίες έξυπνων πόλεων και της χρήσης υποκείμενων τεχνολογιών όπως το IoT και το Cloud of Things (CoT). Για τον μετριασμό των κινδύνων και την προστασία ευαίσθητων δεδομένων και υπηρεσιών και των συνεπειών αυτών των απειλών είναι σημαντική η χρήση ισχυρών μέτρων ασφαλείας όπως αναφέρονται στη συνέχεια.

3.3. Στρατηγικές μετριασμού της απειλής

Οι στρατηγικές μετριασμού των απειλών σε περιβάλλοντα υπολογιστικών νεφών στοχεύουν στην πρόληψη και τον εντοπισμό κακόβουλης δραστηριότητας, την προστασία από παραβιάσεις και διαρροές δεδομένων, τη διασφάλιση της διαθεσιμότητας και της ακεραιότητας των υπηρεσιών υπολογιστικών νεφών. Αυτές οι στρατηγικές μετριασμού περιλαμβάνουν μία σειρά προσεγγίσεων, όπως δυναμικούς μηχανισμούς ασφαλείας και λύσεις ασφαλείας για την εικονικοποίηση και τη διαχείριση δεδομένων, με έμφαση στη δημιουργία ενός ολοκληρωμένου

και προσαρμοστικού πλαισίου ασφαλείας για την αντιμετώπιση των εξελισσόμενων προκλήσεων σε περιβάλλοντα υπολογιστικών νεφών.

Οι στρατηγικές μετριασμού, οι οποίες αναλύονται στη συνέχεια, έχουν στόχο την ενίσχυση της ασφάλειας και την προστασίας της ιδιωτικής ζωής σε υπηρεσίες, οι οποίες βασίζονται σε περιβάλλοντα υπολογιστικών νεφών, αντιμετωπίζοντας συγκεκριμένες προκλήσεις, τρωτά σημεία και απειλές. Επικεντρώνονται στη βελτίωση του απορρήτου των δεδομένων, του ελέγχου πρόσβασης, της κρυπτογράφησης και της ευαισθητοποίησης των χρηστών με στόχο τη δημιουργία ενός πιο ασφαλούς περιβάλλοντος με έμφαση στο απόρρητο στο πλαίσιο των τεχνολογιών υπολογιστικού νέφους.

Μία πολύ γνωστή μέθοδος για την αποτροπή απειλών από επιθέσεις όπως η άρνηση υπηρεσίας (DoS) ή η κατανεμημένη άρνηση υπηρεσίας (DDoS), η επίθεση flooding και τα τρωτά σημεία στο πρωτόκολλο Διαδικτύου είναι η χρήση της τεχνολογία τειχών προστασίας ή η χρήση των εργαλείων DMaaS (DDoS Mitigation as a Service). Το Firewall-as-a-Service (FWaaS) προσφέρει την ίδια προστασία με τα κοινά παραδοσιακά τείχη προστασίας, αλλά είναι πιο αποτελεσματικό, ευέλικτο και οικονομικά αποδοτικό. Τα εικονικά τείχη προστασίας, τα οποία εγκαθίστανται από εικονικές μηχανές χειρίζονται βασικές λειτουργίες τείχους προστασίας, ενώ η φυσική υποδομή λαμβάνει υπηρεσίες ασφαλείας από τον πάροχο υπηρεσιών υπολογιστικών νεφών. Αυτή η αρχιτεκτονική έχει στόχο τη βελτιστοποίηση της διαχείρισης αποφάσεων και της απόδοσης διαθεσιμότητας. Ακόμη, τα Honeypots είναι συστήματα πρόληψης έναντι επιθέσεων κατανεμημένη άρνηση υπηρεσίας. Ο ρόλος τους είναι να εξαπατούν τους εισβολείς εμφανιζόμενοι ως νόμιμα συστήματα και με αυτό τον τρόπο συλλέγουν πληροφορίες σχετικά με τις ενέργειες των επιτιθέμενων και ταξινομούν τους τύπους και τις μεθόδους επίθεσης. Ωστόσο, παρόλο που τα honeypots βελτιώνουν την ασφάλεια του δικτύου και βοηθούν στην κατανόηση των στρατηγικών των εισβολέων, εμφανίζουν και περιορισμούς λόγω της στατικής και παθητικής φύσης τους.

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS) και τα συστήματα πρόληψης εισβολής (Intrusion Prevention Systems – IPS) είναι απαραίτητα για την ασφάλεια σε περιβάλλοντα υπολογιστικών νεφών. Το συστήματα ανίχνευσης εισβολών εντοπίζει και καταγράφει κάθε κακόβουλη πρόσβαση στο δίκτυο, ενώ το συστήματα πρόληψης εισβολής αποτρέπει οποιαδήποτε κακόβουλη πρόσβαση στο δίκτυο. Ο στόχος αυτών των συστημάτων είναι

να ανιχνεύουν και να αποτρέπουν επιθέσεις, καθώς και να καταγράφουν χρήσιμα δεδομένα για μελλοντικές αναλύσεις ασφάλειας.

Ένα σημαντικό μέτρο ασφαλείας είναι η εφαρμογή ισχυρών διαδικασιών ελέγχου ταυτότητας και περιορισμών πρόσβασης είναι δυνατόν να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και υπηρεσίες, τα οποία φιλοξενούνται ή παρέχονται από την τεχνολογία υπολογιστικού νέφους. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων και οι πολιτικές ισχυρών κωδικών πρόσβασης μπορούν επίσης να αποτρέψουν την παραβίαση λογαριασμών χρηστών και την πρόσβαση σε υπηρεσίες.

Σχετικά με την προσέγγιση STRIDE, η οποία όπως αναλύθηκε και προηγουμένως, περιλαμβάνει απειλές όπως είναι η πλαστογράφηση, η παραποίηση, η απόρριψη, η αποκάλυψη πληροφοριών, η επίθεση άρνησης υπηρεσίας και η αύξηση των προνομίων.

Για να αποφευχθεί η πλαστογράφηση (spoofing), είναι εφικτό να ληφθούν μέτρα όπως η εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας, όπως είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων, για να αποτραπεί η διείσδυση πλαστών πακέτων σε ένα δίκτυο και η διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στις υπηρεσίες υπολογιστικού νέφους. Η μέθοδος αυτή εξετάζει τα εισερχόμενα πακέτα IP και εξετάζει τις κεφαλίδες προέλευσης τους, απορρίπτοντας πακέτα με κεφαλίδες πηγής, οι οποίες δεν ταιριάζουν με την προέλευσή του.

Για την αποφυγή της απειλής παραβίασης, οι εισβολείς κρίνεται αναγκαίο να εμποδίζονται να τροποποιούν δεδομένα, με τα οποία στόχο έχουν να παρεμβαίνουν σε λειτουργίες. Η προστασία του λογισμικού από επιθέσεις κατανεμημένης άρνησης υπηρεσίας διαδραματίζει πολύ σημαντικό ρόλο στην πρόληψη τέτοιου τύπου επίθεσης. Ακόμη, η εφαρμογή ελέγχων πρόσβασης, όπως ο έλεγχος πρόσβασης βάσει ρόλου (RBAC), είναι σημαντική για τη διασφάλιση της χρήσης υπηρεσιών και της τροποποίησης των δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλοντα υπολογιστικών νεφών μόνο από εξουσιοδοτημένους χρήστες.

Για τον μετριασμό της αποποίησης κρίνεται η χρήση ψηφιακών υπογραφών και ελέγχων προκειμένου να διασφαλιστεί ότι οι χρήστες των υπηρεσιών υπολογιστικού νέφους δε δύναται να αρνηθούν τις ενέργειες τους.

Επιπλέον, για την μείωση της αποκάλυψης δεδομένων είναι απαραίτητη η εφαρμογή ελέγχων πρόσβασης, όπως ο υποχρεωτικός έλεγχος πρόσβασης (MAC), έτσι ώστε να

εξασφαλιστεί ότι μονάχα οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα, τα οποία είναι αποθηκευμένα σε συστήματα υπολογιστικών νεφών.

Για να αποφευχθεί η αύξηση των προνομίων, οι οργανισμοί είναι εφικτό να κάνουν πολλά βήματα, όπως είναι η παρακολούθηση ανακοινώσεων ευπάθειας από παρόχους, η διεξαγωγή τακτικών ελέγχων πολιτικών και ρόλων, οι οποίοι ορίζονται στα περιβάλλοντα υπηρεσιών υπολογιστικών νεφών και η χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων ή ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) και άλλων μέτρων ασφαλείας. Αυτά θα έχουν ως αποτέλεσμα ότι οι χρήστες δεν μπορούν να αυξήσουν τα προνόμιά τους.

Ένα κρίσιμο μέτρο ασφάλειας για την αποθήκευση και προστασία ευαίσθητων δεδομένων σε περιβάλλοντα υπολογιστικού νέφους αποτελεί η κρυπτογράφηση. Η κρυπτογράφηση δεδομένων πριν την αποθήκευσή τους σε περιβάλλοντα υπολογιστικών νεφών μπορεί να αποτρέψει παραβιάσεις δεδομένων. Η διαδικασία της κρυπτογράφησης περιλαμβάνει τη μετατροπή δεδομένων σε κωδικοποιημένη μορφή στην οποία μπορούν να έχουν πρόσβαση μόνο εξουσιοδοτημένοι χρήστες, ενώ η διαδικασία της αποκρυπτογράφησης ασχολείται με τη μετατροπή των κωδικοποιημένων δεδομένων στην αρχική τους μορφή. Επιπλέον, οι τεχνικές διαχείρισης κλειδιών και οι αποτελεσματικοί έλεγχοι πρόσβασης μπορούν να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.

Ακόμη, η διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων σε περιβάλλοντα υπολογιστικού νέφους και η εφαρμογή στρατηγικών πρόληψης απώλειας δεδομένων είναι δυνατόν να αποτρέψει την απώλεια δεδομένων λόγω ανθρώπινου λάθους, «μόλυνσης» από κακόβουλο λογισμικό, αποτυχίας υλικού, διακοπών ρεύματος ή φυσικών καταστροφών.

Την ίδια στιγμή, οι μηχανικοί λογισμικού κρίνεται αναγκαίο να δημιουργούν διεπαφές προγραμματισμού εφαρμογών (API) σύμφωνα με τις αρχές της ασφάλειας στον τομέα της πληροφορικής. Οι πάροχοι υπηρεσιών υπολογιστικών νεφών είναι απαραίτητο να διασφαλίζουν ότι όλες οι διεπαφές προγραμματισμού εφαρμογών, οι οποίες χρησιμοποιούνται σε περιβάλλοντα υπολογιστικών νεφών έχουν κατασκευαστεί με γνώμονα την ασφάλεια. Η εφαρμογή ισχυρών διαδικασιών ελέγχου ταυτότητας, περιορισμών πρόσβασης, ασφαλών πρακτικών κωδικοποίησης, εκτιμήσεων ευπάθειας και ασφαλή κύκλου ζωής ανάπτυξης μπορεί να μετριάσει τους κινδύνους και να προστατεύσει τα δεδομένα και τις υπηρεσίες από την έκθεση μέσω μη ασφαλών διεπαφών χρήστη και διεπαφών προγραμματισμού εφαρμογών.

Αξιοσημείωτη είναι η ασφαλής επικοινωνία, η οποία περιλαμβάνει τη χρήση ασφαλών καναλιών και πρωτοκόλλων επικοινωνίας για τη διασφάλιση της ασφαλούς μετάδοσης των δεδομένων μεταξύ των παρόχων υπηρεσιών υπολογιστικών νεφών και των χρηστών. Για την επίτευξη αυτού είναι απαραίτητη η χρήση πρωτοκόλλων επιπέδου ασφαλών υποδοχών (SSL) και ασφάλειας επιπέδου μεταφοράς (TLS) για την κρυπτογράφηση δεδομένων κατά τη μεταφορά και τη διασφάλιση ότι τα δεδομένα δε θα υποκλαπούν και δε θα παραβιαστούν από μη εξουσιοδοτημένους χρήστες. Σχετικά με τη μεταφορά δεδομένων καλό είναι να γίνεται χρήση της τεχνικής εξισορρόπησης φορτίου, η οποία είναι απαραίτητη για να αντιμετωπιστεί η πρόκληση της κυκλοφορίας πληροφοριών σε πραγματικό χρόνο για εφαρμογές n-tier.

Σημαντικός παράγοντας για τον μετριασμό των απειλών είναι η τακτική παρακολούθηση της υποδομής υπολογιστικού νέφους και η διεξαγωγή αξιολογήσεων – ελέγχων ασφαλείας, προκειμένου να βοηθήσει στον εντοπισμό και την πρόληψη πιθανών απειλών και τρωτών σημείων. Ο έλεγχος μπορεί να βοηθήσει στη διαδικασία της ανίχνευσης απειλών και τρωτών σημείων ασφαλείας στο σύστημα. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους είναι αναγκαίο να θεσπίσουν προδιαγραφές για την εφαρμογή βιομηχανικών προτύπων εφαρμογών και υπηρεσιών υπολογιστικού νέφους. Ακόμη, αναγκαία είναι η εκτέλεση αξιολογήσεων ευπάθειας και δοκιμών διείσδυσης βάσει προτύπων ασφαλείας όπως το OWASP.

Συμπληρωματικά, η εφαρμογή μίας στρατηγικής αποκατάστασης από καταστροφές και των διαδικασιών δημιουργίας αντιγράφων ασφαλείας μπορεί να διασφαλίσει τη συνέχεια του οργανισμού σε περίπτωση διακοπής των υπηρεσιών, οι οποίες παρέχονται από τα περιβάλλοντα υπολογιστικών νεφών. Η δοκιμή ανά τακτά χρονικά διαστήματα του σχεδίου αποκατάστασης από καταστροφή διασφαλίζει ότι είναι αποτελεσματικό και ενημερωμένο.

Η τεχνολογία Blockchain είναι ένα αποκεντρωμένο και κατανεμημένο σύστημα καθολικού, το οποίο είναι εφικτό να χρησιμοποιηθεί για την ασφάλεια των συναλλαγών σε περιβάλλοντα υπολογιστικού νέφους και την πρόσβαση σε κώδικες εφαρμογών και δεδομένων. Ακόμη, μπορεί να βοηθήσει στη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων σε περιβάλλοντα υπολογιστικού νέφους.

Η σωστή διαμόρφωση των πολιτικών ασφαλείας στην υποδομή υπολογιστικών νεφών είναι εξαιρετικά σημαντική. Οι εσφαλμένες διαμορφώσεις είναι απραίτητο να αντιμετωπιστούν

με τη χρήση μηχανισμών ασφαλούς διαγραφής και διαδικασιών περιοδικού ελέγχου για συσκευές αποθήκευσης.

Τέλος, οι πάροχοι υπηρεσιών υπολογιστικών νεφών είναι αναγκαίο να συμμορφώνονται με τους κανονισμούς προστασίας δεδομένων, τα βιομηχανικά πρότυπα και τους νόμους περί απορρήτου των δεδομένων ανάλογα με τη χώρα, στην οποία τα δεδομένα θα αποθηκεύονται και θα υποβάλλονται σε επεξεργασία. Όπως επίσης και να παρέχουν αποδεικτικά στοιχεία για τα κατάλληλα μέτρα κρυπτογράφησης και διαχωρισμού των δεδομένων για τη διασφάλιση του απορρήτου των δεδομένων. Τα παραπάνω θα μπορούσαν να επιτευχθούν με μεγαλύτερη ευκολία, αν οι οργανισμοί κάνουν χρήση πολιτικών και οδηγιών ασφαλείας, οι οποίες είναι απαραίτητες προκειμένου να διασφαλιστεί ότι οι πάροχοι και οι χρήστες υπηρεσιών υπολογιστικών νεφών ακολουθούν τις βέλτιστες πρακτικές για την ασφάλεια των συστημάτων και των δεδομένων, τα οποία φιλοξενούν.

Αυτές οι στρατηγικές μετριασμού μπορούν να βοηθήσουν στην αντιμετώπιση των απειλών ασφαλείας και των τρωτών σημείων σε ένα ασφαλές περιβάλλον υπολογιστικού νέφους και να διασφαλίσουν ότι τα δεδομένα είναι ασφαλή και προστατευμένα. Ωστόσο, αξιοσημείωτο είναι ότι καμία μεμονωμένη στρατηγική δεν έχει τη δυνατότητα να παρέχει πλήρη προστασία και είναι αναγκαία η χρήση μίας ολοκληρωμένης προσέγγισης, η οποία συνδυάζει πολλαπλές στρατηγικές ασφαλείας για τη διασφάλιση της ασφάλειας ενός συστήματος υπολογιστικού νέφους. Η εφαρμογή και ο σχεδιασμός στρατηγικών μετριασμού για την πρόληψη πιθανών απειλών και τρωτών σημείων, τα οποία σχετίζονται με την τεχνολογία υπολογιστικού νέφους. Εφαρμόζοντας τέτοιου είδους στρατηγικών, οι οργανισμοί θα είναι ικανοί να διασφαλίσουν την ασφάλεια και το απόρρητο των δεδομένων και των υπηρεσιών τους σε περιβάλλοντα υπολογιστικού νέφους. Το πλαίσιο ασφαλείας, το οποίο θα σχεδιαστεί και εφαρμοστεί είναι αναγκαίο να βασίζεται σε πρότυπα, όπως το ISO 27001 και το NIST SP 800-53, με απαραίτητη προϋπόθεση να επανεξετάζεται και να ενημερώνεται ανά τακτά χρονικά διαστήματα για την αντιμετώπιση νέων απειλών και τρωτών σημείων.

3.4. Προγράμματα Ελέγχου Ασφαλείας (Security Audit Programs)

Στο σημερινό ταχέως εξελισσόμενο ψηφιακό κόσμο, η τεχνολογία έχει γίνει πανταχού παρόν, για τον λόγο αυτό η διασφάλιση της ορθότητας και της ασφάλειας των δεδομένων κατά τη

μεταφορά από και προς τα περιβάλλοντα υπολογιστικών νεφών είναι ζωτικής σημασίας. Η αυξανόμενη χρήση του υπολογιστικού νέφους για την αποθήκευση και τον υπολογισμό δεδομένων απαιτεί ισχυρούς μηχανισμούς για την προστασία των ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και τροποποίηση. Η δημιουργία ενός ολοκληρωμένου προγράμματος ελέγχου ασφάλειας για τις υπηρεσίες υπολογιστικού νέφους απαιτεί την εξέταση διαφόρων παραγόντων τόσο από την οπτική γωνία των παρόχων υπηρεσιών υπολογιστικού νέφους όσο και από την πλευρά των πελατών της τεχνολογίας του υπολογιστικού νέφους. Η έλλειψη σαφών κατευθυντήριων γραμμών έκανε τη δημιουργία τέτοιων προγραμμάτων δύσκολη. Ωστόσο, με την πάροδο του χρόνου, έχει γίνει μία αυξανόμενη κατανόηση της πολυπλοκότητας του υπολογιστικού νέφους, η οποία οδήγησε στην εμφάνιση εργαλείων και πλαισίων, τα οποία χρησιμοποιούνται για την υποστήριξη των επαγγελματιών ασφάλειας σε αυτήν την προσπάθεια.

Τα πιο γνωστά και βασικά πλαίσια είναι το Cloud Control Matrix (CCM) V4 της Cloud Security Alliance (CSA), το οποίο απευθύνεται σε 17 τομείς ασφαλείας με 197 στοιχεία ελέγχου. Με αυτό τον τρόπο καλύπτει τομείς όπως είναι η ασφάλεια διεπαφών προγραμματισμού εφαρμογών (API), η διαχείριση συμβάντων και η διακυβέρνηση. Ακόμη, το Πρόγραμμα Ασφάλεια, Εμπιστοσύνη, Διασφάλιση και Κίνδυνος (STAR), το οποίο βασίζεται στο προαναφερόμενο πλαίσιο CCM, προσφέρει δύο επίπεδα διασφάλισης για την αξιολόγηση της ασφάλειας, αυτό της αυτοαξιολόγησης και αυτό της αξιολόγηση τρίτων, υποστηρίζοντας πιστοποιήσεις όπως το SOC2 και το ISO27001.

Την ίδια στιγμή, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) παρέχει το εργαλείο Εκτίμησης Κινδύνων Υπολογιστικού Νέφους, το οποίο παρουσιάζει κρίσιμους κινδύνους σε περιβάλλοντα υπολογιστικού νέφους. Σε αυτούς τους κινδύνους συμπεριλαμβάνονται οι κίνδυνοι πολιτικής, τεχνικών, νομικών και γενικών κινδύνων. Το ISO/IEC 27017:2015 προσφέρει κατευθυντήριες γραμμές για την ασφάλεια των υπηρεσιών υπολογιστικών νεφών, συμπληρώνοντας το ISO27001 και ενσωματώνοντας σε αυτό στοιχεία ελέγχου απορρήτου.

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους κρίνεται αναγκαίο να ενσωματώνουν ελέγχους ασφαλείας σε όλο τον κύκλο ζωής του προϊόντος, λαμβάνοντας υπόψη τομείς όπως η ασφάλεια εφαρμογών και διεπαφής χρήστη, η κρυπτογράφηση και η διαδικασία διαχείρισης και ελέγχου αλλαγών. Μπορούν να συνδυάσουν διαφορετικά πρότυπα και πλαίσια προκειμένου να προσαρμόσουν ένα πρόγραμμα ελέγχου στους συγκεκριμένους κινδύνους υπηρεσιών τους.

Οι πελάτες υπηρεσιών υπολογιστικού νέφους διαδραματίζουν, αντίστοιχα, κρίσιμο ρόλο στους ελέγχους ασφαλείας, ιδιαίτερα στην αξιολόγηση πτυχών όπως είναι η κρυπτογράφηση, η διαχείριση ταυτότητας και πρόσβασης, η ασφάλεια σε επίπεδο συσκευής, η καταγραφή ασφαλείας και οι συμβατικές συμφωνίες. Ανάλογα με το μοντέλο υπηρεσίας (IaaS, PaaS, SaaS), το οποίο έχουν μισθώσει, η έκταση των ελέγχων ποικίλλει, δηλαδή για παράδειγμα το μοντέλο Υποδομή ως Υπηρεσία (IaaS) επιτρέπει πιο εκτεταμένους ελέγχους σε σύγκριση με το μοντέλο Λογισμικό ως Υπηρεσία (SaaS).

Ωστόσο, οι προκλήσεις, οι οποίες παρουσιάζονται στο υπολογιστικό νέφος συνεχίζουν να δημιουργούν ενστάσεις. Για τον λόγο αυτό, κατά τον Carrera (2021) προτείνεται μία καινοτόμος προσέγγιση, η οποία ασχολείται με την ακεραιότητα και την εμπιστευτικότητα των δεδομένων σε περιβάλλοντα υπολογιστικών νεφών, συνδυάζοντας τη χρήση κρυπτογραφικών τεχνικών, μηχανισμών ελέγχου πρόσβασης και ελέγχου τρίτων. Ένα από τα βασικά στοιχεία της προτεινόμενης μεθόδου είναι η συμμετοχή ενός τρίτου ελεγκτή (Third Party Auditor – TPA), ο οποίος θα επαληθεύει ανεξάρτητα την ακεραιότητα και την ασφάλεια των δεδομένων, τα οποοία είναι αποθηκευμένα στο υπολογιστικό νέφος. Ακόμη, ο τρίτος ελεγκτής θα είναι υπεύθυνος για την κρυπτογράφηση αρχείων μεταδεδομένων με έναν τροποποιημένο αλγόριθμο AES και με την εισαγωγή ενός μηχανισμού batch processing, θα επιτρέπεται στον τρίτο ελεγκτή η ταυτόχρονη επαλήθευση δεδομένων για αρκετούς χρήστες.

Η επιλογή ενός βασικού πλαισίου όπως είναι το ISO27001 ή η δημιουργία εσωτερικών πλαισίων με βάση τα πρότυπα του οργανισμού εξαρτάται από τις ανάγκες του εκάστοτε οργανισμού. Η συνεχής εκπαίδευση και η ενημέρωση για τις βέλτιστες πρακτικές του κλάδου είναι απαραίτητες, υποστηριζόμενες αρκετές φορές από πιστοποιήσεις όπως το Certificate of Cloud Auditing Knowledge (CCAK) από την Information Systems Audit and Control Association (ISACA) και την Cloud Security Alliance (CSA).

Συμπερασματικά, η οικοδόμηση ενός ισχυρού προγράμματος ελέγχου ασφάλειας για υπηρεσίες υπολογιστικών νεφών περιλαμβάνει μία ολιστική προσέγγιση, η οποία λαμβάνει υπόψη τόσο τις προοπτικές του κάθε παρόχου όσο και των πελατών. Με την παρουσία πληθώρας πλαισίων, εργαλείων και πιστοποιήσεων, οι επαγγελματίες ασφάλειας έχουν τη δυνατότητα να δημιουργήσουν προσαρμοσμένα προγράμματα ελέγχου για την αντιμετώπιση των μοναδικών προκλήσεων και κινδύνων, οι οποίες σχετίζονται με την τεχνολογία υπολογιστικού νέφους,

διασφαλίζοντας την ασφάλεια και το απόρρητο δεδομένων και υπηρεσιών στο περιβάλλον υπολογιστικού νέφους.

3.5. Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση διαδραματίζει πολύ σημαντικό ρόλο στη διασφάλιση της ασφάλειας και του απορρήτου των δεδομένων όταν ανατίθενται σε εξωτερικούς συνεργάτες στο περιβάλλον υπολογιστικού νέφους, μετατρέποντας το απλό κείμενο σε μη αναγνώσιμο κρυπτογραφημένο κείμενο χρησιμοποιώντας αλγόριθμους. Η συμμετρική κρυπτογράφηση και η ασύμμετρη κρυπτογράφηση είναι οι δύο κύριες μέθοδοι κρυπτογράφησης. Από τη μεριά της, η ασύμμετρη κρυπτογράφηση, γνωστή και ως κρυπτογράφηση δημόσιου κλειδιού, προσφέρει μεγαλύτερη ευκολία καθώς περιλαμβάνει ένα ζεύγος κλειδιών, ένα δημόσιο κλειδί για τη διαδικασία της κρυπτογράφησης και ένα ιδιωτικό κλειδί για τη διαδικασία της αποκρυπτογράφησης.

Η κρυπτογράφηση με βάση την ταυτότητα (Identity-Based Encryption – IBE) είναι ένα κρυπτογραφικό σύστημα, στο οποίο η ταυτότητα του χρήστη είναι ενσωματωμένη στο δημόσιο κλειδί και το ιδιωτικό κλειδί, καθιστώντας αυτό τον τύπο κρυπτογράφησης κατάλληλο για την προστασία των ιδιωτικών δεδομένων ενός μόνο ή ενός μικρού αριθμού των χρηστών. Χρησιμοποιείται σε εφαρμογές όπως η κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου και η εκ νέου κρυπτογράφηση διακομιστή μεσολάβησης.

Η ιεραρχική κρυπτογράφηση βάσει ταυτότητας (Hierarchical Identity-Based Encryption – HIBE) αποτελεί ένα σύστημα κρυπτογράφησης, το οποίο ενισχύει την επεκτασιμότητα της κρυπτογράφησης βάσει ταυτότητας (IBE) αναθέτοντας το φόρτο εργασίας της γεννήτριας ιδιωτικού κλειδιού ρίζας μεταξύ παραγωγών ιδιωτικών κλειδιών χαμηλότερου επιπέδου. Η ιεραρχική κρυπτογράφηση βάσει ταυτότητας υπάρχει η δυνατότητα να αναπτυχθεί σε συστήματα υπολογιστικού νέφους, σε ασύρματα δίκτυα αισθητήρων αλλά και σε διάχυτα υπολογιστικά συστήματα.

Η κρυπτογράφηση με βάση χαρακτηριστικά (ABE) αποτελεί έναν τύπο συστήματος κρυπτογράφησης, ο οποίος διασφαλίζει ότι η αποκρυπτογράφηση του κρυπτογραφημένου κειμένου είναι δυνατή μόνο εάν τα βασικά χαρακτηριστικά του χρήστη ταιριάζουν με τα χαρακτηριστικά του κρυπτογραφημένου κειμένου. Ταυτόχρονα, είναι μία ασαφής

κρυπτογράφηση ταυτότητας με υψηλότερη επεκτασιμότητα, η οποία επιτρέπει στον κάτοχο δεδομένων να προσδιορίσει ποιος μπορεί να έχει πρόσβαση στα κρυπτογραφημένα δεδομένα. Υπάρχουν δύο κύριοι τύποι σχημάτων κρυπτογράφησης με βάση χαρακτηριστικά, οι οποίοι είναι η κρυπτογράφηση βασισμένη σε χαρακτηριστικά κλειδιού πολιτικής (KP-ABE) και η κρυπτογράφηση βάσει χαρακτηριστικών πολιτικής κρυπτογραφημένου κειμένου (CP-ABE). Η κρυπτογράφηση βασισμένη σε χαρακτηριστικά κλειδιού πολιτικής συσχετίζει κάθε κρυπτογραφημένο κείμενο με ένα σύνολο χαρακτηριστικών και το ιδιωτικό κλειδί του χρήστη σχετίζεται με μία πολιτική πρόσβασης για τα χαρακτηριστικά. Ενώ, κρυπτογράφηση βάσει χαρακτηριστικών πολιτικής κρυπτογραφημένου κειμένου ενσωματώνει την πολιτική στο κρυπτογραφημένο κείμενο και ο κάτοχος των δεδομένων μπορεί να ορίσει την πολιτική πρόσβασης προκειμένου να προσδιορίσει σε ποια χαρακτηριστικά το κάθε άτομο μπορεί να έχει πρόσβαση στο κρυπτογραφημένο κείμενο.

Η κρυπτογράφηση με δυνατότητα αναζήτησης (Searchable Encryption – SE) είναι πάρα πολύ σημαντική για την προστασία του απορρήτου των δεδομένων και τη διασφάλιση της διαθεσιμότητας των δεδομένων σε περιβάλλοντα υπολογιστικού νέφους. Δίνει τη δυνατότητα στους εξουσιοδοτημένους χρήστες να αναζητούν και να ανακτούν κρυπτογραφημένα δεδομένα χωρίς να είναι απαραίτητο να αποκαλύπτουν ευαίσθητες πληροφορίες. Τα σχήματα κρυπτογράφησης με δυνατότητα αναζήτησης συνήθως περιλαμβάνουν κρυπτογράφηση, δημιουργία διακριτικών, αναζήτηση λέξεων – κλειδιών και διαδικασίες αποκρυπτογράφησης. Ακόμη, μπορεί να χωριστεί σε συμμετρική κρυπτογράφηση με δυνατότητα αναζήτησης (Searchable Symmetric Encryption – SSE) και κρυπτογράφηση δημόσιου κλειδιού με αναζήτηση λέξεων-κλειδιών (Public Key Encryption with keyword Search – PEKS). Η συμμετρική κρυπτογράφηση με δυνατότητα αναζήτησης βασίζεται στη συμμετρική κρυπτογραφία, ενώ η κρυπτογράφηση δημόσιου κλειδιού με αναζήτηση λέξεων-κλειδιών βασίζεται στην κρυπτογραφία δημόσιου κλειδιού.

Η ασύμμετρη κρυπτογράφηση με δυνατότητα αναζήτησης (SAE) περιλαμβάνει κρυπτογράφηση δημόσιου κλειδιού με αναζήτηση λέξεων-κλειδιών (PEKS), κρυπτογράφηση βάσει χαρακτηριστικών με αναζήτηση λέξεων-κλειδιών (Attribute-Based Encryption with Dynamic Keyword Search – ABKS) και εκ νέου κρυπτογράφηση διακομιστή μεσολάβησης με αναζήτηση λέξεων-κλειδιών (PRKS). Αυτές οι μέθοδοι κρυπτογράφησης έχουν παρατηρηθεί ότι

βελτιώνουν την απόδοση όσον αφορά την ασφάλεια και το απόρρητο με τις εξελίξεις στην τεχνολογία υλικού.

Τέλος, η κρυπτογραφία ανθεκτική σε διαρροές έχει σχεδιαστεί με στόχο να χειρίζεται καταστάσεις όπου ένας εισβολέας μπορεί να λάβει μέρος πληροφοριών σχετικά με το μυστικό κλειδί, όπως μέσω επιθέσεων πλευρικού καναλιού. Επιπλέον, χρησιμοποιείται για τη διασφάλιση της εμπιστευτικότητας των δεδομένων σε περιβάλλοντα υπολογιστικών νεφών.

Οι προκλήσεις, οι οποίες έχουν παρατηρηθεί, περιλαμβάνουν την αποτελεσματική διαχείριση των χαρακτηριστικών των χρηστών, η οποία αντιμετωπίζεται μέσω δυναμικής παραγωγής κλειδιού και κρυπτογραφίας δημόσιου κλειδιού. Οι δομές πρόσβασης στη κρυπτογράφηση βάσει χαρακτηριστικών, μπορούν να χωριστούν σε τρείς κατηγορίες, κατηγοριοποιημένες σε κατώφλι, δέντρο ελέγχου πρόσβασης και κοινή χρήση μυστικών και επηρεάζουν την αποτελεσματικότητα και την ευαισθησία προστασίας ολόκληρου του συστήματος ελέγχου πρόσβασης. Τα Bilinear Pairings και η απόφαση Bilinear Diffie-Hellman (DBDH) διαδραματίζουν κρίσιμο ρόλο στην κρυπτογράφηση και πιο συγκεκριμένα τα Bilinear Pairings χρησιμοποιούνται στη κρυπτογράφηση βάσει χαρακτηριστικών για την κρυπτογράφηση μηνυμάτων και τα στοιχεία κρυπτογραφημένου κειμένου σχετίζονται με χαρακτηριστικά, καθορίζοντας με αυτό τον τρόπο τα απαραίτητα χαρακτηριστικά για την αποκρυπτογράφηση. Την στιγμή που το Decision Bilinear Diffie-Hellman (DBDH) είναι ένα μαθηματικό πρόβλημα, το οποίο χρησιμοποιείται στην απόδειξη ασφαλείας της κρυπτογράφησης βάσει χαρακτηριστικών.

Ταυτόχρονα, η τεχνολογία εξωτερικής ανάθεσης ασφαλείας εισάγεται στην κρυπτογράφηση βάσει χαρακτηριστικών προκειμένου να επιλύσει την επαληθευσιμότητα των αποτελεσμάτων από τρίτα μέρη. Οι μηχανισμοί ιχνηλασιμότητας ενισχύουν την ασφάλεια του ελέγχου πρόσβασης και κατηγοριοποιούνται σε προσεγγίσεις λευκού κουτιού και μαύρου κουτιού με βάση τις διαφορετικές απαιτήσεις του αλγόριθμου. Το λευκό κουτί χρησιμοποιεί το κλειδί ως το περιεχόμενο εισόδου του αλγόριθμου ανίχνευσης για να παρακολουθεί το κλειδί του χρήστη, ενώ το μαύρο κουτί δεν γνωρίζει τον αλγόριθμο αποκρυπτογράφησης και τις πληροφορίες του κλειδιού αποκρυπτογράφησης. Διερευνώνται τεχνικές κρυπτογράφησης με δυνατότητα αναζήτησης (SET), με ορισμένες μη πρακτικές λόγω ζητημάτων απόδοσης και διαχείρισης κλειδιών.

Αυτές οι τεχνολογίες κρυπτογράφησης χρησιμοποιούνται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και του απορρήτου των δεδομένων στο χώρο αποθήκευσης, ο οποίος φιλοξενείται σε περιβάλλοντα υπολογιστικών νεφών. Οι τεχνικές έχουν σχεδιαστεί έτσι ώστε να προστατεύουν τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, να διασφαλίζουν την ακεραιότητα των δεδομένων και να αποτρέπουν τη διαρροή ευαίσθητων πληροφοριών.

4. Μελέτες περίπτωσης Ασφάλειας και Απορρήτου Υπολογιστικών Νεφών

4.1. Ασφάλεια υπολογιστικών νεφών για το Industry 4.0

Η Τέταρτη Βιομηχανική Επανάσταση (Industry 4.0) προαναγγέλλει μία νέα εποχή τεχνολογικής προόδου, κατά την οποία η τεχνολογία υπολογιστικών νεφών παίζει καθοριστικό ρόλο στη διευκόλυνση των επιχειρηματικών λειτουργιών. Το περιβάλλον υπολογιστικών νεφών, το οποίο χαρακτηρίζεται από εργαλεία υλικού και λογισμικού που βασίζονται στο Διαδίκτυο, προσφέρει απομακρυσμένη πρόσβαση σε πόρους, όπως το παράδειγμα δημοφιλών εφαρμογών όπως το Microsoft SharePoint και το Google Apps. Ωστόσο, η ταχεία επέκταση των υπηρεσιών υπολογιστικών νεφών εγείρει σημαντικές ανησυχίες για την ασφάλεια, κυριώς όσον αφορά την προστασία των δεδομένων των χρηστών και την αξιοπιστία των παρόχων υπηρεσιών.

Η ευρεία υιοθέτηση του υπολογιστικού νέφους επιδεινώνει τις προκλήσεις ασφαλείας, οι οποίες είναι εγγενείς στα ανοιχτά συστήματα και στο διαδίκτυο. Οι ανησυχίες περιστρέφονται γύρω από την προστασία δεδομένων κατά τη μετάδοση και αποθήκευση, τον έλεγχο ταυτότητας των χρηστών και την προστασία από μη εξουσιοδοτημένη πρόσβαση. Η κρυπτογράφηση αναδύεται ως θεμελιώδες εργαλείο για την αντιμετώπιση για αρκετές από αυτές τις προκλήσεις, επιτρέποντας την ασφαλή επικοινωνία μέσω μη ασφαλών καναλιών.

Έχουν αναπτυχθεί διάφορα πρωτόκολλα κρυπτογράφησης και κρυπτογραφικά συστήματα για την ενίσχυση της ασφάλειας στα περιβάλλοντα υπολογιστικών νεφών. Η κρυπτογράφηση διασφαλίζει σε μεγάλο βαθμό την εμπιστευτικότητα, την ακεραιότητα και τον έλεγχο ταυτότητας των δεδομένων. Τεχνικές όπως η Ελλειπτικής Καμπύλης Κρυπτογραφίας (Elliptic Curve Cryptography – ECC) και το Προηγμένου Προτύπου Κρυπτογράφησης (Advanced Encryption Standard – AES) έχουν κερδίσει ξεχωριστή θέση για την αποτελεσματικότητά τους στην εξασφάλιση της ιδιωτικότητας ευαίσθητων πληροφοριών. Αυτές οι κρυπτογραφικές μέθοδοι χρησιμοποιούν πολύπλοκους αλγόριθμους για την κωδικοποίηση δεδομένων, καθιστώντας τα ανεκρυπτογραφήσιμα σε μη εξουσιοδοτημένες οντότητες.

Ένας από τους εγγενείς κινδύνους που υφίσταται στο υπολογιστικό νέφος είναι η ταυτόχρονη πρόσβαση σε δεδομένα από πολλούς χρήστες μέσω προσωπικών συνδέσεων στο διαδίκτυο. Αυτό πολλαπλασιάζει τα πιθανά σημεία ευπάθειας, αυξάνοντας ταυτόχρονα την

πιθανότητα παραβίασης δεδομένων. Η αντιμετώπιση αυτού του κινδύνου απαιτεί ισχυρά μέτρα ασφαλείας για την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Για την αντιμετώπιση των προκλήσεων ασφαλείας του υπολογιστικού νέφους, έχει προταθεί μία υβριδική προσέγγιση, η οποία συνδυάζει την Ελλειπτικής Καμπύλης Κρυπτογραφίας (ECC) και Προηγμένου Προτύπου Κρυπτογράφησης (AES). Αυτή η προσέγγιση αξιοποιεί τα δυνατά σημεία και των δύο κρυπτογραφικών τεχνικών για την ενίσχυση της ασφάλειας δεδομένων σε περιβάλλοντα υπολογιστικών νεφών. Η Ελλειπτικής Καμπύλης Κρυπτογραφίας (ECC) προσφέρει αποτελεσματική παραγωγή κλειδιών και μικρότερα μεγέθη κλειδιών, καθιστώντας με αυτό τον τρόπο το κατάλληλο για περιβάλλοντα με περιορισμένους πόρους, όπως η τεχνολογία υπολογιστικών νεφών. Το Προηγμένο Πρότυπο Κρυπτογράφησης (AES), από την άλλη πλευρά, παρέχει ισχυρή κρυπτογράφηση και υιοθετείται ευρέως ως πρότυπο για την ασφάλεια των δεδομένων.

Τα πειραματικά αποτελέσματα επιβεβαιώνουν την αποτελεσματικότητα της προτεινόμενης υβριδικής προσέγγισης στην ενίσχυση της ασφάλειας του περιβάλλοντος υπολογιστικών νεφών. Η συγκριτική ανάλυση έναντι των υφιστάμενων προτύπων καταδεικνύει ανώτερη απόδοση όσον αφορά την εμπιστευτικότητα, τον έλεγχο ταυτότητας και την ακεραιότητα των δεδομένων. Την ίδια στιγμή που η υβριδική τεχνική ECC – AES έχει την ικανότητα να προσφέρει μία βιώσιμη λύση για τη διασφάλιση της ασφάλειας και της ακεραιότητας των πληροφοριών σε περιβάλλοντα υπολογιστικών νεφών.

Συμπερασματικά, η εξέλιξη της Τέταρτης Βιομηχανικής Επανάστασης (Industry 4.0) απαιτεί ισχυρά μέτρα ασφαλείας για τον μετριασμό των κινδύνων, οι οποίοι εγκυμονούν στο υπολογιστικό νέφος. Η προτεινόμενη υβριδική προσέγγιση της Ελλειπτικής Καμπύλης Κρυπτογραφίας (ECC) και του Προηγμένου Προτύπου Κρυπτογράφησης (AES) προσφέρει μία πολλά υποσχόμενη λύση για την αντιμετώπιση προβλημάτων ασφάλειας σε περιβάλλοντα υπολογιστικών νεφών. Με τον συνδυασμό των δυνατών σημείων της Ελλειπτικής Καμπύλης Κρυπτογραφίας (ECC) και του Προηγμένου Προτύπου Κρυπτογράφησης (AES) διασφαλίζεται ο έλεγχος ταυτότητας, η ακεραιότητα των δεδομένων και η εμπιστευτικότητα, ενισχύοντας έτσι τη συνολική θέση ασφαλείας του υπολογιστικού νέφους στο περιβάλλον της Τέταρτης Βιομηχανικής Επανάστασης (Industry 4.0).

4.2. Ασφάλεια 6G Moblie

Η επικοινωνία απολαμβάνει μία ραγδαία εξέλιξη τα τελευταία χρόνια. Όλα ξεκίνησαν από την εφεύρεση του τηλεφώνου του Alexander Graham Bell το 1876 στις Ηνωμένες Πολιτείες Αμερικής (Η.Π.Α.) έως τη σημερινή τεχνολογία κινητής τηλεφωνίας, συμπεριλαμβανομένων φυσικά των επερχόμενων δικτύων κινητής τηλεφωνίας 6ης γενιάς (6G), η τεχνολογία έχει φέρει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι ανταλλάσσουν πληροφορίες. Οι τηλεπικοινωνίες, εξυπηρετούνται από ηλεκτρονικές συσκευές, έχουν προχωρήσει σημαντικά, με τα κινητά τηλέφωνα να γίνονται το κύριο μέσο επικοινωνίας και μετάδοσης δεδομένων. Η στροφή προς τα δίκτυα 5G διαδραματίζεται στο παρόν, με τις προσδοκίες ότι το 6G θα είναι το πρότυπο μέχρι το 2030. Το 6G θα έχιε την δυνατότητα να καλύψει τις τρέχουσες απαιτήσεις των χρηστών και να προσφέρει ακόμη πιο προηγμένες δυνατότητες.

Η ενοποίηση των τηλεπικοινωνιών με την τεχνολογία υπολογιστικού νέφους οδήγησε στην εμφάνιση του Κινητού Υπολογιστικού Νέφους (Mobile Cloud Computing), προσφέροντας προσαρμόσιμες επιλογές και ευέλικτες υλοποιήσεις. Η τεχνητή νοημοσύνη (Artificial Intelligence – AI) διαδραματίζει κρίσιμο ρόλο σε αρκετούς τομείς, μεταξύ των οποίων βρίσκονται οι υπηρεσίες δικτύου κινητής τηλεφωνίας (Mobile Network Services – MNS). Στις υπηρεσίες δικτύου κινητής τηλεφωνίας, η τεχνητή νοημοσύνη χρησιμοποιείται για την παρακολούθηση, τη διαχείριση και τον εντοπισμό απάτης, τη βελτίωση της ασφάλειας και της λειτουργίας του δικτύου.

Η σύγκλιση της τεχνολογίας του υπολογιστικού νέφους, της τεχνητής νοημοσύνης και των δικτύων κινητής τηλεφωνίας στο 6G αναμένεται να φέρει σημαντικές βελτιώσεις στις ανθρώπινες ζωές. Μερικά παραδείγματα αποτελούν η μείωση των τροχαίων ατυχημάτων, η προώθηση της υγειονομικής περίθαλψης και η μείωση των ποσοστών εγκληματικότητας. Ωστόσο, εξακολουθούν να υφίστανται προκλήσεις, όπως είναι η διαχείριση μεγάλου όγκου δεδομένων και η διασφάλιση συνδεσιμότητας υψηλής ταχύτητας για πολλές συσκευές.

Η ανάπτυξη των δικτύων 6G βρίσκεται σε εξέλιξη, εστιάζοντας κυρίως στην ενίσχυση της ασφάλειας μέσω εγκληματολογικών μηχανισμών, μέσω της αξιοποίησης υπολογιστών υψηλής απόδοσης για καλύτερες υπηρεσίες τελικού χρήστη. Μεθοδολογίες έρευνας, συμπεριλαμβανομένων τεχνικών, οργανωτικών και εστιασμένων στην εφαρμογή προσεγγίσεων στο περιβάλλον υπολογιστικού νέφους, χρησιμοποιούνται για την αντιμετώπιση διαφόρων πτυχών

όπως η επεξεργασία ροής σε πραγματικό χρόνο, η σύνδεση απομακρυσμένης επιφάνειας εργασίας και η δοκιμή απόδοσης.

Ταυτόχρονα, καταβάλλονται προσπάθειες για την παροχή δυναμικής και ποικίλης κατανομής πόρων για υπηρεσίες κατ' απαίτηση, έχοντας ως στόχο να καλύψουν ένα ευρύ φάσμα βιωματικών ευκαιριών, διασφαλίζοντας παράλληλα αξιοπιστία και αιτιολόγηση. Αυτή η προσέγγιση στοχεύει να περιορίσει το κοινό στόχο παγκοσμίως, παρέχοντας εξατομικευμένες υπηρεσίες, οι οποίες καλύπτουν αποτελεσματικά τις ατομικές ανάγκες.

Συνολικά, η πρόοδος της τεχνολογίας στον τομέα της επικοινωνίας από τα τηλέφωνα στα κινητά τηλέφωνα και τα επερχόμενα δίκτυα 6G, σε συνδυασμό με την τεχνολογία υπολογιστικών νεφών και την τεχνητή νοημοσύνη, υπόσχονται τα μέγιστα για τη βελτίωση των ανθρώπινων ζωών. Προκλήσεις όπως η διαχείριση δεδομένων, η συνδεσιμότητα, η ασφάλεια και η βελτιστοποίηση απόδοσης αντιμετωπίζονται μέσω συνεχών προσπαθειών έρευνας και ανάπτυξης. Τέλος, ο στόχος είναι η παροχή αποτελεσματικών, αξιόπιστων και εξατομικευμένων υπηρεσιών, οι οποίες ενισχύουν τη συνολική εμπειρία επικοινωνίας και συμβάλλουν στην κοινωνική ευημερία.

4.3. Διαδίκτυο των Πραγμάτων (IoT), Έξυπνες πόλεις

Η τεχνολογία υπολογιστικών νεφών και η τεχνολογία του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) είναι βασικές αναδυόμενες τεχνολογίες με επιπτώσεις στην ασφάλεια και το απόρρητο των δεδομένων. Οι προαναφερόμενες τεχνολογίες έχουν διευκολύνει τη διασύνδεση έξυπνων αντικειμένων σε έξυπνες πόλεις, οδηγώντας με αυτό τον τρόπο σε πολυάριθμες μελέτες, οι οποίες χρησιμοποιούν τεχνολογίες όπως είναι το IoT, τα Μεγάλα Δεδομένα (Big Data) και η τεχνολογία υπολογιστικού νέφους. Αυτές οι μελέτες καλύπτουν διάφορες πτυχές όπως για παράδειγμα είναι η ανάλυση της κυκλοφορίας, ο έλεγχος της ατμοσφαιρικής ρύπανσης, η συνδεσιμότητα των οχημάτων και οι υπηρεσίες έξυπνης στάθμευσης. Πολλά πλαίσια και πλατφόρμες έχουν προταθεί από τους Djigal, Jun, Lu (2017) για την επίτευξη της επεξεργασίας μεγάλου όγκου δεδομένων μεταφοράς, χρησιμοποιώντας τεχνολογίες υπολογιστικών νεφών όπως είναι τα GeoServer, GeoMesa, Accumulo, Spark και Hadoop.

Ωστόσο, καθώς η τεχνολογία υπολογιστικών νεφών είναι διακρατική, παρουσιάζει μία ποικιλία προκλήσεων ασφάλειας και απορρήτου σε τεχνικούς, επιχειρηματικούς και ρυθμιστικούς τομείς. Η ενοποίηση της τεχνολογίας Διαδικτύου των Πραγμάτων (IoT) και των δικτύων έξυπνων πόλεων ενισχύει περαιτέρω αυτές τις ανησυχίες. Οι προκλήσεις στην αποθήκευση και ανάλυση δεδομένων καταγραφής, οι οποίες δημιουργούνται από τα Intelligent Transport Systems (ITS) αντιμετωπίζονται μέσω πλατφορμών, οι οποίες ενσωματώνουν τεχνολογίες κατανεμημένης αποθήκευσης και μεγάλων δεδομένων όπως είναι το Apache Flume, το Hadoop HDFS, το Hive και το Spark. Έχουν προταθεί μηχανισμοί ασφαλείας για εφαρμογές έξυπνων πόλεων, συμπεριλαμβανομένων πλαισίων όπως το SMARTIE και πλατφορμών όπως το iKaas, τα οποία δίνουν προτεραιότητα στην ανωνυμία των χρηστών, το απόρρητο των δεδομένων και τον έλεγχο πρόσβασης και ταυτότητας. Ακόμη, από τους Djigal, Jun, Lu (2017) συζητούνται πρωτόκολλα, τα οποία βασίζονται σε αποδείξεις μηδενικής γνώσης (ZKP), τα οποία αντιμετωπίζουν συγκεκριμένα ζητήματα απορρήτου, τα οποία και σχετίζονται με δεδομένα τοποθεσίας, παράλληλα με προτάσεις για την προστασία του απορρήτου των οικονομικών πελατών μέσω των Προληπτικών Δυναμικών Ασφαλών Σχημάτων Δεδομένων (P2DS), τα οποία βασίζονται στον Έλεγχο πρόσβασης βάσει επιστροφών.

Η τεχνολογία υπολογιστικών νεφών προσφέρει πλεονεκτήματα όπως η αποθήκευση δεδομένων, η επεκτασιμότητα και η προσβασιμότητα, καθιστώντας τη ελκυστική για τους οργανισμούς, ώστε να διεξάγουν επιχειρηματικές δραστηριότητες. Ωστόσο, καθώς αυξάνεται η χρήση της τεχνολογίας υπολογιστικών νεφών, αυξάνονται και οι ανησυχίες για την ασφάλεια. Παρόλο που αρκετές έρευνες έχουν ασχοληθεί με την ασφάλεια στα περιβάλλοντα υπολογιστικών νεφών, υπάρχει έλλειψη εστίασης στις περιορισμένες εφαρμογές, οι οποίες ασχολούνται με το Διαδίκτυο των Πραγμάτων (IoT) και των έξυπνων δικτύων πόλεων.

Η άνοδος, λοιπόν, της τεχνολογίας του Διαδικτύου των Πραγμάτων (IoT) οδήγησε σε τεράστιο όγκο δεδομένων, τα οποία παράγονται από διαφορετικές πηγές. Η τεχνολογία του Διαδικτύου των Πραγμάτων (IoT) παρουσιάζει προκλήσεις στη διαλειτουργικότητα, την ασφάλεια και τη διαχείριση δεδομένων λόγω της τεράστιας και ετερογενούς φύσης των συσκευών. Πολλά πλαίσια ισχυρίζονται ότι έχουν τη δυνατότητα να αντιμετωπίσουν αυτά τα ζητήματα ενώ συμμορφώνονται και με τους κανονισμούς GDPR.

Η εξέλιξη στον τομέα της κεντρικής επεξεργασίας μεγάλων δεδομένων για πλαίσιο των έξυοπνων πόλεων και του Διαδικτύου των Πραγμάτων απαιτεί ισχυρά μέτρα ασφαλείας. Κατά τους Badii, Bellini, Difino, Nesi (2020) η αρχιτεκτονική Snap4City προσφέρει μία ολοκληρωμένη λύση ασφαλείας, συμπεριλαμβανομένων εφαρμογών, οι οποίες φιλοξενούνται σε περιβάλλοντα υπολογιστικών νεφών όσο και για εφαρμογές Διαδικτύου των Πραγμάτων (IoT) εντός εγκατάστασης, αναλυτικών στοιχείων δεδομένων και πινάκων εργαλείων, δίνοντας έμφαση στην ασφάλεια από το σχεδιασμό και την προεπιλογή για την προστασία ευαίσθητων δεδομένων πόλεων και προσωπικών δεδομένων. Ξεπερνά τις πιο πρόσφατες τεχνολογίες, όπως αποδεικνύεται από τις συγκρίσεις μεταξύ πλατφορμών και τα stress tests, συμπεριλαμβανομένων των δοκιμών διείσδυσης. Το Snap4City αναπτύχθηκε ως απάντηση σε μία ερευνητική πρόκληση από το έργο Select4Cities H2020, το οποίο στόχευε την κάλυψη των αναγκών των σύγχρονων έξυπνων πόλεων. Μετά από τρία χρόνια ανάπτυξης, το Snap4City επιλέχθηκε ως η νικήτρια λύση, έχοντας υποβληθεί σε αυστηρές δοκιμές και πιλοτικά σε ευρωπαϊκές πόλεις όπως η Αμβέρσα, το Ελσίνκι και η περιοχή της Τοσκάνης, αποδεικνύοντας υψηλά επίπεδα ασφάλειας και συμμόρφωσης με τον GDPR. Η πλατφόρμα αντιμετωπίζει διάφορα σενάρια περιπτώσεων χρήσης, προσφέροντας ακόμη διαφορετικά επίπεδα προστασίας με βάση την ευαισθησία των δεδομένων. Το Snap4City πληροί τις απαιτήσεις του GDPR και υπερβαίνει τις προσδοκίες εισάγοντας καινοτόμες λύσεις και καλύπτοντας συγκεκριμένες ανάγκες έργων.

Την ίδια στιγμή, προκλήσεις παρουσιάζονται στη δυναμική κοινή χρήση και τη διαχείριση δεδομένων, διατηρώντας παράλληλα το απόρρητο των χρηστών. Για την αντιμετώπιση αυτών των προκλήσεων, οι Djigal, Jun, Lu (2017) προτείνεται το Ασφαλές Πλαίσιο για τη Μελλοντική Έξυπνη Πόλη (SEFSCITY), το οποίο βασίζεται στην τεχνολογία υπολογιστικών νεφών, στην τεχνολογία του Διαδικτύου των Πραγμάτων και την τεχνολογία κατανεμημένου υπολογισμού (Distributed Computing). Η αρχιτεκτονική του SEFSCITY, με μία προσέγγιση Multi-Cloud και Cloud Federation. Ένα πρωτόκολλο ασφαλείας, το οποίο βασίζεται στο Πρωτόκολλο Μηδενικής Γνώσης και στο Πρόβλημα Διακριτού Λογαρίθμου Ελλειπτικής Καμπύλης προτείνεται για την προστασία ευαίσθητων δεδομένων. Το πλαίσιο επικυρώνεται μέσω διαφόρων σεναρίων, τα οποία εφαρμόζονται χρησιμοποιώντας το εργαλείο Cloud Analyst, επιδεικνύοντας σταθερό κόστος υποδομής για πελάτες υπηρεσιών υπολογιστικών νεφών και οφέλη για τους παρόχους υπηρεσιών υπολογιστικών νεφών, όσον αφορά τα έσοδα και το χρόνο επεξεργασίας δεδομένων.

Συνολικά, η ασφάλεια των δεδομένων αποτελεί σημαντική ανησυχία σε περιβάλλοντα υπολογιστικού νέφους, με αρκετές ευπάθειες να εμφανίζονται για εισβολές και παραβιάσεις δεδομένων. Τα ζητήματα ακεραιότητας δεδομένων, τα οποία επιτυγχάνονται μέσω της κρυπτογράφησης και με ελέγχους πρόσβασης, οι οποίοι σε συνδυασμό με τους ελέγχους ασφαλείας, οι οποίοι απαιτούνται πριν από τη μετεγκατάσταση των υπηρεσιών σε περιβάλλοντα υπολογιστικού νέφους. Ακόμη, κρίνεται αναγκαίο να υπάρχει τήρηση προτύπων ασφαλείας, έλεγχος των παρόχων υπηρεσιών, των ασφαλών API, της προστασίας επιπέδου μεταφοράς, του ελέγχου ταυτότητας, της διαχείρισης κλειδιών κρυπτογράφησης και των ισχυρών συμφωνιών υπηρεσιών μεταξύ παρόχων και καταναλωτών των υπηρεσιών υπολογιστικών νεφών.

4.4. Κοινωνικά Δίκτυα

Η ταχεία ανάπτυξη των κοινωνικών δικτύων και των υπηρεσιών υπολογιστικών νεφών είχε ως αποτέλεσμα την αύξηση των διαδικτυακών χρηστών, διευκολύνοντας τον μετασχηματισμό και την πρόσβαση στις πληροφορίες μεγάλης κλίμακας. Η ανάπτυξη, αυτή, συνοδεύτηκε από σημαντική κερδοφορία για τους οργανισμούς, οι οποίοι κατέχουν τους ιστότοπους κοινωνικής δικτύωσης και τις σχετικές εφαρμογές και οι οποίες τροφοδοτούνται από τη διευρυνόμενη βάση χρηστών. Ωστόσο την ίδια στιγμή, αυτή η αύξηση της διαδικτυακής δραστηριότητας εγείρει ανησυχίες και προκλήσεις, οι οποίες σχετίζονται με την αποθήκευση προσωπικών δεδομένων και το απόρρητο, ωθώντας για τον λόγο αυτό τους ερευνητές να εντοπίσουν λύσεις για την αντιμετώπιση ζητημάτων ασφάλειας στα κοινωνικά δίκτυα, τα οποία βασίζονται στην τεχνολογία υπολογιστικού νέφους.

Η τεχνολογία υπολογιστικού νέφους αναδεικνύεται ως μια βασική λύση για την αντιμετώπιση των κλιμακούμενων απαιτήσεων αποθήκευσης, οι οποίες προκύπτουν από την εκθετική αύξηση των δεδομένων. Η προσφορά του μοντέλου της αποθήκευσης ως υπηρεσία, οι πλατφόρμες υπηρεσιών υπολογιστικού νέφους επιτρέπουν στους χρήστες να διαχειρίζονται και να αποθηκεύουν τεράστιες ποσότητες δεδομένων με ευέλικτο και επεκτάσιμο τρόπο. Εντούτοις, η αποθήκευση προσωπικών δεδομένων σε ιστότοπους κοινωνικής δικτύωσης δημιουργεί εύλογες ανησυχίες σχετικά με παραβιάσεις του απορρήτου. Ως εκ τούτου, οι ερευνητές έχουν επικεντρώσει τις προσπάθειές τους στον μετριασμό των θεμάτων ασφάλειας, τα οποία εντοπίζονται στα

κοινωνικά δίκτυα, τα οποία βασίζονται στο υπολογιστικό νέφος και ιδιαιτέρως εκείνων που σχετίζονται με παραβιάσεις του απορρήτου και της ιδιωτικής ζωής.

Παρά τον αυξημένο αριθμό πλεονεκτημάτων, τα οποία προσφέρουν τα μοντέλα υπολογιστικού νέφους, εξακολουθούν να υπάρχουν προκλήσεις, οι οποίες σχετίζονται με την ασφάλεια, επηρεάζοντας με αυτό τον τρόπο την απόδοση και την αξιοπιστία των υπηρεσιών υπολογιστικού νέφους. Οι προκλήσεις περιλαμβάνουν ένα ευρύ φάσμα θεμάτων, στα οποία συμπεριλαμβάνονται παραβιάσεις του απορρήτου, ανησυχίες για την ακεραιότητα των δεδομένων, παραβιάσεις του απορρήτου, ζητήματα διαθεσιμότητας και περιορισμοί εξουσιοδότησης. Τα αδύναμα πρωτόκολλα κρυπτογράφησης και τα τρωτά σημεία, τα οποία παρουσιάζονται κατά την κρυπτογράφηση της κυκλοφορίας δικτύου ενέχουν πρόσθετους κινδύνους, εκθέτοντας δυνητικά εμπιστευτικές πληροφορίες σε μη εξουσιοδοτημένη πρόσβαση και χειραγώγηση.

Η πρόσβαση στα δεδομένα αναδεικνύεται ως σημαντικό εστιακό σημείο ανησυχιών για την ασφάλεια στα περιβάλλοντα υπολογιστικού νέφους. Η διασφάλιση της ακεραιότητας των δεδομένων σε όλη την κυκλοφορία του δίκτυου είναι πρωταρχικής σημασίας, προκειμένου να αποτραπεί η μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή δεδομένων. Παράλληλα, η διατήρηση ισχυρών μηχανισμών εξουσιοδότησης κρίνεται απαραίτητη για τη διασφάλιση της ασφαλούς μετάδοσης πληροφοριών και την αποτροπή μη εξουσιοδοτημένης πρόσβασης από κακόβουλους παράγοντες.

Οι πρόσφατες τεχνολογικές εξελίξεις, όπως οι ειδικές θήκες σύνδεσης, όπως οι κινητές συσκευές προηγμένης τεχνολογίας, έχουν προωθήσει περαιτέρω την εξέλιξη των κοινωνικών δικτύων και των τεχνολογιών ασύρματης επικοινωνίας. Οι καινοτομίες αυτές ταυτόχρονα με την ενίσχυση, τη συνδεσιμότητα και την προσβασιμότητα, εισάγουν νέες προκλήσεις ασφάλειας, γεγονός το οποίο απαιτεί προληπτικά μέτρα για την προστασία των χρηστών από πιθανές απειλές.

Η αντιμετώπιση των ανησυχιών για την ασφάλεια υπερβαίνει τις τεχνικές λύσεις. Μία πολύ σπουδαία παράμετρος είναι η διατήρηση της εμπιστοσύνης και της αυτονομίας των χρηστών. Η ενίσχυση του ελέγχου των εφαρμογών, των δεδομένων και των υπηρεσιών στους χρήστες αποτελεί παράγοντα ζωτικής σημασίας για τη διαφύλαξη του απορρήτου και της ασφάλειάς τους. Η τεχνολογία του Υπολογισμού Ακμών (Edge Computing) αναδεικνύεται ως ένα πολλά υποσχόμενο παράδειγμα, το οποίο μετατοπίζει τον έλεγχο των πόρων υπολογιστικού νέφους πιο

κοντά στην άκρη του δικτύου, ενισχύοντας με αυτό τον τρόπο την ασφάλεια και την απόδοση διατηρώντας παράλληλα την αυτονομία του χρήστη.

Υπό το φως αυτών των προκλήσεων αλλά και ευκαιριών περαιτέρω ανάπτυξης, προτείνεται ένα ολοκληρωμένο πλαίσιο για την εξέταση των θεμάτων ασφάλειας και απορρήτου, τα οποία εντοπίζονται στα κοινωνικά δίκτυα, τα οποία βασίζονται σε περιβάλλοντα υπολογιστικού νέφους. Αυτό το πλαίσιο έχει ως στόχο να παρέχει μια συστηματική προσέγγιση για τον εντοπισμό, την ανάλυση και τον μετριασμό των κινδύνων ασφαλείας, διασφαλίζοντας έτσι την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων σε περιβάλλοντα υπολογιστικών νεφφών.

Συμπερασματικά, η αντιμετώπιση των ανησυχιών για την ασφάλεια και το απόρρητο στα κοινωνικά δίκτυα, τα οποία βασίζονται στην τεχνολογία υπολογιστικών νεφών κρίνεται αναγκαία για την ενίσχυση της εμπιστοσύνης, της αυτονομίας των χρηστών και τη διευκόλυνση της υπεύθυνης και ηθικής χρήσης της τεχνολογίας στην ψηφιακή εποχή. Με την αξιοποίηση καινοτόμων λύσεων και με την υιοθέτηση προληπτικών μέτρων, οι ενδιαφερόμενοι έχουν την δυνατότητα να πλοηγηθούν στο εξελισσόμενο περιβάλλον του υπολογιστικού νέφους, προστατεύοντας παράλληλα τα συμφέροντα και τα δικαιώματα των χρηστών.

4.5. Blockchain

Σε περιβάλλοντα υπολογιστικών νεφών, η ασφάλεια παίζει πρωταγωνιστικό ρόλο για την προστασία των δεδομένων, των εφαρμογών και των υποδομών, χρησιμοποιώντας διάφορες πολιτικές και τεχνολογίες έτσι ώστε να εξασφαλιστεί αυτή η προστασία. Η τεχνολογία υπολογιστικών νεφών παίζει κεντρικό ρόλο στην ασφάλεια δικτύων και πληροφοριών, προσφέροντας στους οργανισμούς διαφορετικά μοντέλα υπηρεσιών και ανάπτυξης. Οι ανησυχίες, οι οποίες εγείρονται για την ασφάλεια στο φάσμα του υπολογιστικού νέφους κατηγοριοποιούνται σε ζητήματα, τα οποία αντιμετωπίζουν οι πάροχοι και οι καταναλωτές, τονίζοντας την ανάγκη για ισχυρή αρχιτεκτονική ασφάλειας για τον μετριασμό των επιθέσεων.

Η τεχνολογία Blockchain αναδεικνύεται ως μία πολλά υποσχόμενη λύση, γεγονός το οποίο οφείλεται στα χαρακτηριστικά ασφαλείας του ελέγχου ταυτότητας, της κρυπτογράφησης και της αξίας κατακερματισμού, καθώς και από το γεγονός ότι χαρακτηρίζεται από την αποκεντρωμένη

και αμετάβλητη φύση της, διαδραματίζει κρίσιμο ρόλο στην ενίσχυση της ασφάλειας και της αποτελεσματικότητας σε διάφορες πτυχές του υπολογιστικού νέφους. Η αποτελεσματικότητα και η διαθεσιμότητα της τεχνολογίας υπολογιστικού νέφους το καθιστούν ακρογωνιαίο λίθο των περιβαλλόντων πληροφορικής, με οργανισμούς να φιλοξενούν όλο και περισσότερο εφαρμογές σε πλατφόρμες υπολογιστικών νεφών όπως η Amazon, η Microsoft και η IBM, μειώνοντας με αυτό τον τρόπο το κόστος και βελτιώνοντας την προσβασιμότητα.

Ουσιαστικά, η ασφάλεια στα περιβάλλοντα υπολογιστικών νεφών είναι απαραίτητη και η τεχνολογία blockchain παρουσιάζει μία καινοτόμο προσέγγιση για την αντιμετώπιση των προκλήσεων ασφαλείας, διασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων σε περιβάλλοντα υπολογιστικών νεφών.

Η ασφάλεια της τεχνολογίας υπολογιστικών νεφών περιλαμβάνει τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλοντα υπολογιστικών νεφών και απαιτούν ισχυρά μέτρα ασφαλείας, εμπιστοσύνη, διασφάλιση, παρακολούθηση και διακυβέρνηση. Πολλές προκλήσεις, όπως ο προγραμματισμός εργασιών, η προστασία δεδομένων, η διαθεσιμότητα υπηρεσιών, η συμμόρφωση και οι νομικοί κίνδυνοι, σχετίζονται με υπολογισμούς και δεδομένα σε περιβάλλοντα υπολογιστικών νεφών.

Η διατήρηση του απορρήτου στο πλαίσιο της τεχνολογίας υπολογιστικών νεφών αντιμετωπίζεται μέσω διαφόρων αλγορίθμων κρυπτογράφησης όπως είναι ο αλγόριθμος RSA, ο αλγόριθμος AES και συναρτήσεων κατακερματισμού όπως η SHA512 και η bcrypt. Μέθοδοι όπως το Υβριδικό Κρυπτογραφικό Σύστημα (HCS) και οι ομομορφικοί αλγόριθμοι κρυπτογράφησης διασφαλίζουν την ασφάλεια και το απόρρητο των δεδομένων. Ωστόσο, ορισμένα συστήματα απαιτούν ασφαλή κανάλια μετάδοσης, κάτι το οποίο μπορεί να εμφανίσει μειονεκτήματα.

Η ακεραιότητα των δεδομένων στα περιβάλλοντα υπολογιστικών νεφών διασφαλίζεται μέσω προσεγγίσεων όπως τα σχήματα MAC, η αποδεδειγμένη κατοχή δεδομένων (PDP), η απόδειξη δυνατότητας ανάκτησης (POR), ο κατακερματισμός και η κρυπτογράφηση. Αλγόριθμοι όπως ο SHA-2 και ο AES χρησιμοποιούνται για τον έλεγχο της ακεραιότητας και για την κρυπτογράφηση. Ωστόσο, υπάρχουν προκλήσεις σχετικά με τον πλεονασμό δεδομένων και την υποστήριξη για λειτουργίες χειρισμού δεδομένων.

Τα ζητήματα στον χώρο αποθήκευσης και ελέγχου στα περιβάλλοντα υπολογιστικών νεφών περιλαμβάνουν τη διαρροή δεδομένων, τη διαχείριση κλειδιών και προβλήματα απόδοσης. Οι λύσεις, οι οποίες προτείνονται περιλαμβάνουν διαφανή διαχείριση κλειδιών, πρωτόκολλα ελέγχου ακεραιότητας απομακρυσμένων δεδομένων βάσει ταυτότητας και αποτελεσματικούς μηχανισμούς ανάκλησης χρήστη. Οι τρίτοι ελεγκτές διαδραματίζουν κρίσιμο ρόλο στην επαλήθευση της ακεραιότητας των δεδομένων και στην περιοδική ενημέρωση των κλειδιών, διασφαλίζοντας έτσι την αποτελεσματικότητα και την ασφάλεια των συστημάτων αποθήκευσης στα πλαίσια του υπολογιστικού νέφους.

Κατά τους Pavithra, Ramya και Prathibha (2019) προτείνεται ένα σύστημα, το οποίο αξιοποιεί την τεχνολογία blockchain, και ονομάζεται Cloud Trust, με στόχο την αύξηση της διαφάνειας και τη μείωση της εξάρτησης από αξιόπιστα τρίτα μέρη. Τα έξυπνα συμβόλαια σε πλατφόρμες όπως το Ethereum διευκολύνουν τις αλληλεπιδράσεις μεταξύ διαφορετικών μερών χωρίς να υπάρχει ανάγκη για μεσάζοντες. Το πλαίσιο ενσωματώνει ένα μοντέλο πεποίθησης και σύστασης, το οποίο υπολογίζει τα όρια εμπιστοσύνης προμηθευτών με βάση στοιχεία και εμπειρία. Ταυτόχρονα, παρουσιάζεται ένα άλλο σύστημα με το όνομα Saranyu, το οποίο χρησιμοποιεί έξυπνα συμβόλαια, τα οποία εκτελούνται σε ένα κατανεμημένο καθολικό για τη διαχείριση λογαριασμών ενοικιαστών και υπηρεσιών σε κέντρα δεδομένων υπολογιστικών νεφών. Προσφέρει υπηρεσίες διαχείρισης και ελέγχου ταυτότητας, εξουσιοδότησης και χρέωσης. Το Saranyu εφαρμόζεται στο σύστημα blockchain Quorum, παρόμοιο με το Ethereum, επιτρέποντας αποκεντρωμένες αρχιτεκτονικές υπολογιστικών νεφών. Ακόμη, το ChainFS, ένα σύστημα ενδιάμεσου λογισμικού, εισάγεται για την ασφαλή αποθήκευση δεδομένων σε περιβάλλοντα υπολογιστικών νεφών χρησιμοποιώντας τεχνολογία blockchain. Εφαρμοσμένο σε πλατφόρμες όπως το Ethereum και το Amazon S3, το ChainFS ελαχιστοποιεί τα έξοδα, διασφαλίζοντας την ίδια στιγμή την ακεραιότητα και την ασφάλεια των δεδομένων. Χρησιμοποιεί δοκιμές Merkle και λειτουργίες κατακερματισμού όπως το SHA256 για επαλήθευση και αλληλεπίδραση μεταξύ των πελατών Fuse και του blockchain.

Το προτεινόμενο σύστημα έχει στόχο συστήματα υγειονομικής περίθαλψης, δίνοντας έμφαση στην ασφαλή μεταφορά και αποθήκευση δεδομένων σε περιβάλλοντα υπολογιστικών νεφών. Τα αρχεία κρυπτογραφούνται χρησιμοποιώντας τον αλγόριθμο AES και η ακεραιότητα διατηρείται μέσω αλγορίθμων MD5 ή SHA. Οποιεσδήποτε τροποποιήσεις στα δεδομένα υπάρχει

η δυνατότητα να εντοπιστούν. Επιπλέον, η τεχνολογία blockchain χρησιμοποιείται για την περαιτέρω βελτίωση της ασφάλειας της τεχνολογίας υπολογιστικού νέφους.

Η ενοποίηση του blockchain και της τεχνολογίας υπολογιστικών νεφών αντιμετωπίζει διάφορες προκλήσεις, ιδιαίτερα ως προς τη μείωση του κόστους και την αποκέντρωση. Το κόστος των υπηρεσιών υπολογιστικού νέφους μπορεί να μετριαστεί με την αξιοποίηση της αποκεντρωμένης φύσης του blockchain και της αδράνειας υπολογιστικής ισχύος από μία ομάδα παρόχων. Οι λύσεις υπολογιστικών νεφών, οι οποίες υποστηρίζονται από blockchain προσφέρουν βελτιωμένη ασφάλεια καθώς τα δεδομένα διαχέονται και είναι δύσκολο για τους επιτιθέμενους (χάκερ) να έχουν πρόσβαση σε σύγκριση με τις παραδοσιακές μεθόδους αποθήκευσης. Ουσιαστικά, η τεχνολογία blockchain παρουσιάζει ευκαιρίες για τη βελτίωση διαφόρων πτυχών της τεχνολογίας υπολογιστικών νεφών, συμπεριλαμβανομένων των σημαντικών παραγόντων της εμπιστοσύνης, της ασφάλειας και της σχέσης κόστους-αποτελεσματικότητας, καθιστώντας την μία πολλά υποσχόμενη λύση για την αντιμετώπιση προκλήσεων σε περιβάλλοντα υπολογιστικών νεφών.

Συνολικά, η τεχνολογία υπολογιστικών νεφών υπόσχεται σημαντικά το μέλλον της τεχνολογίας υπολογιστών και αποθήκευσης. Διάφορες μέθοδοι και πρωτόκολλα αντιμετωπίζουν διαφορετικές πτυχές της ασφάλειας στην τεχνολογία υπολογιστικών νεφών, με στόχο τον μετριασμό των κινδύνων και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, τα οποία είναι αποθηκευμένα σε περιβάλλοντα υπολογιστικών νεφών.

4.6. Κυβερνητικά Υπολογιστικά Νέφη

Πολλές κυβερνητικές υπηρεσίες και δημόσιες διοικήσεις ανά τον κόσμο πλησιάζουν στην πλήρη μεταφορά των υπολογιστικών τους πόρων σε περιβάλλοντα υπολογιστικών νεφών. Η διεργασία αυτή παρουσιάζει πάρα πολλές πολυπλοκότητες αλλά και δυσκολία ως προς την υιοθέτηση των υπηρεσιών υπολογιστικών νεφών από τους δημόσιους φορείς. Ταυτόχρονα, η πιθανή χρήση της τεχνολογίας υπολογιστικών νεφών μπορεί να εμφανίσει οφέλη, όπως η επεκτασιμότητα, η ελαστικότητα, η απόδοση, αλλά και η ανθεκτικότητα στους τομείς της ασφάλειας και της οικονομικής απόδοσης. Ωστόσο, κατά τη διαδικασία της υιοθέτησης και

ενσωμάτωσης των τεχνολογιών υπολογιστικών νεφών, πολύ σημαντική θεωρείται η διαχείριση κινδύνων.

Η έκθεση του ENISA (2011) δίνει έμφαση στα οφέλη, τα οποία μπορεί να προσφέρει η τεχνολογία υπολογιστικού νέφους για δημόσιους φορείς, συμπεριλαμβανομένης της επεκτασιμότητας, της ελαστικότητας, της απόδοσης, της ανθεκτικότητας, της ασφάλειας και της οικονομικής απόδοσης. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) (2011) πρότεινε ένα δομημένο μοντέλο λήψης αποφάσεων, το οποίο απευθύνεται σε ανώτερα στελέχη και στόχο έχει την αξιολόγηση των παραμέτρων ασφάλειας και ανθεκτικότητας, των λειτουργικών και νομικών πτυχών και των διαθέσιμων αρχιτεκτονικών επιλογών κατά την εξέταση λύσεων, οι οποίες βασίζονται σε τεχνολογίες υπολογιστικών νεφών. Ακόμη, επισημαίνει ότι καλό είναι να γίνεται σύγκριση μεταξύ των μοντέλων υπολογιστικών νεφών (κοινοτικά, ιδιωτικά και δημόσια) σημειώνοντας την σπουδαιότητα της ανάλυσης SWOT για το καθένα, αλλά και εστιάζοντας κυρίως στις πτυχές ασφάλειας και ανθεκτικότητας, τις λειτουργικές, νομικές και αρχιτεκτονικές παραμέτρους.

Σε ένα ενδεικτικό σενάριο, το οποίο παρουσιάζεται στην έκθεση, ο Υπουργός Επικοινωνιών και Τεχνολογίας βρίσκεται αντιμέτωπος με μία πολύ σημαντική απόφαση για το αν θα μεταφέρει τις κυβερνητικές υπηρεσίες υπολογιστών σε περιβάλλον υπολογιστικού νέφους. Το σενάριο περιλαμβάνει μία ομάδα εργασίας, η οποία αποτελείται από άτομα διαφόρων τομέων, τα οποία συζητούν τα πλεονεκτήματα και τα μειονεκτήματα της υιοθέτησης της τεχνολογίας υπολογιστικού νέφους. Οι ανησυχίες, οι οποίες εκφράζονται περιλαμβάνουν τροποποιήσεις σε υπάρχουσες εφαρμογές, ανάκτηση από κάποια ενδεχόμενη καταστροφή, ευθύνη, απώλεια άμεσου ελέγχου, τοποθεσία αποθήκευσης δεδομένων και πιθανούς κινδύνους, οι οποίοι και σχετίζονται με τη χρήση μη ευρωπαϊκών παρόχων υπηρεσιών υπολογιστικού νέφους. Η έκθεση υπογραμμίζει τις πολυπλοκότητες και τις εκτιμήσεις, οι οποίες εμπλέκονται στην υιοθέτηση της τεχνολογίας υπολογιστικού νέφους από την κυβέρνηση, αγγίζοντας θέματα όπως ο έλεγχος δεδομένων, η ασφάλεια και οι εθνικές δυνατότητες.

Επιπλέον, η έκθεση περιγράφει διάφορα σενάρια όπως η χρήση της τεχνολογίας υπολογιστικού νέφους σε υπηρεσίες υγειονομικής περίθαλψης, σε ηλεκτρονικές διοικητικές διαδικασίες αλλά και σε κυβερνητικό περιβάλλον υπολογιστικού νέφους ως θερμοκοιτίδα επιχειρήσεων. Πιο αναλυτικά παραδείγματα αυτών των σεναρίων είναι τα Ηλεκτρονικά Μητρώα

Υγείας (EHR) και οι Ηλεκτρονικές Διοικητικές Διαδικασίες (EAP), στα οποία είναι αναγκαίο να υπογραμμιστεί η σημασία της ασφαλούς πρόσβασης σε πραγματικό χρόνο στα αρχεία υγείας των ασθενών, την υποστήριξη αποφάσεων για τους κλινικούς ιατρούς, την αυτοματοποίηση των ροών εργασίας και την ασφάλεια δεδομένων. Τέλος, πρωτοβουλίες όπως το CSA Guidance και το Cybersecurity Assessment and Management Methodology (CAMM) στοχεύουν στην ενίσχυση της διαφάνειας και της διασφάλισης για τη χρήση των δημόσιων περιβαλλόντων υπολογοστικών νεφών σε εφαρμογές, οι οποίες διαχειρίζονται ευαίσθητα δεδομένα.

Συνολικά, η έκθεση του ENISA (2011) στοχεύει να βοηθήσει τους δημόσιους οργανισμούς και τα κράτη μέλη της Ευρωπαϊκής Ένωσης στον καθορισμό στρατηγικών στο περιβάλλον υπολογιστικών νεφών, λαμβάνοντας παράλληλα υπόψη την ασφάλεια, την ανθεκτικότητα και τις νομικές πτυχές. Ταυτόχρονα, η έκθεση παρέχει μία ολοκληρωμένη επισκόπηση των ευκαιριών, των προβληματισμών και των προκλήσεων, οι οποίες σχετίζονται με την υιοθέτηση της τεχνολογία υπολογιστικών νεφών από κυβερνητικούς φορείς, προσφέροντας παράλληλα πληροφορίες για τη διαδικασία λήψης αποφάσεων, εκτιμήσεις κινδύνου και πρακτικές συστάσεις για τις εθνικές κυβερνήσεις και τους δημόσιους φορείς, οι οποίοι αξιολογούν τις επιλογές υπολογιστικών νεφών. Συνιστάται στις κυβερνήσεις να υιοθετήσουν μία σταδιακή προσέγγιση για την ενσωμάτωση της τεχνολογίας υπολογιστικών νεφών στις δραστηριότητές τους λόγω της πολυπλοκότητας και των άγνωστων μεταβλητών, οι οποίες είναι εγγενείς στα περιβάλλοντα υπολογιστικών νεφών. Οι δημόσιοι διαχειριστές κρίνεται απαραίτητο να αξιολογούν προσεκτικά τις διασυνδέσεις και τις εξαρτήσεις του συστήματος κατά τη μεταφορά υπηρεσιών σε περιβάλλοντα υπολογιστικών νεφών. Οι απαιτήσεις ασφάλειας και ανθεκτικότητας κάθε εφαρμογής είναι αναγκαίο να αξιολογούνται μεμονωμένα σε σχέση με τις διαθέσιμες αρχιτεκτονικές υπολογιστικών νεφών και τους ελέγχους ασφαλείας. Οι κυβερνήσεις, σε συνεργασία με την Ευρωπαϊκή Ένωση, θα πρέπει να αναπτύξουν μακροπρόθεσμες στρατηγικές λαμβάνοντας υπόψη τις επιπτώσεις στην ασφάλεια και την ανθεκτικότητα. Πολύ σημαντική παράμετρος είναι η μελέτη του ρόλου της τεχνολογίας υπολογιστικών νεφών στην προστασία των κρίσιμων υποδομών πληροφοριών και της εξέτασης το ενδεχομένου ενός ευρωπαϊκού κυβερνητικού υπολογιστικού νέφους για εναρμονισμένους κανόνες και διαλειτουργικότητα. Επομένως, συνιστάται μία ολοκληρωμένη προσέγγιση για την αποτελεσματική υιοθέτηση της τεχνολογίας υπολογιστικών νεφών, αντιμετωπίζοντας παράλληλα ζητήματα ασφάλειας, ανθεκτικότητας και νομικής φύσεως.

4.7. Υπολογιστικά νέφη προσωπικών δεδομένων

Τα περιβάλλοντα υπολογιστικών νεφών για προσωπικά δεδομένα (Personal Data Cloud – PDC) έχουν σχεδιαστεί με μεγάλη έμφαση στον έλεγχο των χρηστών, τη διαχείριση κοινής χρήσης δεδομένων και στις τεχνολογίες ενίσχυσης της ιδιωτικότητας, ενσωματώνοντας διάφορους μηχανισμούς προστασίας δεδομένων. Τα μέτρα ασφαλείας, τα οποία συνιστώνται από τον ENISA (2016) για τα PDC περιλαμβάνουν την εφαρμογή ισχυρότερου ελέγχου ταυτότητας, διαφανείς διαδικασίες παραβίασης δεδομένων και κρυπτογράφηση με στόχο την ενίσχυση της ασφάλειας δεδομένων.

Ωστόσο, τα περιβάλλοντα υπολογιστικών νεφών για προσωπικά δεδομένα αντιμετωπίζουν πολλές προκλήσεις απορρήτου σχετικά με την ποιότητα των δεδομένων, την ευαισθησία του ελέγχου των χρηστών και τη λεπτή ισορροπία μεταξύ της χρηστικότητας και των μοντέλων, τα οποία βασίζονται στη συναίνεση. Για την αντιμετώπιση αυτών των προκλήσεων, οι προτάσεις του ENISA (2016) περιλαμβάνουν την προώθηση του ελέγχου των χρηστών, την υιοθέτηση τεχνολογιών, οι οποίες βελτιώνουν το απόρρητο και την υποστήριξη πολιτικών, οι οποίες αναγνωρίζουν τα PDC ως εργαλεία ενίσχυσης της ιδιωτικής ζωής.

Η χρηστοκεντρικότητα, δηλαδή η φιλικότητα προς το χρήστη, βρίσκεται στον πυρήνα του σχεδιασμού των περιβαλλόντων υπολογιστικών νεφών για προσωπικά δεδομένα, επιτρέποντας με αυτό τον τρόπο στους χρήστες να ελέγχουν την επεξεργασία δεδομένων, τις προτιμήσεις και τα μέτρα ασφαλείας, όπως η κρυπτογράφηση και ο έλεγχος ταυτότητας. Η διαχείριση των προνομίων και του ελέγχου πρόσβασης ενδυναμώνει ακόμη περισσότερο τους χρήστες, αφού τους επιτρέπουν να ορίζουν δικαιώματα πρόσβασης και κοινής χρήσης δεδομένων, ενισχύοντας έτσι τον έλεγχο των χρηστών και την ασφάλεια των δεδομένων.

Η ιχνηλασιμότητα εντός των περιβαλλόντων υπολογιστικών νεφών για προσωπικά δεδομένα είναι ζωτικής σημασίας για την παρακολούθηση των ενεργειών των χρηστών, των τροποποιήσεων δεδομένων και της πρόσβασης, αποτελεί απαραίτητο παράγοντα για τη διαχείριση καταχρήσεων και τη διασφάλιση της λογοδοσίας. Επιπλέον, οι δυνατότητες φορητότητας δεδομένων επιτρέπουν στους χρήστες να αποθηκεύουν δεδομένα σε αναγνώσιμες μορφές και να

τα μεταφέρουν πολύ εύκολα μεταξύ περιβαλλόντων υπολογιστικών νεφών για προσωπικά δεδομένα, βελτιώνοντας έτσι τον έλεγχο και τη φορητότητα των δεδομένων.

Η τεχνική επιβολή των προτιμήσεων απορρήτου παραμένει μία πρόκληση, ο ENISA (2016) επισημαίνει την ανάγκη για πρακτικές εφαρμογές όσον αφορά τη διασφάλιση του ελέγχου των χρηστών. Συμπληρωματικά, η έννοια των Δικαιωμάτων Παραγωγού Δεδομένων αντιμετωπίζει ιδιαίτερες προκλήσεις ιδιοκτησίας στην εποχή των συνδεδεμένων συσκευών και των αναλυτικών στοιχείων μεγάλων δεδομένων, υποστηρίζοντας τη δίκαιη κατανομή κερδών, τα οποία δημιουργούνται από δεδομένα.

Συμπερασματικά, τα ενδιαφερόμενα μέρη γύρω από τα περιβάλλοντα υπολογιστικών νεφών για προσωπικά δεδομένα ενθαρρύνονται να συνεχίσουν να αναπτύσσουν κέντρα δεδομένων, με έμφαση όμως στην ενίσχυση του ελέγχου των χρηστών, των χαρακτηριστικών απορρήτου και των εργαλείων διαχείρισης δεδομένων για την καθιέρωση των περιβαλλόντων υπολογιστικών νεφών για προσωπικά δεδομένα ως αποτελεσματικών τεχνολογιών που βελτιώνουν το απόρρητο.

4.8. Ασφάλεια και Προστασία Απορρήτου για την Αποθήκευση Δεδομένων

Όλο και περισσότεροι οργανισμοί αλλά και ιδιώτες επιλέγουν για την αποθήκευση των δεδομένων τους, τις υπηρεσίες υπολογιστικού νέφους. Το γεγονός αυτό πέρα από τα πλεονεκτήματα, τα οποία μπορεί να προσφέρει η τεχνολογία του υπολογιστικού νέφους, συμπεριλαμβανομένων του χαμηλού κόστους και της ελαστικότητας, εγκυμονεί και αρκετούς κινδύνους και προκλήσεις. Οι απαιτήσεις ασφαλείας των δεδομένων και η προστασία του απορρήτου στα συστήματα αποθήκευσης, τα οποία φιλοξενούνται σε περιβάλλοντα υπολογιστικών νεφών είναι η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα των δεδομένων, η ασφαλής κοινή χρήση δεδομένων, η ανθεκτικότητα στη διαρροή και η πλήρης διαγραφή δεδομένων.

Την ίδια στιγμή, παρουσιάζονται προκλήσεις όπως είναι ο λεπτομερής έλεγχος πρόσβασης, ο οποίος αφορά τον καθορισμό των πολιτικών ελέγχου πρόσβασης, οι οποίες είναι υπεύθυνες για τη διασφάλιση της εξουσιοδοτημένης πρόσβασης σε συγκεκριμένα δεδομένα. Ταυτόχρονα, ένα σημαντικό ζήτημα, το οποίο κρίνεται αναγκαίο να θιχτεί είναι αυτό των κακόβουλων παρόχων

υπηρεσιών υπολογιστικού νέφους, οι οποίοι έχουν τη δυνατότητα να αποτελέσουν σημαντικό κίνδυνο για την ασφάλεια και το απόρρητο των δεδομένων, τα οποία φιλοξενούν. Ακόμη, η συμμόρφωση με τη διαγραφή δεδομένων αποτελεί σημαντικό παράγοντα για να διασφαλιστεί ότι τα δεδομένα διαγράφονται με ασφάλεια και είναι μη ανακτήσιμα όταν δεν χρειάζονται πλέον. Αυτό είναι σημαντικό στην αποθήκευση δεδομένων σε περιβάλλοντα υπολογιστικού νέφους για την αποφυγή παραβιάσεων και τη διασφάλιση του απορρήτου των δεδομένων. Τέλος, οι επιθέσεις πλευρικού καναλιού είναι ένας τύπος επίθεσης, ο οποίος εκμεταλλεύεται τη διαρροή πληροφοριών από αλγόριθμους κρυπτογράφησης. Αυτές οι επιθέσεις μπορούν να χρησιμοποιηθούν για την απόκτηση ευαίσθητων πληροφοριών, όπως κλειδιά κρυπτογράφησης, παρακολουθώντας την κατανάλωση ενέργειας, την ηλεκτρομαγνητική ακτινοβολία ή άλλες πληροφορίες πλευρικών καναλιών.

Η κρυπτογράφηση δεδομένων σε περιβάλλοντα υπολογιστικών νεφών κρίνεται απαραίτητα καθώς αποτελεί αξιοσημείωτο μέτρο για την ιδιωτικότητα των δεδομένων. Πολύ συχνά παρατηρείται η χρήση της κρυπτογράφησης βάσει χαρακτηριστικών (Attribute-Based Encryption – ABE) για την ασφαλή κοινή χρήση δεδομένων σε συστήματα αποθήκευσης υπολογιστικών νεφών. Η κρυπτογράφηση βάσει χαρακτηριστικών (ABE) είναι μία μορφή κρυπτογράφησης, η οποία δίνει τη δυνατότητα λεπτομερή έλεγχου πρόσβασης σε κρυπτογραφημένα αρχεία με βάση τα χαρακτηριστικά του χρήστη. Δύο βασικοί τύποι κρυπτογράφησης βάσει χαρακτηριστικών ABE είναι η κρυπτογράφηση βασισμένη σε χαρακτηριστικά κλειδιού (Key-Policy Attribute-Based Encryption – KP-ABE) και κρυπτογράφηση με βάση το χαρακτηριστικό της πολιτικής κρυπτογράφησης (Ciphertext-Policy Attribute-Based Encryption – CP-ABE). Στην περίπτωση της KP-ABE, κάθε κρυπτογραφημένο κείμενο σχετίζεται με ένα σύνολο χαρακτηριστικών, ενώ το ιδιωτικό κλειδί του χρήστη σχετίζεται με μία πολιτική πρόσβασης για αυτά τα χαρακτηριστικά. Ενώ, στην περίπτωση της CP-ABE, η πολιτική είναι ενσωματωμένη στο κρυπτογραφημένο κείμενο και το ιδιωτικό κλειδί του χρήστη σχετίζεται με το σύνολο των αντίστοιχων χαρακτηριστικών.

Συνοπτικά, η διατήρηση της ασφάλειας και του απορρήτου των δεδομένων είναι σημαντική στο χώρο αποθήκευσης στο περιβάλλον υπολογιστικού νέφους, προκειμένου να διασφαλιστεί ότι τα ευαίσθητα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση,

παραβίαση και διαρροή. Αυτό μπορεί να επιτευχθεί μέσω κρυπτογράφησης, ελέγχου πρόσβασης και άλλων μέτρων ασφαλείας.

4.9. Μεγάλα Δεδομένα (Big Data)

Τα μεγάλα δεδομένα αφορούν μεγάλους όγκους δομημένων, ημιδομημένων και μη δομημένων δεδομένων, τα οποία συνεχώς αυξάνονται. Η διαχείριση μεγάλων ποσοτήτων δεδομένων παρουσιάζει δυσκολία με τα παραδοσιακά συστήματα βάσεων δεδομένων, τα οποία απαιτούν υψηλή συντήρηση και κόστος. Η τεχνολογία υπολογιστικού νέφους έχει αναδειχθεί ως πιθανή λύση σε αυτό το πρόβλημα λόγω της επεκτασιμότητας και της προσβασιμότητας του, καθιστώντας έτσι το επικρατέστερο από άποψη χρήσης σε διάφορους τομείς, όπως για παράδειγμα είναι οι κυβερνήσεις, η υγειονομική περίθαλψη και οι τράπεζες. Ωστόσο, δεδομένου ότι η διαχείριση των διακομιστών σε περιβάλλοντα υπολογιστικών νεφών γίνεται από τρίτους παρόχους, η ασφάλεια των δεδομένων αποτελεί ίσως την σημαντικότερη ανησυχία τόσο για προσωπικούς όσο και για επιχειρηματικούς χρήστες. Απειλές όπως το phishing, τα botnets και η απώλεια δεδομένων απαιτούν ιδιαίτερη προσοχή σε περιβάλλοντα υπολογιστικών νεφών. Οι παραδοσιακές τεχνικές ασφαλείας όπως τα τείχη προστασίας (firewalls) και το λογισμικό προστασίας από ιούς (antivirus) δεν είναι πάντα αρκετά για την προστασία μεγάλων δεδομένων σε εικονικά συστήματα.

Τα μεγάλα δεδομένα περιλαμβάνουν πολύ μεγάλα σύνολα δεδομένων, τα οποία προέρχονται από διάφορες πηγές, όπως τραπεζικές εργασίες, μάρκετινγκ και μέσα κοινωνικής δικτύωσης. Οι ορισμοί των μεγάλων δεδομένων ποικίλλουν μεταξύ των διάφορων βιομηχανιών εστιάζοντας συχνά σε χαρακτηριστικά όπως ο όγκος, η ποικιλία, η ταχύτητα, η ορατότητα, η ακρίβεια και η αξία των δεδομένων. Η τεχνολογία υπολογιστικού νέφους ενσωματώνεται όλο και περισσότερο με τεχνολογίες μεγάλων δεδομένων, παρέχοντας με αυτό τον τρόπο πόρους κατά απαίτηση για αποθήκευση, επεξεργασία και ανάλυση.

Η διαχείριση μεγάλων δεδομένων συνοδεύεται από προκλήσεις, όπως για παράδειγμα είναι οι απαιτήσεις χώρου, το υψηλό κόστος και τα ζητήματα συντήρησης. Η τεχνολογία υπολογιστικού νέφους εμφανίζεται ως μία πιθανή λύση, αφού έχει τη δυνατότητα να παρέχει απεριόριστους πόρους για την ανάλυση, την αποθήκευση και τη διαχείριση μεγάλων δεδομένων.

Το εξελισσόμενο τοπίο των μεγάλων δεδομένων και της τεχνολογίας υπολογιστικού νέφους, εμφανίζει προκλήσεις ασφαλείας και απορρήτου από εσωτερικές και εξωτερικές παραβιάσεις δεδομένων και διαρροή. Η ασφάλεια των δεδομένων, λοιπόν, έχει γίνει μία κρίσιμη ανησυχία και ιδιαίτερα κατά τη μεταφορά και αποθήκευση δεδομένων σε διακομιστές, οι οποίοι φιλοξενούνται σε περιβάλλοντα υπολογιστικών νεφών. Οι ανησυχίες αυτές είναι σημαντικό να αντιμετωπιστούν, ούτως ώστε να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα των δεδομένων σε περιβάλλοντα υπολογιστικών νεφών.

Σε έρευνες έχουν προταθεί διάφορες τεχνικές για τη βελτίωση της ασφάλειας δεδομένων στην τεχνολογία υπολογιστικού νέφους, μέσα στις οποίες συγκαταλέγονται η κρυπτογράφηση πολλαπλών επιπέδων, η κατηγοριοποίηση δεδομένων και οι μηχανισμοί ελέγχου ταυτότητας. Αναλυτικότερα, η χρήση της κρυπτογράφησης πολλαπλών επιπέδων, χαρακτηριστικά παραδείγματα της οποίας είναι οι αλγόριθμοι RSA και AES, για την ασφάλεια των δεδομένων, τα οποία αποστέλλονται σε περιβάλλοντα υπολογιστικών νεφών, καθιστώντας έτσι δύσκολη την αποκρυπτογράφηση για μη εξουσιοδοτημένους χρήστες. Η κατηγοριοποίηση δεδομένων, από την άλλη πλευρά, κατηγοριοποιεί τα δεδομένα σε κανονικές, ευαίσθητες και κρίσιμες κατηγορίες και τα αποθηκεύει σε διαφορετικά κέντρα υπολογιστικών νεφών με βάση τη σημασία τους και τη χρήση τεχνικών κρυπτογράφησης για την προστασία τους από επιθέσεις πλευρικού καναλιού. Την ίδια στιγμή, ένας μηχανισμός ασφαλείας πολλαπλών σταδίων συνδυάζει τεχνικές ελέγχου ταυτότητας, ανίχνευσης εισβολής και κρυπτογράφησης, με σκοπό την προστασία από επιθέσεις κατανεμημένη άρνηση υπηρεσίας (DDoS) και επιθέσεις man-in-the-middle, και ο οποίος έχει δυνατότητες ενσωμάτωσης σε διάφορα μοντέλα ανάπτυξης υπολογιστικών νεφών.

Συμπερασματικά, ο ρόλος της ασφάλειας δεδομένων σε περιβάλλοντα υπολογιστικών νεφών κρίνεται ιδιαίτερα κρίσιμος και υπάρχει συνεχής ανάγκη για καινοτόμες προσεγγίσεις σχετικά με την προστασία των δεδομένων, τα οποία αποθηκεύονται και υποβάλλονται σε επεξεργασία στο περιβάλλον υπολογιστικών νεφών.

Συμπεράσματα και Μελλοντική έρευνα

Η τεχνολογία υπολογιστικών νεφών έχει αποκτήσει σε σύντομο χρονικό διάστημα δημοτικότητα λόγω της ζήτησης για υπηρεσίες, οι οποίες βασίζονται στο διαδίκτυο από διάφορους οργανισμούς και ιδιώτες. Τα δεδομένα μεταφέρονται σε διακομιστές υπολογιστικών νεφών με γρήγορο ρυθμό. Οι οργανισμοί μεταφέρουν όλο και περισσότερο τον φόρτο εργασίας σε διακομιστές, οι οποίοι παρέχονται σε περιβάλλοντα υπολογιστικών νεφών για να μειώσουν το κόστος, τον χώρο και τα προβλήματα συντήρησης, τα οποία σχετίζονται με μεγάλα δεδομένα. Ωστόσο, παρά τα πλεονεκτήματά του, τα δεδομένα, τα οποία φιλοξενούνται σε περιβάλλοντα υπολογιστικών νεφών δεν είναι απολύτως ασφαλή από εσωτερικές και εξωτερικές επιθέσεις, καθώς οι διακομιστές διαχειρίζονται από παρόχους υπηρεσιών υπολογιστικού νέφους (τρίτα μέρη). Αυτό έχει ως συνέπεια, η διασφάλιση της ασφάλειας των δεδομένων να αποτελεί ζωτικής σημασίας παράγοντα, ειδικά για ευαίσθητες πληροφορίες, οι οποίες είναι αποθηκευμένες σε περιβάλλοντα υπολογιστικών νεφών.

Οι συνεχόμενες προκλήσεις και απειλές, τις οποίες αντιμετωπίζουν οι διακομιστές σε περιβάλλοντα υπολογιστικών νεφών, όπως παραβιάσεις δεδομένων και διαρροή, τονίζει την ανάγκη για συνεχή ανάπτυξη και βελτιστοποίηση πλαισίων και αρχιτεκτονικών με στόχο τη διασφάλιση της ασφάλειας δεδομένων στο περιβάλλον υπολογιστικού νέφους. Αυτό συνεπάγεται το γεγονός ότι η ασφάλεια στην τεχνολογία υπολογιστικού νέφους είναι ένα εξελισσόμενο πεδίο και αναγνωρίζεται ότι οι μελλοντικές βελτιώσεις θα είναι απαραίτητες ώστε να οδηγούν στην αποτελεσματική αντιμετώπιση των αναδυόμενων απειλών και προκλήσεων. Ακόμη, καλό είναι να υπάρχει μία προληπτική προσέγγιση για τη βελτίωση της ασφάλειας στα περιβάλλοντα υπολογιστικών νεφών, όπως υποδεικνύεται από τη σύσταση για εφαρμογή διαφόρων μεθοδολογιών, όπως είναι οι τεχνικές ελέγχου ταυτότητας πολλαπλών επιπέδων και κρυπτογράφησης. Συμπερασματικά, η αντιμετώπισης μελλοντικών προκλήσεων και της ενίσχυσης των μέτρων ασφάλειας για τη διασφάλιση της ασφαλούς και ασφαλούς αποθήκευσης δεδομένων σε περιβάλλοντα υπολογιστικών νεφών είναι ζωτικής σημασίας.

Οι τρέχουσες προκλήσεις και απειλές αφορούν την ασφάλεια δεδομένων σε πλατφόρμες υπολογιστικών νεφών. Η ασφάλεια δεδομένων, τα οποία είναι αποθηκευμένα σε διακομιστές υπολογιστικού νέφους είναι πολύ σημαντική τόσο για τους οργανισμούς όσο και για τους προσωπικούς χρήστες. Οι κορυφαίες προκλήσεις είναι η διαρροή και οι παραβιάσεις δεδομένων,

εσφαλμένες ρυθμίσεις παραμέτρων, απειλές σχετικές με τη διαχείριση ταυτότητας και πρόσβασης η έλλειψη αρχιτεκτονικής ασφάλειας, η πειρατεία λογαριασμών, εσωτερικές απειλές και ανασφαλείς διεπαφές χρήστη ή διεπαφές προγραμματισμού εφαρμογής (Application Programming Interface – API) και επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS).

Αρκετοί ερευνητές έχουν προτείνει διάφορα πλαίσια και αρχιτεκτονικές, τα οποία στοχεύουν στην αντιμετώπιση αυτών των προκλήσεων, χρησιμοποιώντας μεθόδους όπως ο διαχωρισμός δεδομένων, ο έλεγχος ταυτότητας και οι τεχνικές κρυπτογράφησης. Αυτά τα πλαίσια στοχεύον στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα, τα οποία είναι αποθηκευμένα σε περιβάλλονται υπολογιστικών νεφών. Ακόμη, προστατεύουν από προηγμένς επιθέσις όπως είναι οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) και επιθέσεις man-in-the-middle.

Η μελλοντική έρευνα κρίνεται αναγκαίο να επικεντρωθεί στην αντιμετώπιση αυτών των προκλήσεων, έχοντας στόχο τον μετριασμό του αντικτύπου τους στις κυβερνήσεις, τους δημόσιους και ιδιωτικού οργανισμούς και τους χρήστες, με έμφαση στην ανάπτυξη ισχυρών στρατηγικών και αρχιτεκτονικών ασφαλείας. Παρόλο που αυτές οι μέθοδοι προσφέρουν βιώσιμες λύσεις για την προστασία δεδομένων, υπάρχει αυξανόμενη ανάγκη για συνεχή προσπάθεια έρευνας και ανάπτυξης για την ενίσχυση και βελτιστοποίηση πλαισίων και αρχιτεκτονικών της ασφάλειας δεδομένων και την προσαρμογή στις εξελισσόμενες απειλές και προκλήσεις σχετικά με την ασφάλεια και εισαγωγή τεχνικών αιχμής, οι οποίες διασφαλίζουν το απόρρητο, την αξιοπιστία και την ακεραιότητα των ευαίσθητων δεδομένων σε όλα τα σενάρια.

Βιβλιογραφικές Αναφορές

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, *14*(1), 11. https://doi.org/10.3390/fi14010011

Alenizi, B. A., Humayun, M., & Jhanjhi, N. (2021). Security and Privacy Issues in Cloud Computing. *Journal of Physics: Conference Series*, *1979*(1), 012038. https://doi.org/10.1088/1742-6596/1979/1/012038

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/access.2021.3073203

Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017). Cloud security ecosystem for data security and privacy. *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*. https://doi.org/10.1109/confluence.2017.7943164

AWS Marketplace Sponsors New E-book - SANS Practical Guide to Security in the AWS Cloud. (2020). https://www.prnewswire.com/news-releases/aws-marketplace-sponsors-new-e-book--sans-practical-guide-to-security-in-the-aws-cloud-301165403.html

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. *IEEE Access*, *8*, 23601–23623. https://doi.org/10.1109/access.2020.2968741

Bhansali, A. (2023). Cloud Security and Privacy. International Journal for Research in Applied Science and Engineering Technology, 11(8), 1539–1542. https://doi.org/10.22214/ijraset.2023.55416

Carrera, G. (2021). BUILDING A COMPREHENSIVE CLOUD SECURITY AUDIT PROGRAM. *EDPACS*, *66*(1), 15–18. https://doi.org/10.1080/07366981.2021.2004689

Cha, J., Singh, S. K., Kim, T. W., & Park, J. H. (2021). Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications*, *57*, 102686. https://doi.org/10.1016/j.jisa.2020.102686

Chen, L., Takabi, H., & Le-Khac, N. A. (2019). *Security, Privacy, and Digital Forensics in the Cloud*. John Wiley & Sons. http://books.google.ie/books?id=R5VPCwAAQBAJ&printsec=frontcover&dq=Security,+Privacy,+and+Digital+Forensics+in+the+Cloud&hl=&cd=1&source=gbs_api

Cloud Computing Tutorial. (n.d.). https://www.tutorialspoint.com/cloud_computing/index.htm

Cloud Computing Use Cases White Paper. (2010). Cloud Computing Use Case Discussion Group.

Cloud Cybersecurity Controls. (2020). National Cybersecurity Authority. https://nca.gov.sa/ccc-en.pdf

Cloud Security Best Practices. (n.d.). Ministry of Electronics & Information Technology, Government of India. https://www.meity.gov.in/writereaddata/files/WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

Cloud Security Technical Reference Architecture. CISA. (2022). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture

Djigal, H., Jun, F., & Lu, J. (2017). Secure Framework for Future Smart City. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. https://doi.org/10.1109/cscloud.2017.21

El Kafhali, S., El Mir, I., & Hanini, M. (2021). Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*, *29*(1), 223–246. https://doi.org/10.1007/s11831-021-09573-y

El Makkaoui, K., Ezzati, A., Beni-Hssane, A., & Motamed, C. (2016). Cloud security and privacy model for providing secure cloud services. *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*. https://doi.org/10.1109/cloudtech.2016.7847682

Giannakoulias, A. (2016). Cloud computing security: protecting cloud-based smart city applications. *Journal of Smart Cities*, *2*(1). https://doi.org/10.18063/jsc.2016.01.007

Gundu, S. R., Charanarur, P., Chandelkar, K. K., Samanta, D., Poonia, R. C., & Chakraborty, P. (2022). Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation. *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/4397610

Gutte, V. S., & Devulapalli, S. (2020). Achieving Cloud Security Using a Third Party Auditor and Preserving Privacy for Shared Data Over a Public Cloud. *International Journal of Knowledge and Systems Science*, *11*(1), 77–95. https://doi.org/10.4018/ijkss.2020010104

Jangjou, M., & Sohrabi, M. K. (2022). A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. *Archives of Computational Methods in Engineering*, *29*(6), 3587–3608. https://doi.org/10.1007/s11831-022-09708-9

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.sp.800-144

Kim, A. (2023). Cloud Security Foundations, Frameworks, and Beyond. *SANS Institute*. https://www.sans.org/white-papers/cloud-security-foundations-frameworks-beyond/

Krishnamoorthy, N., & Umarani, S. (2023). Implementation and management of cloud security for industry 4.O - data using hybrid elliptical curve cryptography. *The Journal of High Technology Management Research*, *34*(2), 100474. https://doi.org/10.1016/j.hitech.2023.100474

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002

Kumar, S. N., & Vajpayee, A. (2016). A Survey on Secure Cloud: Security and Privacy in Cloud Computing. *American Journal of Systems and Software*, *4*(1), 14-26. doi: 10.12691/ajss-4-1-2

Kunduru, A. R. (2023). Security Concerns and Solutions for Enterprise Cloud Computing Applications. *Asian Journal of Research in Computer Science*, *15*(4), 24–33. https://doi.org/10.9734/ajrcos/2023/v15i4327

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'REILLY. https://books.google.gr/books?id=BHazecOuDLYC

Mishra, B. S. P., Das, H., Dehuri, S., & Jagadev, A. K. (2018). Cloud Computing for Optimization: Foundations, Applications, and Challenges. Springer. Retrieved from: https://link.springer.com/book/10.1007/978-3-319-73676-1

Pandi (Jain), G. S., Shah, S., & Wandra, K. (2020). Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. *Procedia Computer Science*, *167*, 163–173. https://doi.org/10.1016/j.procs.2020.03.194

Pavithra, S., Ramya, S., & Prathibha, S. (2019). A Survey On Cloud Security Issues And Blockchain. *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*. https://doi.org/10.1109/iccct2.2019.8824891

Privacy and Security in Personal Data Clouds. (2017). ENISA. https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds

Rao, P. M., & Saraswathi, P. (2021). Evolving cloud security technologies for social networks. *Security in IoT Social Networks*, 179–203. https://doi.org/10.1016/b978-0-12-821599-9.00008-x

Riaz, S., Khan, A. H., Haroon, M., Latif, S., & Bhatti, S. (2020). Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment. *2020*

International Conference on Information Management and Technology (ICIMTech). https://doi.org/10.1109/icimtech50083.2020.9211239

Security and Resilience in Governmental Clouds. (2011). ENISA. https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds

Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. (2017). CSA. Retrieved from: https://cloudsecurityalliance.org/artifacts/security-guidance-v4

Smys, S., Palanisamy, R., Rocha, L., & Beligiannis, G. N. (2021). *Computer Networks and Inventive Communication Technologies*. Springer Nature. https://doi.org/10.1007/978-981-15-9647-6

Soveizi, N., Turkmen, F., & Karastoyanova, D. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184–200. https://doi.org/10.1016/j.future.2023.05.015

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642. https://doi.org/10.1016/j.jnca.2020.102642

Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access*, *7*, 147420–147452. https://doi.org/10.1109/access.2019.2946185

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., & Kim, K. I. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics*, *10*(15), 1811. https://doi.org/10.3390/electronics10151811

THE WHITE BOOK OF... Cloud Security The definitive guide to managing risk in the new ICT landscape. (2011). Fujitsu. https://www.fujitsu.com/sg/imagesgig5/white-book-of-cloud-security.pdf

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/access.2020.3009876

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids*. https://doi.org/10.1109/skg.2010.19