Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπηρεσιών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Διπλωματική Εργασία

Ασφάλεια και ιδιωτικότητα σε περιβάλλον Νεφοϋπολογιστικής

Φοιτήτρια : Δήμητρα Κλειδαρά

ΑΜ: cscyb21012

Επιβλέπων Καθηγητής

Δρ. Παναγιώτης Ηρ. Γιαννακόπουλος

Αιγάλεω, Αύγουστος 2023

Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπηρεσιών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Ασφάλεια και ιδιωτικότητα σε περιβάλλον Νεφοϋπολογιστικής

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ-ΕΠΩΝΥΜΟ	ΥΠΟΓΡΑΦΗ
1	Δρ. Παναγιώτης Γιαννακόπουλος	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.24 08:07:04 +03'00'
2	Δρ. Κωνσταντίνος Μαυρομμάτης	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2023.08.25 14:52:13 +03'00'
3	Δρ. Δημήτρης Κόγιας	

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη **ΔΗΜΗΤΡΑ ΚΛΕΙΔΑΡΑ** του **ΣΩΤΗΡΙΟΥ** με αριθμό μητρώου **cscyb21012,** φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφάλειας του **ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ** της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος **ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ,**

Δηλώνω υπεύθυνα ότι:

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

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

Η Δηλούσα

ΔΗΜΗΤΡΑ ΚΛΕΙΔΑΡΑ του **ΣΩΤΗΡΙΟΥ**

Συντομεύσεις - Ακρωνύμια	
AI	Artificial intelligence
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interfaces
AWS	Amazon Web Services
CICA	Canadian Institute of Chartered Accountants
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DDoS	Distributed denial-of-service
GAPP	Generally Accepted Principles and Practices
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection Systems
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
ML	Machine Learning
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a service
PIN	Personal identification number
PIPA	Personal Information Protection Act
REST	Representational State Transfer
SaaS	Software as a service
SIEM	Security Information and Event Management
SMS	Short Message Service
SOA	Service-oriented architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VM	Virtual Machine

Περίληψη

Η παρούσα εργασία επικεντρώνεται στην ανάλυση της ασφάλειας και της ιδιωτικότητας στο υπολογιστικό νέφος και τις τεχνικές προστασίας που χρησιμοποιούνται για την αντιμετώπιση των απειλών και επιθέσεων.

Γίνεται αναφορά στο υπολογιστικό νέφος και στις διάφορες υπηρεσίες που προσφέρει. Αναφέρονται οι βασικές έννοιες και οι σημαντικότεροι τύποι υπολογιστικού νέφους, που είναι το δημόσιο, ιδιωτικό και υβριδικό νέφος, ενώ παρουσιάζονται τα μοντέλα υπηρεσιών IaaS, PaaS και SaaS. Δίνεται μεγάλη έμφαση στην ασφάλεια και την προστασία των προσωπικών δεδομένων στο cloud. Εξετάζονται οι προκλήσεις και οι απειλές που παρουσιάζονται, ενώ αναλύονται οι τεχνικές προστασίας για την αντιμετώπιση τους. Η έννοια της ιδιωτικότητας στις cloud υπηρεσίες αναλύεται επίσης, καθώς και οι προκλήσεις που έχουν προκύψει, και παρουσιάζονται σχετικές τεχνικές προστασίας, όπως η ανωνυμοποίηση δεδομένων, ο περιορισμός πρόσβασης και η προστασία από Account Hijacking. Τέλος, αναλύεται το τρέχων νομοθετικό πλαίσιο, με έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης.

Στο τέλος της εργασίας, παρουσιάζονται τα συμπεράσματα της έρευνας και των αποτελεσμάτων, ενώ γίνεται συνολική αξιολόγηση των προκλήσεων και των λύσεων που μπορούν να εφαρμοστούν για τη βελτίωση της ασφάλειας και της ιδιωτικότητας στο cloud.

Abstract

This paper focuses on the analysis of security and privacy in cloud computing and the protective techniques used to address threats and attacks.

It references cloud computing and its various services, highlighting fundamental concepts and key cloud computing types: public, private, and hybrid clouds. It also presents the models of IaaS, PaaS, and SaaS services. The paper places significant emphasis on security and the safeguarding of personal data in the cloud. It examines the challenges and threats that arise, while analyzing protective techniques to counter them. The notion of privacy in cloud services is also explored, along with emerging challenges, and relevant protective techniques such as data anonymization, access restriction, and protection against Account Hijacking are presented.

Lastly, the current legislative framework is analyzed, with a focus on the General Data Protection Regulation (GDPR) of the European Union. The paper concludes by presenting research findings and conclusions, providing an overall evaluation of challenges and potential solutions that can be implemented to enhance security and privacy in the cloud.

Πίνακας Περιεχομένων

Κεφάλαιο 1 – Εισαγωγή

1.1 Εισαγωγή στο βασικό θέμα της εργασίας

Το υπολογιστικό νέφος, γνωστό και ως cloud computing, αναφέρεται σε ένα μοντέλο υπηρεσιών πληροφορικής που παρέχει πρόσβαση σε κοινόχρηστους υπολογιστικούς πόρους μέσω του Διαδικτύου.

Τα ζητήματα ασφάλειας και ιδιωτικότητας στο υπολογιστικό νέφος (cloud computing) είναι υψίστης σημασίας λόγω του μεγάλου όγκου δεδομένων που αποθηκεύονται και ανταλλάσσονται. Οι χρήστες αποθηκεύουν, επεξεργάζονται και μεταφέρουν τα δεδομένα τους στο υπολογιστικό νέφος, επομένως είναι αναμενόμενο να έρθουν αντιμέτωποι με προκλήσεις που αφορούν στην ασφάλεια και στην ιδιωτικότητα των δεδομένων τους. Ορισμένα από τα βασικά ζητήματα περιλαμβάνουν:

- Απομακρυσμένη αποθήκευση δεδομένων: Οι χρήστες αποθηκεύουν τα δεδομένα τους σε απομακρυσμένους διακομιστές του υπολογιστικού νέφους. Αυτό απαιτεί μέτρα ασφαλείας για την προστασία των δεδομένων από απώλεια, κλοπή ή μη εξουσιοδοτημένη πρόσβαση.

- Εξουσιοδότηση και πρόσβαση: Οι πάροχοι cloud πρέπει να διαχειρίζονται την εξουσιοδότηση των χρηστών και τον έλεγχο της πρόσβασης στους πόρους του νέφους. Αυτό απαιτεί να ληφθούν μέτρα για την ταυτοποίηση και την αυθεντικοποίηση των χρηστών, καθώς και τον έλεγχο των δικαιωμάτων πρόσβασης σε επίπεδο χρήστη.

- Απομονωμένο περιβάλλον: Οι χρήστες μοιράζονται την ίδια υποδομή με άλλους χρήστες στο υπολογιστικό νέφος. Αυτό επιβάλλει την ανάγκη να διατηρείται απομόνωση και ασφάλεια μεταξύ των διάφορων χρηστών, ώστε να αποτραπεί η δυνατότητα παραβίασης ή κατάχρησης των δεδομένων.

- Κρυπτογράφηση δεδομένων: Η κρυπτογράφηση είναι σημαντική για την προστασία του απορρήτου της πληροφορίας. Οι χρήστες μπορούν να χρησιμοποιήσουν μηχανισμούς κρυπτογράφησης για την προστασία των δεδομένων τους κατά τη μετάδοση και την αποθήκευσή τους στο υπολογιστικό νέφος.

- Επιθέσεις και παραβιάσεις: Το υπολογιστικό νέφος είναι ευάλωτο σε επιθέσεις και παραβιάσεις ασφάλειας. Οι παρόχοι cloud πρέπει να λαμβάνουν μέτρα για την ανίχνευση, τον περιορισμό και την αντιμετώπιση των επιθέσεων, καθώς και για την αποκατάσταση των συστημάτων σε περίπτωση παραβίασης.

- Νομικά ζητήματα και συμμόρφωση: Η αποθήκευση και η επεξεργασία δεδομένων στο υπολογιστικό νέφος ενέχει νομικά ζητήματα, όπως ο σεβασμός των προτύπων ασφάλειας και ιδιωτικότητας, η συμμόρφωση με τους κανονισμούς περί προστασίας δεδομένων και η διαχείριση της ευθύνης για την προστασία των δεδομένων των χρηστών.

Οι παραπάνω προκλήσεις και ζητήματα απαιτούν την ύπαρξη κατάλληλων τεχνικών, διαδικασιών και πολιτικών για την ασφάλεια και την ιδιωτικότητα στο υπολογιστικό νέφος. Οι πάροχοι cloud και οι χρήστες οφείλουν να συνεργαστούν προκειμένου να αντιμετωπίσουν αυτές τις προκλήσεις και να εξασφαλίσουν ένα ασφαλές και ιδιωτικό περιβάλλον στο υπολογιστικό νέφος.

1.2 Στόχος της εργασίας και ερευνητικά ερωτήματα

Βασικός σκοπός της παρούσας εργασίας είναι η καταγραφή και η παρουσίαση των βασικών ζητημάτων ασφαλείας και ιδιωτικότητας των δεδομένων στο υπολογιστικό νέφος καθώς και η αναφορά των διαθέσιμων μηχανισμών και τεχνικών αντιμετώπισης αυτών των ζητημάτων. Από τα παραπάνω, η εργασία αυτή καλείται να απαντήσει στα παρακάτω ερευνητικά ερωτήματα:

- Ανάλυση των απειλών και επιθέσεων στο cloud: Ποιες είναι οι κύριες απειλές και επιθέσεις που παρατηρούνται στον τομέα του cloud computing; Πώς επηρεάζουν την ασφάλεια των δεδομένων και την ιδιωτικότητα των χρηστών;
- Ανάλυση των επιπτώσεων απειλών και επιθέσεων: Ποιες είναι οι επιπτώσεις που μπορεί να έχουν οι απειλές και επιθέσεις στην ασφάλεια και ιδιωτικότητα των δεδομένων στο cloud; Πώς επηρεάζονται οι χρήστες και οι οργανισμοί που αξιοποιούν υπηρεσίες cloud;
- Αξιολόγηση των τεχνικών μεθόδων προστασίας: Ποιες τεχνικές μέθοδοι χρησιμοποιούνται για την προστασία απειλών και επιθέσεων στο cloud; Πώς λειτουργούν αυτές οι μέθοδοι και με ποιο τρόπο διασφαλίζεται η ασφάλεια και η ιδιωτικότητα;
- Ανάπτυξη νέων τεχνικών προστασίας: Ποιες είναι οι προηγμένες τεχνικές προστασίας που μπορούν να αναπτυχθούν για την αντιμετώπιση των απειλών και επιθέσεων στο cloud; Πώς μπορούν αυτές οι τεχνικές να βελτιώσουν την ασφάλεια και ιδιωτικότητα των δεδομένων;
- Αξιολόγηση νομοθεσίας και πολιτικών προστασίας: Πώς επηρεάζει η υφιστάμενη νομοθεσία την προστασία απειλών, επιθέσεων και ιδιωτικότητας στο cloud; Ποιες πολιτικές προστασίας μπορούν να εφαρμοστούν για την ενίσχυση της ασφάλειας και ιδιωτικότητας στον τομέα αυτό;

Κεφάλαιο 2 – Υπολογιστικό νέφος και υπηρεσίες

2.1 Τί είναι το υπολογιστικό νέφος

Το cloud computing είναι μια τεχνολογία που επιτρέπει στους χρήστες να αποθηκεύουν και να προσπελάζουν δεδομένα και εφαρμογές μέσω του Διαδικτύου. Χρησιμοποιώντας τις υπηρεσίες του cloud, οι χρήστες έχουν τη δυνατότητα να διαχειρίζονται και να εκτελούν τις εφαρμογές τους σε απομακρυσμένους

διακομιστές και να πάψουν να αποθηκεύουν τα δεδομένα ή να εκτελούν τις εφαρμογές τους σε τοπικούς υπολογιστές ή σε εσωτερικά δίκτυα.

Οι υπηρεσίες cloud computing προσφέρουν πολλά πλεονεκτήματα. Αρχικά, επιτρέπουν στους χρήστες να έχουν πρόσβαση στα δεδομένα και τις εφαρμογές τους από οπουδήποτε στο κόσμο και από οποιαδήποτε συσκευή που μπορεί να συνδεθεί στο Διαδίκτυο. Επιπλέον, παρέχουν δυνατότητα κλιμάκωσης, καθώς οι πόροι του cloud μπορούν να αυξομειωθούν ανάλογα με τις ανάγκες του χρήστη. Τέλος, παρέχουν στο χρήστη τη δυνατότητα να δημιουργήσει και αποθηκεύσει αντίγραφα ασφάλειας των πληροφοριών του, μειώνοντας έτσι τον κίνδυνο απώλειας δεδομένων λόγω βλάβης του εξοπλισμού.

Οι υπηρεσίες cloud computing χωρίζονται σε τρεις βασικές κατηγορίες:

- Υποδομή ως Υπηρεσία - Infrastructure as a Service (IaaS), ένα μοντέλο υπηρεσίας που παρέχει πρόσβαση σε υπολογιστικούς πόρους όπως για παράδειγμα διακομιστές, αποθηκευτικό χώρο, δίκτυο ή εικονοποίηση.
- Πλατφόρμα ως Υπηρεσία - Platform as a Service (PaaS), μια κατηγορία υπηρεσιών υπολογιστικού νέφους που περιλαμβάνει οτιδήποτε μπορεί να χρειαστεί ένας προγραμματιστής για να δημιουργήσει, να τρέξει και να χειριστεί εφαρμογές. Αυτό το περιβάλλον ανάπτυξης μπορεί να περιλαμβάνει γλώσσες προγραμματισμού, εργαλεία και βιβλιοθήκες.
- Λογισμικό ως Υπηρεσία - Software as a Service (SaaS), όπου οι χρήστες μπορούν να αποκτήσουν και να χρησιμοποιήσουν λογισμικό ως συνδρομητική υπηρεσία γλιτώνοντας έτσι τα κόστη αγοράς.

Γενικά, το cloud computing έχει επανασχεδιάσει τον τρόπο που αποθηκεύουμε, διαχειριζόμαστε και χρησιμοποιούμε τα δεδομένα και τις εφαρμογές μας. Παρέχει ευελιξία, ασφάλεια και πρόσβαση από οπουδήποτε, επιτρέποντας σε επιχειρήσεις και χρήστες να εκμεταλλευτούν τις δυνατότητες του Διαδικτύου για την αποτελεσματική διαχείριση και αξιοποίηση των πόρων τους.

2.2 Ιστορική αναδρομή

Για το cloud computing ως έννοια και ως τεχνολογία δεν μπορεί να οριστεί ένα συγκεκριμένο σημείο εκκίνησης. Ωστόσο, μπορούμε να παρατηρήσουμε την εξέλιξή του στα πλαίσια της ανάπτυξης του υπολογιστικού και διαδικτυακού τομέα.

Τη δεκαετία του 1950, οι μεγάλοι υπολογιστές τύπου mainframe χρησιμοποιούνταν για να παρέχουν κοινόχρηστους υπολογιστικούς πόρους σε διάφορους χρήστες μέσω του δικτύου. Αυτή η ιδέα της κοινόχρηστης πρόσβασης σε απομακρυσμένους υπολογιστικούς πόρους αποτέλεσε μια πρώιμη μορφή του cloud computing. Στη δεκαετία του 1960, η ιδέα της δημιουργίας μιας "παγκόσμιας υπολογιστικής υπηρεσίας" εμφανίστηκε χάρη στην διορατικότητα του πρωτοπόρου Joseph Licklider. Ο Licklider προέβλεπε ένα συστηματικά συνδεδεμένο δίκτυο υπολογιστών που θα μπορούσε να παρέχει πρόσβαση σε υπολογιστικούς πόρους από οπουδήποτε στον κόσμο. Αν και η τεχνολογία της εποχής δεν ήταν ακόμη έτοιμη να υποστηρίξει πλήρως αυτήν την ιδέα, η

πρωτοποριακή του σκέψη συνέβαλε στην ανάπτυξη του cloud computing όπως το γνωρίζουμε σήμερα. Τη δεκαετία του 1990, ο όρος "cloud computing" άρχισε να εμφανίζεται, αναφερόμενος στην ιδέα της απομακρυσμένης πρόσβασης σε υπηρεσίες και πόρους μέσω του Διαδικτύου. Επίσης, η επικράτηση του Διαδικτύου και η ανάπτυξη των εικονικών μηχανών (virtual machines) συνέβαλαν στην περαιτέρω εξέλιξη του cloud computing. Στα μέσα της δεκαετίας του 2000, η Amazon εισήγαγε το Amazon Web Services (AWS), το οποίο αποτελεί μια πλατφόρμα υπολογισμού στο cloud. Αυτή η εισαγωγή έδωσε τη δυνατότητα στις επιχειρήσεις και στους προγραμματιστές να αξιοποιήσουν τους υπολογιστικούς πόρους της Amazon για την ανάπτυξη και την εκτέλεση εφαρμογών. Στη συνέχεια, η Microsoft και η Google ακολούθησαν με τις αντίστοιχες πλατφόρμες τους, το Microsoft Azure και το Google Cloud Platform αντίστοιχα. Από τότε, το cloud computing συνεχίζει να αναπτύσσεται και να εξελίσσεται με ταχείς ρυθμούς. Οι πάροχοι cloud προσφέρουν πλέον μια τεράστια γκάμα υπηρεσιών, συμπεριλαμβανομένων υπηρεσιών υποδομής ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS) και λογισμικο ως υπηρεσία (SaaS). Η τεχνολογία του cloud computing έχει αλλάξει τον τρόπο με τον οποίο οι επιχειρήσεις διαχειρίζονται τους υπολογιστικούς τους πόρους, προσφέροντας ευελιξία, δυνατότητα κλιμάκωσης και εξοικονόμηση πόρων.

Την τελευταία δεκαετία, το cloud computing έχει καταλάβει μια σημαντική θέση στην βιομηχανία της τεχνολογίας. Οι μεγαλύτεροι πάροχοι τέτοιων υπηρεσιών, όπως είναι η Amazon, η Microsoft και η Google, έχουν αναπτύξει δυναμικές πλατφόρμες νέφους που παρέχουν μια ευρεία γκάμα υπηρεσιών και λειτουργιών σε επιχειρήσεις άλλα και σε ιδιώτες. Τα τελευταία χρόνια η εξέλιξη που έχει παρατηρηθεί στον τομέα του cloud computing είναι αξιοσημείωτη. Οι τεχνολογίες και οι υπηρεσίες του cloud έχουν αναπτυχθεί και βελτιωθεί σε πολλούς τομείς. Ορισμένες από τις σημαντικότερες εξελίξεις περιλαμβάνουν μεταξύ άλλων τα παρακάτω:

1. Υπολογιστική ισχύς και δυνατότητα κλιμάκωσης: Οι πάροχοι cloud έχουν αυξήσει την υπολογιστική ισχύ των υπηρεσιών τους, επιτρέποντας στους χρήστες να εκτελούν ακόμη πιο απαιτητικές εφαρμογές. Επίσης, η δυνατότητα κλιμάκωσης έχει βελτιωθεί, δίνοντας τη δυνατότητα να αυξάνονται ή να μειώνονται οι πόροι ανάλογα με τις εκάστοτε ανάγκες των χρηστών.

2. Τεχνητή νοημοσύνη και μηχανική μάθηση: Οι πάροχοι cloud έχουν ενσωματώσει δυνατότητες τεχνητής νοημοσύνης (Artificial Intelligence – AI) και μηχανικής μάθησης (Machine Learning – ML) στις υπηρεσίες τους. Αυτό επιτρέπει την ανάπτυξη και την εκτέλεση προηγμένων εφαρμογών που βασίζονται σε αλγόριθμους μηχανικής μάθησης, όπως αναγνώριση εικόνας και φωνής, αυτόματη μετάφραση και προβλέψη δεδομένων.

3. Διαχείριση δεδομένων και εργαλεία ανάλυσης: Οι πάροχοι cloud έχουν εισαγάγει μια πληθώρα υπηρεσιών για τη διαχείριση και ανάλυση δεδομένων. Αυτές οι υπηρεσίες παρέχουν ευέλικτες βάσεις δεδομένων, εργαλεία ανάλυσης δεδομένων και υπηρεσίες business intelligence που επιτρέπουν στις επιχειρήσεις να αξιοποιήσουν τα δεδομένα τους για βελτιστοποιημένη λήψη αποφάσεων και πρόβλεψη των μελλοντικών τάσεων.

4. Ασφάλεια και προστασία δεδομένων: Έχει δοθεί μεγάλη έμφαση στην ασφάλεια και την προστασία των δεδομένων στον χώρο του cloud computing. Οι πάροχοι cloud έχουν εφαρμόσει προηγμένες τεχνικές κρυπτογράφησης, μηχανισμούς πρόληψης απώλειας δεδομένων και συστήματα ανίχνευσης απειλών για να διασφαλίσουν την ασφάλεια των πληροφοριών που αποθηκεύονται, μεταδίδονται και επεξεργάζονται στο cloud.

2.3 Βασικές έννοιες

Service-Oriented Architecture (SOA)

Το Service-Oriented Architecture (SOA) είναι ένα αρχιτεκτονικό πρότυπο λογισμικού που βασίζεται στην ιδέα της οργάνωσης και παροχής λειτουργιών ως υπηρεσίες. Στο πλαίσιο του SOA, οι λειτουργίες ενός συστήματος λογισμικού παρέχονται ως ανεξάρτητες υπηρεσίες που μπορούν να ανακληθούν και να συνδυαστούν ώστε να δημιουργήσουν όλο και πιο πολύπλοκες εφαρμογές.

Σύμφωνα με την αρχιτεκτονική SOA, οι υπηρεσίες αντιπροσωπεύουν συγκεκριμένες λειτουργίες που μπορούν να εκτελεστούν από ένα μέρος λογισμικού. Πρόκειται για υπηρεσίες που είναι αυτόνομες, και η πρόσβαση σε αυτές γίνεται μέσω πρωτοκόλλων δικτύου, παρέχοντας τη δυνατότητα να ανακληθούν από άλλες εφαρμογές ή υπηρεσίες. Αυτή η προσέγγιση επιτρέπει την ανακατανομή και την επαναχρησιμοποίηση των λειτουργιών, προωθώντας έτσι την ευελιξία και την ανεξαρτησία μεταξύ των εφαρμογών.

Οι υπηρεσίες στο πλαίσιο του SOA συνδέονται μεταξύ τους μέσω προτύπων δια λειτουργικότητας, όπως είναι το SOAP (Simple Object Access Protocol) ή το REST (Representational State Transfer). Αυτά τα πρωτόκολλα επιτρέπουν την ανταλλαγή μηνυμάτων και την επικοινωνία μεταξύ των υπηρεσιών. Ένα σημαντικό πλεονέκτημα του SOA είναι η δυνατότητα επαναχρησιμοποίησης των υπηρεσιών. Κάθε υπηρεσία μπορεί να χρησιμοποιηθεί από πολλές εφαρμογές και να συνδυαστεί με άλλες υπηρεσίες για τη δημιουργία νέων λειτουργιών. Αυτό μειώνει τον κώδικα που πρέπει να αναπτυχθεί, ενώ παράλληλα αυξάνει την αποδοτικότητα και επιτρέπει την ευελιξία στην ανάπτυξη και τη συντήρηση των συστημάτων λογισμικού.

2.4 Τύποι υπολογιστικού νέφους

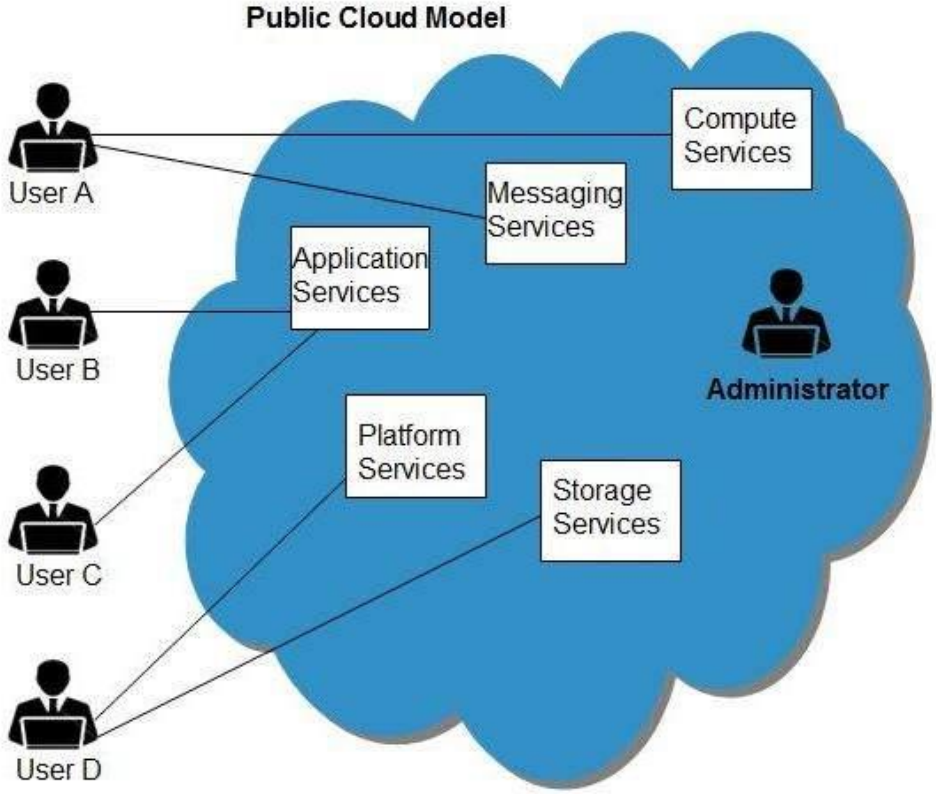
Οι τύποι του cloud αναφέρονται στις διάφορες μορφές οργάνωσης και παροχής υπηρεσιών cloud computing. Οι τρεις βασικοί τύποι του cloud είναι το δημόσιο νέφος (Public Cloud), το ιδιωτικό νέφος (Private Cloud) και τέλος το υβριδικό νέφος (Hybrid Cloud) τα οποία θα αναλυθούν παρακάτω.

2.4.1 Δημόσιο νέφος

Το Public Cloud ανακατεύθυνε τον τρόπο με τον οποίο οι επιχειρήσεις και οι οργανισμοί αξιοποιούν και διαχειρίζονται τις υπολογιστικές τους ανάγκες. Αναπτύχθηκε ως μια πρωτοποριακή λύση που παρέχει πρόσβαση σε υπηρεσίες υπολογιστικού νέφους μέσω του διαδικτύου, και αποτελεί μια επιλογή που παρέχει

ευελιξία για την αποθήκευση δεδομένων, την εκτέλεση εφαρμογών και την ανάπτυξη λογισμικού. Παρακάτω θα εξεταστούν και θα αναλυθούν τα βασικά χαρακτηριστικά του Public Cloud, τα οφέλη του και ο τρόπος με τον οποίο έχει επανασχεδιάσει τον κόσμο της τεχνολογίας και της επιχειρηματικότητας.

Το Public Cloud είναι ο πιο συνηθισμένος τύπος νέφους. Οι πόροι του cloud όπως είναι για παράδειγμα οι διακομιστές και ο αποθηκευτικός χώρος ανήκουν στους παρόχους του cloud και διαχειρίζονται από αυτούς, ενώ παραδίδονται στους χρήστες μέσω του διαδικτύου. Οι πάροχοι αυτοί διατίθενται να παρέχουν αποθήκευση, υπολογιστική ισχύ και άλλες υπηρεσίες, απελευθερώνοντας τις επιχειρήσεις από το βάρος της φυσικής υποδομής και παρέχοντας τη δυνατότητα να αποκτήσουν πρόσβαση σε αυτές τις υπηρεσίες κατά απαίτηση (on demand). Το δημόσιο νέφος χρησιμοποιείται πιο συχνά για παροχή διαδικτυακού ηλεκτρονικού ταχυδρομείου (e-mail), διαδικτυακών εφαρμογών γραφείου (office), αποθήκευσης και για περιβάλλοντα ανάπτυξης και δοκιμής (testing and development environments).



Εικόνα 1- *Δημόσιο Υπολογιστικό Νέφος*

Ένα από τα κύρια οφέλη του Public Cloud είναι η ευελιξία του. Οι χρήστες μπορούν να αυξομειώσουν τις απαιτήσεις τους για υπολογιστική ισχύ και αποθήκευση ανάλογα με τις επιχειρησιακές ανάγκες τους, πληρώνοντας έτσι μόνο για τους πόρους που χρησιμοποιούν. Με αυτό το τρόπο δεν είναι απαραίτητο να αγοράσουν περιττό εξοπλισμό και λογισμικό. Αυτό επιτρέπει στις επιχειρήσεις να αποφύγουν τον περιορισμό της φυσικής υποδομής και να αντιμετωπίσουν απρόβλεπτες αυξήσεις ή μειώσεις στη ζήτηση των υπηρεσιών τους.

Ένα άλλο σημαντικό οφέλος είναι η κλιμακούμενη φύση του Public Cloud. Οι πάροχοι του Cloud μπορούν να παρέχουν αμέτρητους πόρους υπολογιστικής ισχύος, επιτρέποντας στις επιχειρήσεις να αναπτύσσονται χωρίς περιορισμούς. Ανεξάρτητα από το μέγεθος ή τον τύπο της επιχείρησης, το Public Cloud παρέχει τη δυνατότητα κλιμάκωσης προς τα πάνω ή προς τα κάτω, ανάλογα με τις ανάγκες.

Ένα ακόμη σημαντικό στοιχείο του Public Cloud είναι η διαθεσιμότητα και η πρόσβαση σε παγκόσμιο επίπεδο. Οι επιχειρήσεις μπορούν να αποκτήσουν πρόσβαση σε υπηρεσίες Cloud από οπουδήποτε στον κόσμο, αρκεί να έχουν σύνδεση στο διαδίκτυο. Επίσης προσφέρει υψηλή αξιοπιστία, μιας και το τεράστιο δίκτυο διακομιστών που διαθέτει διασφαλίζει πως δε πρόκειται να υπάρξει αποτυχία σύνδεσης. Αυτό απλοποιεί την παγκόσμια συνεργασία, την ανάπτυξη και την επέκταση των επιχειρήσεων σε διεθνές επίπεδο.

Το Public Cloud έχει επανασχεδιάσει τον κόσμο της τεχνολογίας και της επιχειρηματικότητας. Έχει επιτρέψει την εμφάνιση νέων μοντέλων επιχειρηματικής δραστηριότητας, όπως η επιχειρηματικότητα ως υπηρεσία (Entrepreneurship as a Service) και η ανάπτυξη λογισμικού με μοντέλα συνεχούς παράδοσης (continuous delivery). Το Public Cloud διευκολύνει ακόμα την καινοτομία, καθώς παρέχει ένα ευέλικτο περιβάλλον για την ανάπτυξη και τη δοκιμή νέων ιδεών χωρίς να υπάρχει ανάγκη αγοράς ακριβών πόρων.

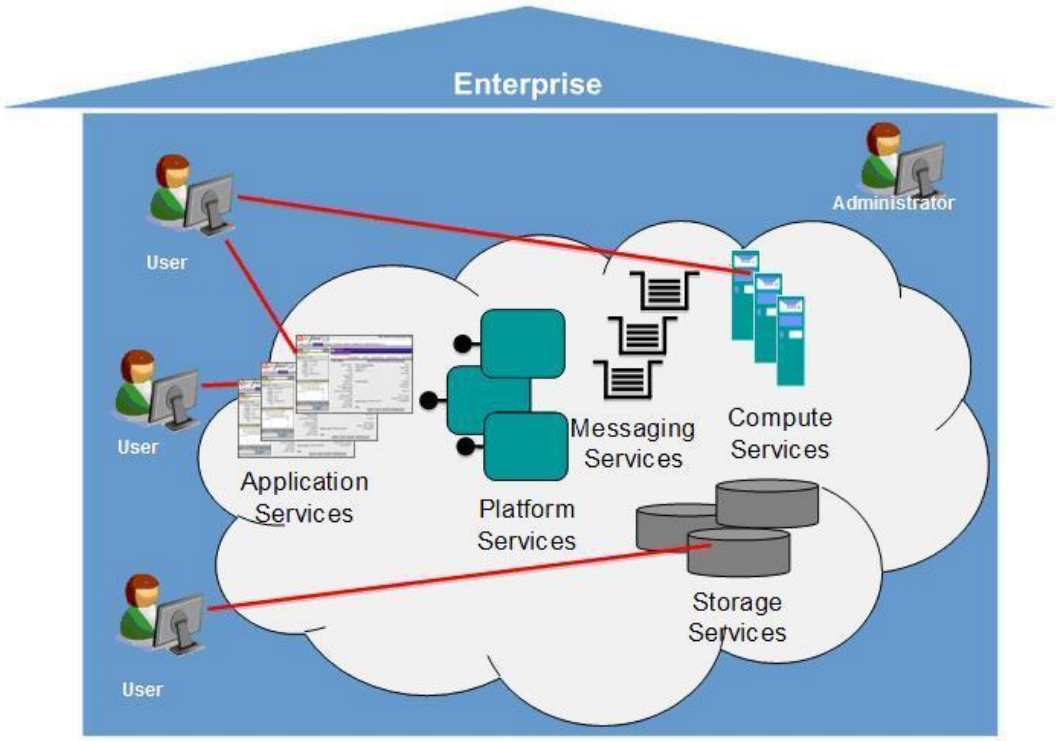
Το δημόσιο νέφος αντιπροσωπεύει μια επαναστατική τεχνολογία που έχει αλλάξει τον τρόπο με τον οποίο οι επιχειρήσεις και οι οργανισμοί αξιοποιούν και διαχειρίζονται τις υπολογιστικές τους ανάγκες. Με την ευελιξία, τη δυνατότητα κλιμάκωσης και τη διαθεσιμότητα σε παγκόσμιο επίπεδο, το Public Cloud προσφέρει στις επιχειρήσεις την απαραίτητη υποδομή για την καινοτομία, την ευελιξία και την επιτυχημένη ανάπτυξη των επιχειρήσεών τους. Είναι μια ισχυρή δύναμη που συνεχίζει να εξελίσσεται και να επαναπροσδιορίζει τον τρόπο με τον οποίο λειτουργούν οι επιχειρήσεις σήμερα.

2.4.2 Ιδιωτικό νέφος

Το Private Cloud αναπτύχθηκε ως μια εναλλακτική λύση στο Public Cloud, παρέχοντας ευελιξία, αυτονομία και καλύτερο έλεγχο στις επιχειρήσεις και τους οργανισμούς για τη διαχείριση των υπολογιστικών τους αναγκών. Παρακάτω θα εξεταστούν τα βασικά χαρακτηριστικά του Private Cloud, τα οφέλη του και ο τρόπος με τον οποίο προσφέρει ασφάλεια, έλεγχο και ευελιξία στους οργανισμούς.

Το Private Cloud αναφέρεται σε μια υποδομή υπολογιστικού νέφους που αποκτάται, διαχειρίζεται και χρησιμοποιείται αποκλειστικά από μια συγκεκριμένη επιχείρηση ή οργανισμό. Αντίθετα με το Public Cloud, το Private Cloud μπορεί να λειτουργεί εντός του φυσικού χώρου μιας επιχείρησης και να προσφέρει έτσι ένα επίπεδο ιδιωτικότητας, ασφάλειας και καλύτερου ελέγχου που απαιτείται για τα ευαίσθητα δεδομένα και εφαρμογές. Αν μια επιχείρηση δεν επιθυμεί να χρησιμοποιεί υπηρεσίες ιδιωτικού νέφους στο δικό της datacenter, υπάρχει δυνατότητα να φιλοξενηθεί από έναν τρίτο πάροχο υπηρεσιών. Σε κάθε περίπτωση, οι υπηρεσίες και η υποδομή όταν πρόκειται για ιδιωτικό νέφος διατηρούνται πάντα σε ένα ιδιωτικό δίκτυο και το λογισμικό είναι αφιερωμένο εξ ολοκλήρου στο συγκεκριμένο οργανισμό ή επιχείρηση.

Ένα από τα βασικά χαρακτηριστικά του Private Cloud είναι ο αποκλειστικός έλεγχος και ιδιωτικότητα που παρέχει. Η επιχείρηση ή ο οργανισμός διαχειρίζεται και ελέγχει όλα τα στοιχεία του Private Cloud, συμπεριλαμβανομένης της υποδομής, των δικτύων και των δεδομένων. Αυτό επιτρέπει στην επιχείρηση να προσαρμόσει το Private Cloud σύμφωνα με τις ανάγκες και τις απαιτήσεις της, διασφαλίζοντας την ευελιξία και την αποτελεσματικότητα των επιχειρησιακών της διαδικασιών.



***Εικόνα 2**- Private cloud*

Ένα άλλο σημαντικό πλεονέκτημα του Private Cloud είναι η ασφάλεια. Εφόσον ολόκληρο το υπολογιστικό περιβάλλον ελέγχεται εσωτερικά και οι πόροι δε μοιράζονται με άλλους, οι επιχειρήσεις μπορούν να εφαρμόσουν προηγμένα μέτρα ασφαλείας και πολιτικές πρόσβασης για την προστασία των δεδομένων τους. Αυτό είναι ιδιαίτερα σημαντικό για επιχειρήσεις που λειτουργούν σε ευαίσθητους τομείς ή κρίσιμες υποδομές, όπως οι χρηματοοικονομικές υπηρεσίες ή η υγειονομική περίθαλψη, όπου η προστασία των δεδομένων και η συμμόρφωση με τους κανονισμούς και τη νομοθεσία αποτελούν μέγιστη προτεραιότητα.

Το ιδιωτικό νέφος ακόμη προσφέρει ευελιξία στις επιχειρήσεις, καθώς μπορούν να προσαρμόσουν τους πόρους τους σύμφωνα με τις μεταβαλλόμενες ανάγκες τους. Αυτό σημαίνει ότι μπορούν να αυξήσουν ή να μειώσουν τους υπολογιστικούς πόρους, τον αποθηκευτικό χώρο και την επεξεργαστική ισχύ ανάλογα με τις εκάστοτε ανάγκες τους, χωρίς να εξαρτώνται από εξωτερικούς παρόχους υπηρεσιών.

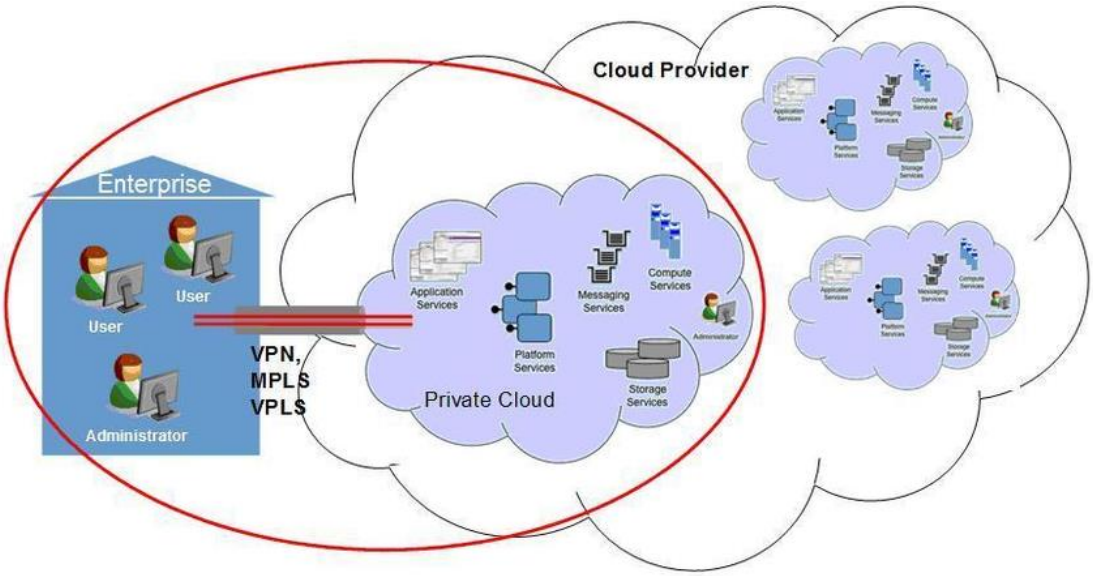
Το Private Cloud αποτελεί μια επιλογή που προσφέρει στις επιχειρήσεις ένα απόρρητο, ελεγχόμενο και προσαρμόσιμο υπολογιστικό περιβάλλον. Με την ασφάλεια, τον έλεγχο και την ευελιξία που παρέχει, οι επιχειρήσεις μπορούν να διαχειριστούν τις υπολογιστικές τους ανάγκες αποτελεσματικά και να προσαρμόσουν το υπολογιστικό περιβάλλον στις απαιτήσεις τους. Είναι μια επιλογή κατάλληλη για επιχειρήσεις που

αναζητούν τον έλεγχο και την ιδιωτικότητα των δεδομένων τους, καθώς και την ευελιξία και την προσαρμοστικότητα στο υπολογιστικό τους περιβάλλον.

2.4.3 Υβριδικό νέφος

Το Hybrid Cloud αντιπροσωπεύει μια εξέλιξη στον κόσμο του υπολογισμού, συνδυάζοντας τα οφέλη του Public Cloud και του Private Cloud, αφού επιτρέπει στα δεδομένα και τις εφαρμογές να μετακινούνται μεταξύ των δύο περιβάλλοντων. Παρακάτω θα εξεταστεί η έννοια του Hybrid Cloud, τα χαρακτηριστικά του και τα οφέλη που προσφέρει στις επιχειρήσεις και τους οργανισμούς.

Το Hybrid Cloud αναφέρεται σε ένα υπολογιστικό περιβάλλον που συνδυάζει τη χρήση του Public Cloud και του Private Cloud, επιτρέποντας στις επιχειρήσεις να εκτελούν εφαρμογές και να αποθηκεύουν τα δεδομένα τους σε διάφορα περιβάλλοντα. Οι επιχειρήσεις μπορούν να διαχειρίζονται εσωτερικά στο ιδιωτικό νέφος ευαίσθητα δεδομένα και εφαρμογές, ενώ ταυτόχρονα αξιοποιούν την ευελιξία και την δυνατότητα κλιμάκωσης του δημόσιου νέφους για τις ανάγκες που απαιτούνται σε εξωτερικές εφαρμογές και φορτία εργασίας.



***Εικόνα 3**- Υβριδικό Νέφος (Hybrid Cloud)*

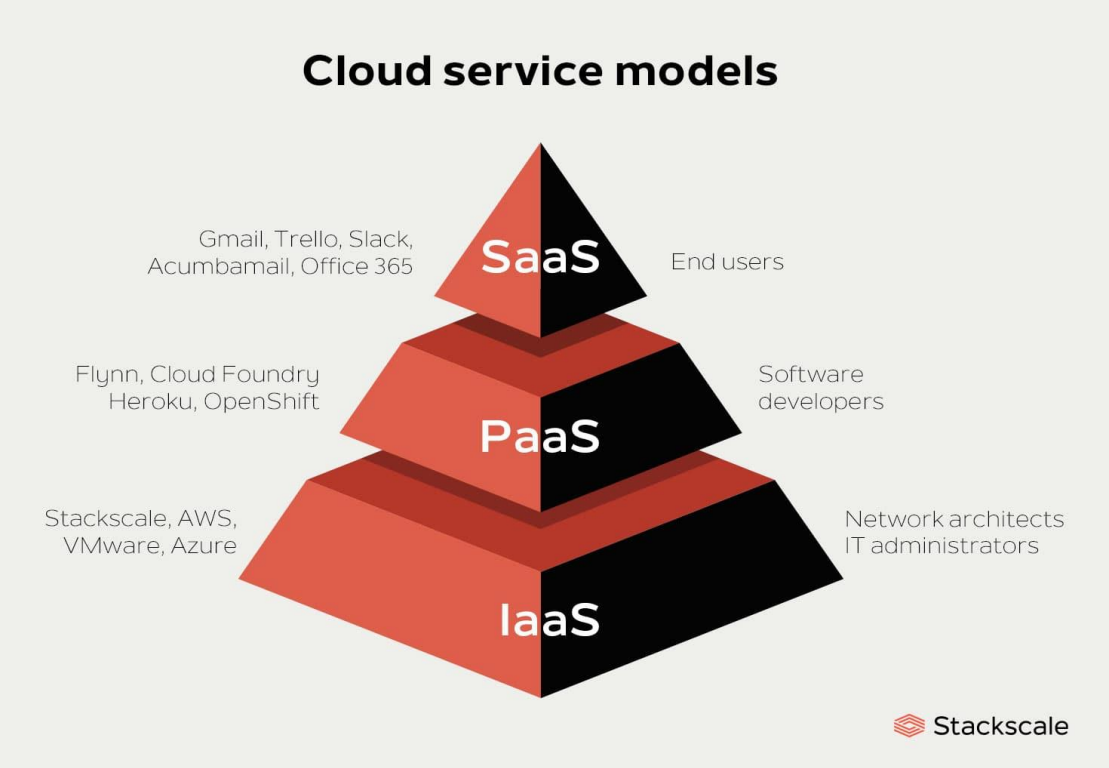
Ένα από τα βασικά χαρακτηριστικά του Hybrid Cloud είναι η ευελιξία. Οι επιχειρήσεις μπορούν να εκμεταλλευτούν τις δυνατότητες του Public Cloud για τις περιοδικές ή απρόβλεπτες αυξήσεις του φόρτου εργασίας, επιτρέποντας τους να αποκτήσουν πρόσθετους υπολογιστικούς πόρους και χώρο αποθήκευσης κατά βούληση. Αυτό σημαίνει πως ένα υβριδικό περιβάλλον cloud μπορεί να χρησιμοποιηθεί για να επιτρέψει σε ένα ιδιωτικό cloud να αυξηθεί για μια προσωρινή ζήτηση, αξιοποιώντας και αναπτύσσοντας δημόσιους πόρους cloud.

Το υβριδικό νέφος μπορεί να χρησιμοποιηθεί για να παρέχει ένα επιπλέον επίπεδο ασφάλειας, αφού οι χρήστες μπορούν να επιλέξουν ευέλικτα ποιες υπηρεσίες θα διατηρούν στο δημόσιο cloud και ποιες θα αναπτύξουν στην ιδιωτική τους cloud υποδομή, που είναι πιο ελεγχόμενη. Ένα άλλο σημαντικό πλεονέκτημα του Hybrid Cloud είναι η αξιοποίηση των ήδη υπάρχοντών επενδύσεων σε υποδομές του Private Cloud. Οι επιχειρήσεις μπορούν να αξιοποιήσουν το υπάρχον υλικό και το λογισμικό τους στο Private Cloud και ταυτόχρονα να επωφεληθούν από τις ευέλικτες δυνατότητες του Public Cloud. Αυτό μειώνει το κόστος και επιτρέπει την αποδοτική χρήση των πόρων.

2.5 Μοντέλα υπηρεσίας στο Νέφος – Cloud service models

Τα μοντέλα υπηρεσίας και ανάπτυξης στο Cloud Computing αντιπροσωπεύουν τις διάφορες προσεγγίσεις και παρεχόμενες υπηρεσίες που διατίθενται στο πλαίσιο του cloud. Αυτά τα μοντέλα παρέχουν στους χρήστες ευελιξία και επιλογές σχετικά με το πώς θα χρησιμοποιήσουν τους υπολογιστικούς πόρους του cloud και πώς θα αναπτύξουν και εκτελέσουν τις εφαρμογές τους. Στη συνέχεια, θα εξεταστούν τα τρία βασικά μοντέλα υπηρεσίας και ανάπτυξης στο cloud computing:

- IaaS
- PaaS
- SaaS



Εικόνα 4*- Τα μοντέλα Υπηρεσίας του cloud computing*

2.5.1 Υποδομή ως υπηρεσία (Iaas)

Το μοντέλο υποδομής ως υπηρεσία (IaaS) παρέχει την υποδομή υπολογιστών ως υπηρεσία. Οι πάροχοι cloud παρέχουν εικονικές μηχανές, αποθηκευτικό χώρο και δίκτυα, που επιτρέπουν στους χρήστες να έχουν πλήρη έλεγχο και ευελιξία στη διαχείριση της υποδομής τους. Οι χρήστες μπορούν να εγκαταστήσουν και να διαμορφώσουν το λειτουργικό σύστημα και το λογισμικό τους, ενώ η πρόσβαση στην υποδομή γίνεται απομακρυσμένα μέσω του διαδικτύου. Αυτό επιτρέπει στους χρήστες να αποκτήσουν ευελιξία στον τρόπο που αξιοποιούν τους υπολογιστικούς πόρους, μειώνοντας την ανάγκη για διαθέσιμους φυσικούς διακομιστές και εξοικονομώντας χρόνο και κόστος.

Η βασική ιδέα πίσω από το IaaS είναι να παρέχεται μια ευέλικτη υποδομή υπολογιστών που μπορεί να προσαρμοστεί ανάλογα με τις ανάγκες των χρηστών. Με αυτό το τρόπο, οι χρήστες δεν αναγκάζονται να αγοράζουν και να διαχειρίζονται δικούς τους φυσικούς διακομιστές και υποδομές, αλλά μπορούν να εκμεταλλευτούν την υποδομή του cloud για την εκτέλεση των εφαρμογών τους.

Σε ένα μοντέλο IaaS, ο πάροχος cloud είναι υπεύθυνος για τη διατήρηση του υλικού, της συνδεσιμότητας δικτύου στο διαδίκτυο και της φυσικής ασφάλειας. Οι χρήστες είναι υπεύθυνοι για οτιδήποτε άλλο: εγκατάσταση, διαμόρφωση και συντήρηση λειτουργικού συστήματος, διαμόρφωση του δικτύου, διαμόρφωση της βάσης δεδομένων και αποθήκευσης και ούτω καθεξής. Με άλλα λόγια, οι χρήστες νοικιάζουν το υλικό σε ένα κέντρο δεδομένων cloud, αλλά το πως θα αξιοποιηθεί αυτό το υλικό εξαρτάται από αυτούς.

Οι πάροχοι IaaS παρέχουν εικονικές μηχανές (Virtual Machines - VMs) που είναι απομακρυσμένα προσβάσιμες μέσω του διαδικτύου. Οι χρήστες μπορούν να εγκαταστήσουν και να διαμορφώσουν το λειτουργικό σύστημα, το λογισμικό και τις εφαρμογές τους στις εικονικές αυτές μηχανές, παρέχοντας τους πλήρη έλεγχο και ευελιξία. Η υποδομή του cloud αυξομειώνεται αυτόματα για να παρέχει τους απαιτούμενους υπολογιστικούς πόρους, όπως είναι η κεντρική μονάδα επεξεργασίας - CPU, η μνήμη και ο αποθηκευτικός χώρος, για την εκτέλεση των VMs.

Ένα σημαντικό χαρακτηριστικό του IaaS είναι η δυνατότητα κλιμάκωσης. Οι χρήστες μπορούν να αυξομειώσουν ή να μειώσουν τους υπολογιστικούς πόρους που χρησιμοποιούν ανάλογα με τις ανάγκες τους. Αυτό επιτρέπει την οικονομική χρήση των πόρων, καθώς οι χρήστες πληρώνουν μόνο για τους πόρους που χρησιμοποιούν και μπορούν να αυξομειώνουν την χωρητικότητα ανάλογα με τις ανάγκες τους.

Επιπλέον, το IaaS παρέχει αποθηκευτικό χώρο ως υπηρεσία. Οι χρήστες μπορούν να αποθηκεύουν τα δεδομένα τους σε απομακρυσμένα αποθηκευτικά συστήματα που παρέχονται από τους πάροχους IaaS. Με αυτό το τρόπο μειώνεται το ρίσκο απώλειας δεδομένων ενώ παράλληλα παρέχεται ευελιξία στην πρόσβαση και την κοινή χρήση των δεδομένων.

2.5.2 Πλατφόρμα ως υπηρεσία (PaaS)

Το μοντέλο πλατφόρμας ως υπηρεσία (PaaS) παρέχει μια πλατφόρμα ανάπτυξης και εκτέλεσης εφαρμογών ως υπηρεσία. Σε ένα περιβάλλον PaaS, ο πάροχος cloud διατηρεί τη φυσική υποδομή, τη φυσική

ασφάλεια και τη σύνδεση στο διαδίκτυο. Διατηρεί ακόμη τα λειτουργικά συστήματα, το ενδιάμεσο λογισμικό, τα εργαλεία ανάπτυξης και τις υπηρεσίες business intelligence που συνθέτουν μια λύση cloud.

Οι πάροχοι cloud παρέχουν ένα περιβάλλον ανάπτυξης που περιλαμβάνει γλώσσες προγραμματισμού, βιβλιοθήκες, εργαλεία ανάπτυξης και υπηρεσίες για τη διαχείριση της υποδομής της εφαρμογής. Οι χρήστες μπορούν να αναπτύξουν, να δοκιμάσουν και να εκτελέσουν τις εφαρμογές τους στο πλαίσιο αυτής της πλατφόρμας χωρίς όμως να ανησυχούν για την άδεια ή την ενημέρωση του κώδικα του λειτουργικού συστήματος και των βάσεων δεδομένων. Αυτό προσφέρει στους χρήστες τη δυνατότητα να επικεντρωθούν στην ανάπτυξη των εφαρμογών τους, αντί να ασχολούνται με τις λεπτομέρειες που σχετίζονται με τη διατήρηση της υποδομής.

2.5.3 Λογισμικό ως υπηρεσία (SaaS)

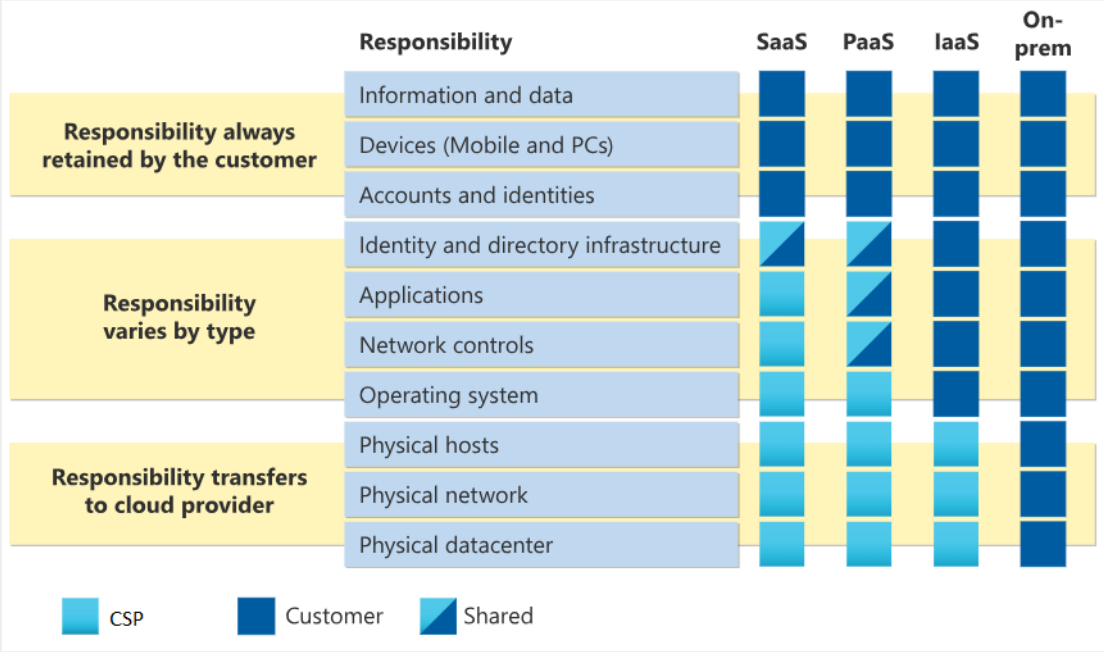
Το μοντέλο λογισμικού ως υπηρεσία (SaaS) παρέχει λογισμικό ως υπηρεσία μέσω του cloud. Οι χρήστες έχουν πρόσβαση σε ένα έτοιμο λογισμικό που εκτελείται απομακρυσμένα στον cloud και μπορούν να το χρησιμοποιήσουν μέσω του διαδικτύου. Αυτό απαλλάσσει τους χρήστες από την ανάγκη να εγκαταστήσουν και να συντηρήσουν το λογισμικό στους δικούς τους υπολογιστές. Οι πάροχοι cloud φροντίζουν για την ενημέρωση και τη συντήρηση του λογισμικού, καθώς και για την ασφάλεια και την απόδοσή του. Το SaaS προσφέρει στους χρήστες αμεσότητα στο λογισμικό και επιτρέπει την ευέλικτη χρήση του, χωρίς να απαιτείται μεγάλη αρχική επένδυση στην αγορά της άδειας και τη συντήρηση του λογισμικού. Μπορεί να θεωρηθεί ως το πιο ολοκληρωμένο μοντέλο υπηρεσιών νέφους, αφού ουσιαστικά ο χρήστης νοικιάζει η χρησιμοποιεί μια πλήρως ανεπτυγμένη εφαρμογή, όπως για παράδειγμα μια υπηρεσία ηλεκτρονικού ταχυδρομείου ή υπηρεσίες ανταλλαγής μηνυμάτων, που αποτελούν τα πιο χαρακτηριστικά παραδείγματα SaaS υλοποιήσεων. Μπορεί το μοντέλο SaaS να είναι το λιγότερο ευέλικτο, είναι όμως το πιο εύκολο να τεθεί σε λειτουργία καθώς απαιτεί λιγότερες τεχνικές γνώσεις για να χρησιμοποιηθεί.

2.5.4 Το μοντέλο κοινής ευθύνης

Τα μοντέλα υπηρεσίας και ανάπτυξης στο cloud computing προσφέρουν διάφορες επιλογές για τους χρήστες, ανάλογα με τις ανάγκες και τις απαιτήσεις τους. Το IaaS παρέχει ευελιξία και έλεγχο, το PaaS προσφέρει μια ολοκληρωμένη πλατφόρμα ανάπτυξης, ενώ το SaaS παρέχει έτοιμες εφαρμογές που μπορούν να χρησιμοποιηθούν απευθείας. Η επιλογή του κατάλληλου μοντέλου εξαρτάται από τις ανάγκες της επιχείρησης ή του χρήστη, καθώς και από το επίπεδο ελέγχου και την ευελιξία που απαιτούν.

Τα μοντέλα υπηρεσίας και ανάπτυξης στο cloud computing παρέχουν επιλογές και ευελιξία στους χρήστες για τη χρήση και ανάπτυξη εφαρμογών στον cloud. Αυτές οι προσεγγίσεις έχουν επαναπροσδιορίσει τον τρόπο με τον οποίο οι επιχειρήσεις αξιοποιούν τους υπολογιστικούς πόρους, προσφέροντας ευελιξία, αποδοτικότητα και οικονομία στον τομέα της υπολογιστικής υποδομής και της ανάπτυξης εφαρμογών.

Το μοντέλο κοινής ευθύνης (Shared Responsibility Model) είναι ένα πλαίσιο ασφάλειας και συμμόρφωσης που περιγράφει τις ευθύνες των παρόχων υπηρεσιών cloud (Cloud Service Providers – CSP) και των χρηστών για κάθε πτυχή του περιβάλλοντος νέφους, συμπεριλαμβανομένου του υλικού, των υποδομών, των δεδομένων, των ρυθμίσεων του λειτουργικού συστήματος, των δικαιωμάτων πρόσβασης κοκ. Το μοντέλο αυτό ισχύει για όλους τους τύπους των υπηρεσιών του cloud. Το SaaS είναι το μοντέλο το οποίο φέρει τη μεγαλύτερη ευθύνη στον πάροχο και τη λιγότερη ευθύνη στο χρήστη, σε ένα μοντέλο PaaS η ευθύνη μοιράζεται μεταξύ αυτών των δύο ενώ σε ένα μοντέλο IaaS οι μεγαλύτερες ευθύνες βαραίνουν το χρήστη. Τα παραπάνω απεικονίζονται γραφικά στην εικόνα που ακολουθεί:



***Εικόνα 5**: Το μοντέλο κοινής ευθύνης*

2.6 Έννοιες και μοντέλα ιδιωτικότητας στο υπολογιστικό νέφος

2.6.1 Η έννοια της ιδιωτικότητας

Η ιδιωτικότητα αποτελεί ένα σημαντικό ζήτημα στον κόσμο του υπολογιστικού νέφους. Το απόρρητο των δεδομένων δίνει στους χρήστες, δηλαδή στα αντικείμενα των δεδομένων, τη δυνατότητα να λαμβάνουν μόνοι τους αποφάσεις σχετικά με το ποιος μπορεί να επεξεργαστεί τα δεδομένα τους, πότε και για ποιους σκοπούς. Οι χρήστες και οργανισμοί επιθυμούν να είναι σίγουροι ότι τα δεδομένα τους παραμένουν ιδιωτικά και ασφαλή κατά την αποθήκευση και επεξεργασία τους στο cloud.

2.6.2 Μοντέλα ιδιωτικότητας

Στην παρούσα ενότητα θα παρουσιαστούν οι έννοιες και τα μοντέλα ιδιωτικότητας που χρησιμοποιούνται στο υπολογιστικό νέφος.

- Ιδιωτικότητα δεδομένων: Η ιδιωτικότητα δεδομένων αναφέρεται στο δικαίωμα και την ευθύνη των χρηστών να προστατεύουν τα προσωπικά τους δεδομένα και να έχουν έλεγχο επί του ποιος έχει πρόσβαση σε αυτά. Στο υπολογιστικό νέφος, η ευθύνη για τη διατήρηση της ιδιωτικότητας των δεδομένων των χρηστών βαραίνει τον πάροχο υπηρεσιών cloud.

- Έλεγχος πρόσβασης: Ένα σημαντικό μοντέλο ιδιωτικότητας στο υπολογιστικό νέφος είναι ο έλεγχος πρόσβασης. Αυτό περιλαμβάνει τον καθορισμό των δικαιωμάτων πρόσβασης στα δεδομένα και τις εφαρμογές που αποθηκεύονται στο cloud. Οι χρήστες μπορούν να ορίσουν ποιοι θα έχουν πρόσβαση στα δεδομένα τους και να ελέγχουν τα επίπεδα πρόσβασης σύμφωνα με τον ρόλο, τις ευθύνες και τις ανάγκες τους.

- Κρυπτογράφηση δεδομένων: Η κρυπτογράφηση δεδομένων είναι μια τεχνική που χρησιμοποιείται για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Οι χρήστες μπορούν να κρυπτογραφήσουν τα δεδομένα τους πριν τα μεταφέρουν ή τα αποθηκεύσουν στο cloud, έτσι ώστε μόνο εξουσιοδοτημένα άτομα να έχουν την ικανότητα να τα αποκρυπτογραφήσουν.

- Νομοθεσία και συμμόρφωση: Η νομοθεσία και η συμμόρφωση αφορούν στις νομικές υποχρεώσεις και στους κανονισμούς που αφορούν την προστασία των δεδομένων και την ιδιωτικότητα στο cloud. Οι παρόχοι υπηρεσιών cloud και οι χρήστες πρέπει να τηρούν τις νομικές απαιτήσεις που ισχύουν για την προστασία των προσωπικών δεδομένων και να συμμορφώνονται με αυτές σε κάθε περίπτωση.

Στο επόμενο κεφάλαιο θα γίνει εκτενής ανάλυση των ζητημάτων και των προκλήσεων που αφορούν στην ασφάλεια των προσωπικών και ιδιωτικών δεδομένων που αποθηκεύονται σε δομές cloud. Επίσης, θα παρουσιαστούν μηχανισμοί ασφάλειας που εφαρμόζονται σήμερα σε υπηρεσίες υπολογιστικού νέφους για την προστασία τους.

Κεφάλαιο 3 – Ασφάλεια και προστασία δεδομένων στο cloud

3.1 Προκλήσεις και απειλές

Το υπολογιστικό νέφος έχει επιφέρει σημαντικές αλλαγές στον τρόπο που αποθηκεύονται, διαχειρίζονται και παρέχονται οι υπηρεσίες πληροφορικής. Παρά τα πλεονεκτήματα που προσφέρει, η χρήση του υπολογιστικού νέφους επιφέρει και ορισμένες προκλήσεις και απειλές που αφορούν σε θέματα ασφαλείας. Στην ενότητα αυτή θα καταγραφούν και θα αναλυθούν οι προκλήσεις και οι απειλές που είναι πιθανό να εμφανιστούν στο υπολογιστικό νέφος.

Παρά τις ευθύνες και τις υποχρεώσεις που έχουν οι πάροχοι για τη διασφάλιση του απορρήτου της πληροφορίας των χρηστών τους, υπάρχουν απαιτήσεις και ενέργειες που μπορούν να γίνουν και από τη πλευρά των χρηστών για τη προστασία των δεδομένων. Η εξασφάλιση της εμπιστευτικότητας των δεδομένων μπορεί

να επιτευχθεί μέσω τεχνολογιών όπως είναι κρυπτογράφηση, τα εικονικά τοπικά δίκτυα, η εφαρμογή ενός τείχους προστασίας και φίλτρα πακέτων και άλλα.

Παράλληλα, υπάρχει ανησυχία σχετικά με τη νομοθεσία ορισμένων χωρών που απαιτεί από τους παρόχους cloud να αποθηκεύουν τα δεδομένα των πελατών και τα αντίγραφά τους εντός των εθνικών συνόρων καθώς ορισμένες επιχειρήσεις ενδέχεται να μην επιθυμούν την πρόσβαση των κρατών στα δεδομένα τους μέσω του δικαστικού συστήματος των χωρών αυτών. Το cloud δίνει στους πάροχους και τους χρήστες του τη δυνατότητα να επιλέξουν τη τοποθεσία στην οποία θα αποθηκευτούν τα δεδομένα τους για τέτοιες περιπτώσεις.

3.1.1 Απώλεια ελέγχου

Η απώλεια ελέγχου μπορεί να συμβεί σε μια επιχείρηση που έχει μεταφέρει όλες τις υπηρεσίες και τα δεδομένα της στο υπολογιστικό νέφος, καθώς τότε παύει να έχει άμεσο έλεγχο επί των φυσικών υποδομών και της ασφάλειας των δεδομένων της και εξαρτάται αποκλειστικά από τον πάροχο υπηρεσιών νέφους για την παροχή αυτής της λειτουργικότητας.

Η απώλεια ελέγχου έχει διάφορες πτυχές, οι οποίες εξετάζονται παρακάτω:

- Φυσική απώλεια ελέγχου: Όταν μια επιχείρηση χρησιμοποιεί υπηρεσίες cloud, δεν έχει πλέον τον άμεσο έλεγχο επί των φυσικών υποδομών που φιλοξενούν τα δεδομένα και τις εφαρμογές της. Οι φυσικές υποδομές, όπως τα διακομιστής, οι αποθήκες δεδομένων και οι δίκτυα, ελέγχονται και διαχειρίζονται από τον πάροχο υπηρεσιών cloud. Αυτό μπορεί να δημιουργήσει ανησυχίες όσον αφορά στη φυσική ασφάλεια των εγκαταστάσεων, την πρόσβαση μη εξουσιοδοτημένων ατόμων σε αυτές και την προστασία από φυσικές καταστροφές.

- Ασφάλεια δεδομένων: Η εμπιστευτικότητα και οι περιορισμοί πρόσβασης στα δεδομένα αποτελούν σημαντικό μέρος του ελέγχου για μια επιχείρηση. Όταν τα δεδομένα μεταφέρονται και αποθηκεύονται σε ένα υπολογιστικό νέφος, η επιχείρηση εξαρτάται από τον πάροχο υπηρεσιών που είναι υπεύθυνος να διασφαλίσει την ασφάλεια και την προστασία των δεδομένων της. Είναι λογικό να εγείρονται ανησυχίες για πιθανές παραβιάσεις ασφάλειας που μπορεί να οδηγήσουν σε διαρροή δεδομένων, απώλεια ευαίσθητων πληροφοριών και παραβίαση των νομοθετικών απαιτήσεων.

- Απώλεια ελέγχου επί των λειτουργιών: Με τη μετάβαση στο υπολογιστικό νέφος, οι επιχειρήσεις παραδίδουν τον έλεγχο των λειτουργιών και των διαδικασιών στον πάροχο υπηρεσιών. Αυτό σημαίνει ότι η επιχείρηση δεν έχει πλήρη ορατότητα και έλεγχο επί της εκτέλεσης των εφαρμογών της, της απόδοσης του συστήματος και της διαχείρισης των προβλημάτων. Αυτό μπορεί να περιορίσει την ικανότητα ανίχνευσης και αντιμετώπισης προβλημάτων ή αποτυχιών, καθώς και την προσαρμοστικότητα και ευελιξία των λειτουργιών της επιχείρησης.

- Εξάρτηση από τον πάροχο υπηρεσιών: Μια επιχείρηση που χρησιμοποιεί υπηρεσίες cloud εξαρτάται από τον πάροχο της, ο οποίος είναι υπεύθυνος να της προσφέρει αξιόπιστες, ασφαλείς

και αποτελεσματικές υπηρεσίες. Οποιαδήποτε απρόοπτη αποτυχία ή παραβίαση ασφάλειας από τον πάροχο μπορεί να επιφέρει σοβαρές συνέπειες στην επιχείρηση. Επιπλέον, η εξάρτηση από έναν μόνο πάροχο μπορεί να περιορίσει την ευελιξία και την ανταγωνιστικότητα μιας επιχείρησης.

3.1.2 Απειλές ασφάλειας δεδομένων

Η ασφάλεια των δεδομένων είναι μία από τις βασικές προκλήσεις στο υπολογιστικό νέφος. Επιθέσεις όπως η παραβίαση δεδομένων, η κλοπή ταυτότητας, η κακόβουλη χρήση και η απώλεια δεδομένων μπορούν να προκαλέσουν σημαντικές ζημιές. Είναι σημαντικό να εφαρμόζονται δυνατά μέτρα ασφαλείας, όπως η κρυπτογράφηση δεδομένων και ο έλεγχος πρόσβασης, προκειμένου να διασφαλιστεί η προστασία των δεδομένων. Για την αποτροπή αυτών των απειλών, είναι απαραίτητο να ληφθούν δραστικά μέτρα ασφαλείας.

Ορισμένες από τις απειλές ασφάλειας δεδομένων που οι χρήστες μπορεί να έρθουν αντιμέτωποι στο υπολογιστικό νέφος περιλαμβάνουν:

- Παραβίαση δεδομένων: Οι κακόβουλοι επιτιθέμενοι μπορεί να εκμεταλλευτούν τις αδυναμίες στην ασφάλεια για να παραβιάσουν τα δεδομένα που αποθηκεύονται στο νέφος. Μια παραβίαση δεδομένων μπορεί να οδηγήσει στην πρόσβαση, στη γνωστοποίηση, στην αλλοίωση ή ακόμη και στην απώλεια των ευαίσθητων πληροφοριών.

- Κλοπή ταυτότητας: Οι επιτιθέμενοι μπορεί να προσποιηθούν εξουσιοδοτημένους χρήστες ή να αποκτήσουν πρόσβαση σε πιστοποιητικά και διαπιστευτήρια πρόσβασης, προκειμένου να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Αυτό μπορεί να οδηγήσει σε κλοπή ταυτότητας χρηστών, απάτες ή κακόβουλη χρήση πληροφοριών.

- Κακόβουλη χρήση: Οι επιτιθέμενοι μπορεί να εκμεταλλευτούν το υπολογιστικό νέφος για να εκτελέσουν κακόβουλες ενέργειες, όπως είναι η εξάπλωση ιών, τροφοδότηση botnets ή να προκαλέσουν επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Destributed Denial Of Service – DDoS). Αυτές οι επιθέσεις διακόπτουν τις υπηρεσίες δικτύου και εξαντλούν τους πόρους μιας εφαρμογής, καθιστώντας την υπηρεσία ανίκανη να εξυπηρετήσει άλλα αιτήματα, που οδηγεί σε κακή λειτουργία η πλήρη αποσύνδεση της, απώλεια δεδομένων ή ζημιές στο σύστημα.

- Απώλεια δεδομένων: Οι διάφοροι παράγοντες, όπως η απρόοπτη αποτυχία του συστήματος, ανθρώπινοι παράγοντες ή φυσικές καταστροφές, μπορούν να οδηγήσουν στην απώλεια δεδομένων στο υπολογιστικό νέφος. Αυτό μπορεί να έχει σοβαρές συνέπειες για μια επιχείρηση, αφού μπορεί να οδηγήσει στην απώλεια ευαίσθητων πληροφοριών, στη μη συμμόρφωση με νομοθεσία που μπορεί να επιφέρει υψηλά πρόστιμα και είναι πιθανό να βλάψει την εικόνα, τη φήμη και την αξιοπιστία της επιχείρησης.

3.1.3 Κοινή χρήση πόρων

Το υπολογιστικό νέφος συχνά χρησιμοποιεί κοινούς πόρους για την αποθήκευση και επεξεργασία δεδομένων από πολλούς χρήστες. Αυτό μπορεί να δημιουργήσει προκλήσεις όσον αφορά την απομόνωση των δεδομένων, καθώς και την προστασία από επιθέσεις μεταξύ των χρηστών. Οι παρόχοι υπηρεσιών cloud πρέπει να εφαρμόζουν κατάλληλες τεχνικές και πολιτικές για τη διασφάλιση της ασφάλειας των πόρων τους.

Όταν πολλοί χρήστες μοιράζονται τους ίδιους φυσικούς πόρους, όπως δίσκους αποθήκευσης, επεξεργαστική ισχύ ή δίκτυο, υπάρχει η ανάγκη για αποτελεσματική απομόνωση των δεδομένων και των εργασιών μεταξύ των χρηστών. Αυτό είναι απαραίτητο προκειμένου να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, καθώς και η αποτελεσματική λειτουργία των εφαρμογών.

Η προστασία από επιθέσεις μεταξύ των χρηστών αποτελεί ύψιστη ανάγκη. Ένας κακόβουλος χρήστης μπορεί να επιχειρήσει να αποκτήσει πρόσβαση σε δεδομένα άλλων χρηστών, να παρεμποδίσει την ορθή λειτουργία των υπηρεσιών ή ακόμα και να εκτελέσει κακόβουλες επιθέσεις.

Για να αντιμετωπιστούν αυτές οι προκλήσεις, οι παρόχοι υπηρεσιών νέφους εφαρμόζουν διάφορες τεχνικές και πολιτικές για τη διασφάλιση της ασφάλειας των πόρων. Αυτές περιλαμβάνουν μεταξύ άλλων τα παρακάτω:

- Απομόνωση των πόρων: Οι πόροι που χρησιμοποιούνται από διάφορους χρήστες πρέπει να είναι απομονωμένοι μεταξύ τους. Αυτό μπορεί να επιτευχθεί με τη χρήση τεχνολογιών εικονικοποίησης και επιμέρους ελέγχου πρόσβασης στους πόρους.

- Ασφάλεια των δεδομένων: Τα δεδομένα πρέπει να κρυπτογραφούνται κατάλληλα κατά τη μεταφορά και την αποθήκευσή τους στο νέφος. Επίσης, πρέπει να εφαρμόζονται μηχανισμοί ελέγχου πρόσβασης για να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα.

- Ανίχνευση επιθέσεων και πρόληψη: Οι παρόχοι υπηρεσιών νέφους χρησιμοποιούν τεχνικές ανίχνευσης και πρόληψης επιθέσεων για να εντοπίζουν και να αντιμετωπίζουν πιθανές απειλές ασφάλειας.

- Πολιτικές ασφαλείας: Οι παρόχοι νέφους θεσπίζουν πολιτικές ασφαλείας και διαδικασίες που πρέπει να ακολουθούν οι χρήστες για να διασφαλιστεί η ασφάλεια των πόρων. Αυτές περιλαμβάνουν τη χρήση δυνατών κωδικών πρόσβασης και συχνή αλλαγή αυτών, την ενημέρωση λογισμικού με παραμέτρους ασφαλείας και την εκπαίδευση των χρηστών σχετικά με τους κινδύνους ασφαλείας και τις βέλτιστες πρακτικές προστασίας.

3.1.4 Επιθέσεις DDoS

Οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας DDoS (Distributed Denial of Service) αποτελούν μια σοβαρή απειλή για το υπολογιστικό νέφος. Οι παρόχοι υπηρεσιών cloud πρέπει να έχουν ειδικά μέτρα

αντιμετώπισης των επιθέσεων DDoS για να διατηρήσουν την αποδοτικότητα και την ασφάλεια των υπηρεσιών τους αλλά και την αξιοπιστία τους.

Κατά την διάρκεια μιας επίθεσης τύπου DDoS, κακόβουλοι χρήστες επιχειρούν να προκαλέσουν διακοπή των υπηρεσιών, «πλημμυρίζοντας» το σύστημα με εκατοντάδες ή ακόμη και χιλιάδες ψεύτικα αιτήματα. Ο σκοπός της επίθεσης αυτής είναι να υπερφορτώσει την υποδομή του νέφους, καταναλώνοντας όλους τους διαθέσιμους πόρους και να προκαλέσουν αποκοπή των υπηρεσιών για τους νόμιμους και αληθινούς χρήστες.

Οι επιθέσεις DDoS μπορούν να προκληθούν από δικτυακούς πόρους που είναι καταχωρημένοι σε διάφορα μέρη του κόσμου και συντονίζονται από τους επιτιθέμενους με σκοπό να ενισχύσουν την επίθεση. Με την αύξηση της χωρητικότητας των δικτύων, οι επιθέσεις DDoS έχουν γίνει πιο εξελιγμένες και δυσκολότερες να αντιμετωπιστούν.

Για να αντιμετωπιστούν αυτού του είδους οι επιθέσεις, οι πάροχοι υπηρεσιών cloud λαμβάνουν ειδικά μέτρα ασφαλείας και υιοθετούν τεχνικές προστασίας. Ορισμένα από τα μέτρα αυτά περιλαμβάνουν:

- Φιλτράρισμα εισερχομένης κίνησης: Οι πάροχοι υπηρεσιών χρησιμοποιούν συστήματα φιλτραρίσματος για να ανιχνεύσουν και να αποκλείσουν την εισερχόμενη κίνηση που προέρχεται από κακόβουλες πηγές. Αυτό μπορεί να επιτευχθεί μέσω της ανάλυσης των πακέτων δεδομένων και των εισερχόμενων συνδέσεων για την ανίχνευση ανωμαλιών και απειλών.

- Κατανομή φόρτου: Οι πάροχοι υπηρεσιών cloud χρησιμοποιούν συστήματα κατανομής φόρτου για να διαχειρίζονται την κίνηση και να ανταποκρίνονται στις αιτήσεις των χρηστών. Αυτό τους επιτρέπει να αντιμετωπίζουν αυξημένη κίνηση από επιθέσεις DDoS, αποκρίνοντας με αποτελεσματικό τρόπο και εξασφαλίζοντας την διαθεσιμότητα των υπηρεσιών για τους νόμιμους χρήστες.

- Ανίχνευση και αντίδραση σε πραγματικό χρόνο: Οι πάροχοι υπηρεσιών cloud χρησιμοποιούν συστήματα ανίχνευσης και αντίδρασης σε πραγματικό χρόνο για την αναγνώριση και απόκριση σε επιθέσεις DDoS. Με τη χρήση προηγμένων αλγορίθμων και τεχνικών ανάλυσης, ανιχνεύονται οι αιτήσεις που προέρχονται από κακόβουλους πηγές και λαμβάνονται αυτόματα μέτρα για τον αποκλεισμό τους.

- Ενισχυμένη υποδομή: Οι πάροχοι υπηρεσιών cloud επενδύουν σε ενισχυμένες υποδομές για να αντιμετωπίζουν επιθέσεις DDoS. Αυτό περιλαμβάνει τη χρήση υψηλής χωρητικότητας δικτυακών συνδέσεων, τη χρήση ανθεκτικών δικτυακών υποδομών και τη δημιουργία αποκλεισμένων περιοχών από την υποδομή του νέφους για την απομόνωση των επιθέσεων.

3.1.5 Ελλείψεις συμμόρφωσης και νομοθεσίας

Οι χρήστες του υπολογιστικού νέφους, καθώς και οι πάροχοι υπηρεσιών, πρέπει να συμμορφώνονται με τα νομοθετικά πλαίσια που αφορούν στην ασφάλεια των δεδομένων και στην προστασία της ιδιωτικότητας. Η μη συμμόρφωση με αυτές τις απαιτήσεις μπορεί να οδηγήσει σε νομικές συνέπειες με υψηλά πρόστιμα και υποβάθμιση της φήμης τους με αποτέλεσμα την απώλεια εμπιστοσύνης των πελατών.

3.1.6 Insecure application programming interfaces

Η ασφάλεια των δεδομένων στο υπολογιστικό νέφος μπορεί να επηρεαστεί από την ελλιπή ασφάλεια των διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces - APIs). Οι πάροχοι υπηρεσιών cloud παρέχουν APIs για να επιτρέψουν στους χρήστες να επικοινωνούν και να αλληλοεπιδρούν με τις υπηρεσίες τους. Η ασφάλεια και η διαθεσιμότητα των υπηρεσιών στο cloud εξαρτώνται σε μεγάλο βαθμό από την ασφάλεια αυτών των APIs.

Αυτό το θέμα γίνεται όλο και πιο περίπλοκο όταν πολλοί οργανισμοί χρησιμοποιούν αυτά τα APIs για να παρέχουν υπηρεσίες στους πελάτες τους. Όταν τα APIs είναι αδύναμα ή δεν είναι αρκετά ασφαλή, τότε κάθε τυχαία ή κακόβουλη προσπάθεια για παραβίασή τους μπορεί να αφήσει τα δεδομένα στο cloud εκτεθειμένα σε πολλαπλές απειλές. Αυτές οι απειλές μπορεί να συνδέονται με θέματα όπως η έλλειψη ελέγχου πρόσβασης, η αδυναμία κλιμάκωσης, η περιορισμένη παρακολούθηση και άλλα ζητήματα ασφάλειας.

Οι κίνδυνοι που σχετίζονται με αδύναμα ή μη ασφαλή APIs περιλαμβάνουν την γνωστοποίηση ή την αλλοίωση δεδομένων, την απώλεια ελέγχου πρόσβασης, τη δυνατότητα εκτέλεσης κακόβουλου λογισμικού, την αποτυχία ανίχνευσης και πρόληψης επιθέσεων και άλλες ευπάθειες που μπορούν να εκθέσουν τα δεδομένα σε κινδύνους. Είναι σημαντικό οι πάροχοι υπηρεσιών cloud να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας για την προστασία των APIs και των δεδομένων που αυτά προσφέρουν.

3.1.7 Ανεπαρκής δέουσα επιμέλεια (Insufficient Due Diligence)

Η ανεπαρκής δέουσα επιμέλεια αναφέρεται στην έλλειψη ενημέρωσης και γνώσης των πιθανών κινδύνων με τους οποίους μπορεί να έρθει αντιμέτωπη μια επιχείρηση που αποφασίζει να μεταφέρει τα δεδομένα και τις υπηρεσίες της στο υπολογιστικό νέφος. Το υπολογιστικό νέφος παρέχει ελκυστικές ευκαιρίες για απεριόριστους υπολογιστικούς πόρους και γρήγορη πρόσβαση, και ως αποτέλεσμα πολλές επιχειρήσεις χρησιμοποιούν το νέφος χωρίς να αξιολογήσουν επαρκώς τους σχετικούς κινδύνους και χωρίς να διασφαλίζουν με κάποιο τρόπο την αξιοπιστία του παρόχου που επέλεξαν. Η ανεπαρκής δέουσα επιμέλεια συμβαίνει όταν οι οργανισμοί προσπαθούν να προχωρήσουν πολύ γρήγορα στην υιοθέτηση της τεχνολογίας χωρίς να την έχουν κατανοήσει πλήρως.

Λόγω της πολύπλοκης αρχιτεκτονικής του νέφους, ορισμένες πολιτικές ασφάλειας των οργανισμών δεν μπορούν να εφαρμοστούν στο περιβάλλον του νέφους. Επιπλέον, ορισμένοι χρήστες του νέφους δεν έχουν

γνώση για τις εσωτερικές διαδικασίες ασφάλειας, τους ελέγχους που πρέπει να υλοποιηθούν, την καταγραφή και την πρόσβαση στα δεδομένα. Σε ορισμένες περιπτώσεις, οι προγραμματιστές των εφαρμογών ενδέχεται να μην αντιλαμβάνονται τις επιπτώσεις που θα έχει η εφαρμογή τους στο περιβάλλον του νέφους, με αποτέλεσμα να προκαλούνται λειτουργικά και αρχιτεκτονικά προβλήματα.

Η βασική συστάση της CSA (Cloud Security Alliance) προς τους οργανισμούς είναι να διασφαλίσουν ότι διαθέτουν αρκετούς πόρους και να διεξάγουν εκτενείς και λεπτομερείς ελέγχους πριν επιλέξουν να χρησιμοποιήσουν τις υπηρεσίες του νέφους.

***Εικόνα 5**- Οι σημαντικές προκλήσεις και αδυναμίες του υπολογιστικού νέφους*

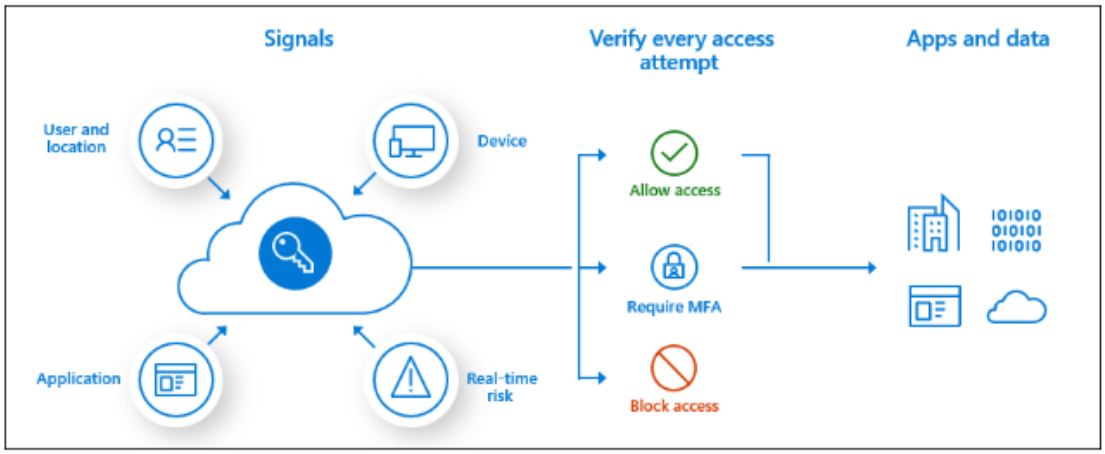
3.2 Τεχνικές ασφάλειας στο υπολογιστικό νέφος

Στο υπολογιστικό νέφος, υπάρχουν διάφορες μέθοδοι και τεχνικές ασφάλειας που χρησιμοποιούνται τόσο για την ταυτοποίηση των χρηστών όσο και για την εξουσιοδότηση, καθώς και για την προστασία από απειλές και την ασφάλεια των προσωπικών δεδομένων. Ορισμένες από αυτές περιλαμβάνουν:

3.2.1 Ταυτοποίηση πολλών παραγόντων (Multi-factor authentication)

Ο έλεγχος ταυτότητας που επιτυγχάνεται με τη χρήση πολλών παραγόντων (Multi-factor authentication – MFA) προσδίδει μεγαλύτερα επίπεδα προστασίας κατά τη διαδικασία εισόδου ενός χρήστη σε ένα λογαριασμό ή μια εφαρμογή. Η ταυτοποίηση υποβάλλει το χρήστη σε μια σειρά από ενέργειες και απαιτεί δύο ή και παραπάνω μεθόδους ελέγχου ταυτότητας προτού επιτραπεί η είσοδος. Από το χρήστη ζητείται κάτι που γνωρίζει, όπως για παράδειγμα ένας κωδικός πρόσβασης ή κάποιο PIN, κάτι που έχει το οποίο μπορεί να είναι μια αξιόπιστη συσκευή όπως ένα τηλέφωνο ή ένα κλειδί υλικού, ή κάτι που είναι, το οποίο μπορεί να αποδείξει

μέσω βιομετρικών στοιχείων. Αυτό ενισχύει την ασφάλεια και δυσκολεύει την εξουσιοδότησή. Σε περίπτωση που κάποιο στάδιο αποτύχει η που παρατηρηθεί ύποπτη δραστηριότητα (για παράδειγμα αν ο χρήστης αιτηθεί είσοδο από διαφορετική χώρα ή νέα συσκευή) μπορεί να ζητηθούν επιπλέον μέτρα ταυτοποίησης όπως για παράδειγμα κάποια επιβεβαίωση μέσω email προτού επιτραπεί η είσοδος, διαφορετικά η είσοδος είναι πιθανό να απαγορευτεί.



***Εικόνα 6**- Τρόπος Λειτουργίας της μεθόδου «Ταυτοποίηση πολλών παραγόντων (Multi-factor authentication)*

Η βασική ιδέα πίσω από την ταυτοποίηση πολλών παραγόντων είναι ότι η χρήση μόνο ενός παράγοντα για την επιβεβαίωση της ταυτότητας (όπως ένας κωδικός πρόσβασης) μπορεί να είναι ανεπαρκής και ευάλωτος σε επιθέσεις.

Συνήθως, η ταυτοποίηση πολλών παραγόντων στο cloud απαιτεί τη συνδυασμένη χρήση τουλάχιστον δύο από τους παρακάτω παράγοντες:

- Κάτι που γνωρίζει ο χρήστης: Αυτό μπορεί να είναι ένας κωδικός πρόσβασης, ένα μυστικό ερώτημα ή ένας κωδικός μιας χρήσης. Ο χρήστης πρέπει να παρέχει τη σωστή απάντηση ή τον σωστό κωδικό για να αποδείξει την ταυτότητά του.

- Κάτι που διαθέτει ο χρήστης: Αυτό μπορεί να είναι μια εγγεγραμμένη συσκευή όπως ένα κινητό ή laptop, μια κάρτα ελέγχου πρόσβασης ή ένα αναγνωριστικό συσκευής. Ο χρήστης πρέπει να διαθέτει το σωστό μέσο και να το χρησιμοποιήσει για να αποδείξει ποιος είναι.

- Κάτι που είναι μοναδικό για τον χρήστη: Αυτό μπορεί να είναι ένα βιομετρικό στοιχείο, όπως αποτυπώματα δακτύλων, αναγνώριση προσώπου ή φωνής ή της ίριδας του ματιού.

Με την ταυτοποίηση πολλών παραγόντων, οι χρήστες πρέπει να παρέχουν πληροφορίες από διαφορετικές κατηγορίες, εξασφαλίζοντας έτσι υψηλότερο επίπεδο ασφάλειας και δυσκολεύοντας την απομίμηση ή την παράκαμψη της ταυτοποίησης. Αυτό μπορεί να περιλαμβάνει τη συνδυασμένη χρήση κωδικού πρόσβασης, SMS επιβεβαίωσης, καρτών πρόσβασης ή βιομετρικών δεδομένων.

Η ταυτοποίηση πολλών παραγόντων αυξάνει την ασφάλεια στο cloud, καθώς οι κακόβουλοι χρήστες θα χρειαστεί να παρέχουν περισσότερες αποδείξεις ταυτότητας για να αποκτήσουν πρόσβαση στο σύστημα. Επιπλέον, σε περίπτωση που ο ένας παράγοντας ταυτοποίησης παραβιαστεί ή αποτύχει, ο άλλος παράγοντας παρέχει επιπλέον προστασία.

3.2.2 Κρυπτογραφημένη επικοινωνία

Η κρυπτογράφηση χρησιμοποιείται για την προστασία των δεδομένων κατά την μετάδοση από τον χρήστη στο νέφος και αντίστροφα. Αυτή η τεχνική εμποδίζει την παρεμβολή τρίτων στην επικοινωνία και διασφαλίζει την εμπιστευτικότητα των δεδομένων. Η κρυπτογραφημένη επικοινωνία αποτελεί μια σημαντική τεχνική ασφάλειας στο υπολογιστικό νέφος. Η κρυπτογράφηση αναφέρεται στη διαδικασία μετατροπής των αρχικών δεδομένων σε μια δυσνόητη μορφή με χρήση αλγορίθμων κρυπτογράφησης. Με την κρυπτογράφηση, τα δεδομένα γίνονται μη αναγνώσιμα για οποιονδήποτε μη εξουσιοδοτημένο χρήστη προσπαθήσει να τα προσπελάσει.

Κατά την επικοινωνία μεταξύ του χρήστη και του νέφους, καθώς και αντίστροφα, η κρυπτογράφηση εφαρμόζεται για την προστασία των δεδομένων. Κατά τη μετάδοση, τα δεδομένα κρυπτογραφούνται χρησιμοποιώντας ένα κλειδί κρυπτογράφησης. Μόνο οι εξουσιοδοτημένοι αποδέκτες, οι οποίοι διαθέτουν το μοναδικό κλειδί αποκρυπτογράφησης, μπορούν να προσπελάσουν τα δεδομένα και να τα διαβάσουν.

Η κρυπτογραφημένη επικοινωνία εμποδίζει την παρεμβολή τρίτων στην επικοινωνία. Οποιαδήποτε απόπειρα προσπέλασης των κρυπτογραφημένων δεδομένων θα αποτύχει, εφόσον οι κακόβουλοι χρήστες δεν διαθέτουν το κατάλληλο κλειδί για να αποκρυπτογραφήσουν τα δεδομένα.

Η κρυπτογραφημένη επικοινωνία είναι απαραίτητη για τη διατήρηση της εμπιστευτικότητας των δεδομένων και της διασφάλισης του απορρήτου στον χώρο του cloud. Με τη χρήση της κρυπτογράφησης, ακόμη και αν κάποιος εξουσιοδοτημένος χρήστης προσπελάσει τα δεδομένα, δεν θα μπορεί να τα διαβάσει ή να τα κατανοήσει εάν δε τα αποκρυπτογραφήσει πρώτα.

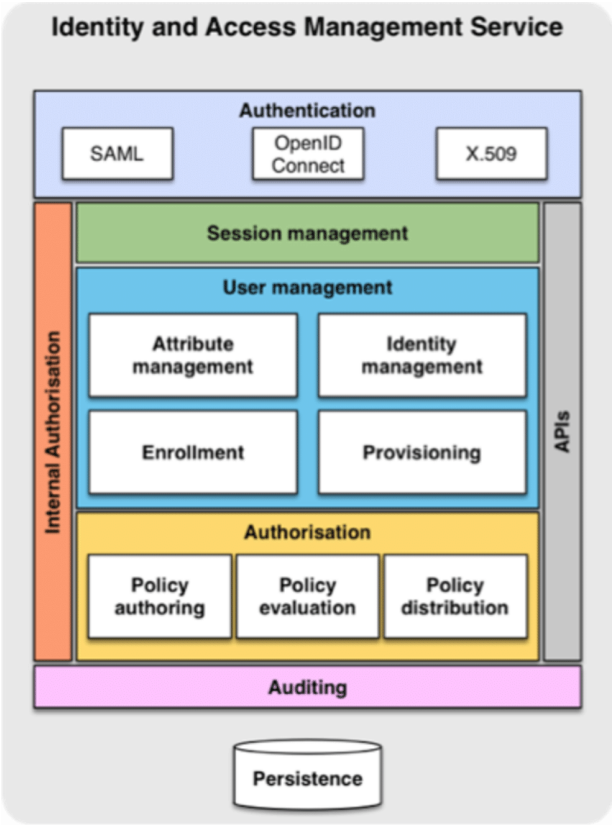
3.2.3 Διαχείριση ταυτοποίησης και πρόσβασης (IAM)

Είναι αναγκαίο να ελέγχεται σε τι επιτρέπεται και σε τι δεν επιτρέπεται να έχει πρόσβαση ένας εξουσιοδοτημένος χρήστης. Η διαχείριση ταυτοποίησης και πρόσβασης (IAM - Identity and Access Management) αποτελεί ένα σημαντικό μέσο για την ασφάλεια στον χώρο του cloud καθώς παρέχει ασφαλή πρόσβαση σε πόρους όπως μηνύματα ηλεκτρονικού ταχυδρομείου, βάσεις δεδομένων, πληροφορίες και εφαρμογές ακόμα και για τους επαληθευμένους χρήστες.

Μέσω των υπηρεσιών IAM, οι διαχειριστές μπορούν να δημιουργήσουν λογαριασμούς χρηστών, να ορίσουν τα δικαιώματα πρόσβασης και να διαχειριστούν τις ρόλους που αντιστοιχούν σε κάθε χρήστη ώστε να

έχουν πρόσβαση μόνο σε όσα χρειάζονται προκειμένου να κάνουν τη δουλεία τους και σε τίποτα περιττό. Οι ρόλοι μπορούν να περιλαμβάνουν διάφορα επίπεδα προνομιακών δικαιωμάτων, όπως πρόσβαση σε συγκεκριμένους πόρους, εκτέλεση συγκεκριμένων ενεργειών και διαχείριση των δικαιωμάτων άλλων χρηστών. Έτσι, αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και η παραβίαση της ασφάλειας του συστήματος. Με το σύστημα IAM ο οργανισμός μπορεί γρήγορα και με ακρίβεια να επαληθεύσει την ταυτότητα ενός ατόμου και να επιβεβαιώσει πως έχει τα απαραίτητα δικαιώματα για να χρησιμοποιήσει ένα συγκεκριμένο πόρο κατά τη διάρκεια μιας προσπάθειας πρόσβασης.

Η διαχείριση ταυτοποίησης και πρόσβασης επιτρέπει επίσης την εφαρμογή πολιτικών ασφαλείας, όπως η απαίτηση χρήσης πολλών παραγόντων (MFA) για την επιβεβαίωση της ταυτότητας των χρηστών πριν από την πρόσβαση σε ευαίσθητα δεδομένα ή πόρους.



***Εικόνα 7**- Διαχείριση ταυτοποίησης και πρόσβασης (IAM)*

Οι υπηρεσίες IAM αποτελούν έναν σημαντικό πυλώνα της ασφάλειας στον χώρο του cloud, επιτρέποντας τη διαχείριση της ταυτότητας και των δικαιωμάτων πρόσβασης των χρηστών, τον έλεγχο της πρόσβασης σε πόρους και δεδομένα, καθώς και την εφαρμογή πολιτικών ασφαλείας για την προστασία του συστήματος και των ευαίσθητων πληροφοριών.

3.2.4 Ελέγχος πρόσβασης και πολιτικές (Access Control and Policies)

Οι πολιτικές πρόσβασης και οι μηχανισμοί ελέγχου πρόσβασης προσδιορίζουν ποιοι χρήστες έχουν πρόσβαση σε ποιους πόρους, πότε και με ποιον τρόπο. Μπορούν να ορίσουν διάφορα επίπεδα πρόσβασης και να εφαρμόζουν κανόνες για τον έλεγχο της πρόσβασης στα δεδομένα και τις υπηρεσίες. Για παράδειγμα, οι πολιτικές μπορούν να ορίζουν ότι ένας χρήστης έχει πρόσβαση μόνο σε συγκεκριμένους φάκελους ή ότι μπορεί να εκτελέσει μόνο συγκεκριμένες ενέργειες σε έναν πόρο, συγκεκριμένες ώρες και από συγκεκριμένες τοποθεσίες.

Οι μηχανισμοί ελέγχου πρόσβασης εφαρμόζουν αυτές τις πολιτικές και ελέγχουν την πρόσβαση των χρηστών σε δεδομένα και υπηρεσίες. Μπορούν να υποστηρίζουν διάφορους μηχανισμούς ελέγχου, όπως χρήση ταυτότητας και κωδικών πρόσβασης, πιστοποιητικών, πιστοποίησης πολλών παραγόντων, κανόνων δικτύου και άλλων τεχνολογιών ασφάλειας. Οι μηχανισμοί αυτοί επαληθεύουν την ταυτότητα των χρηστών και επιτρέπουν ή αποκλείουν την πρόσβασή τους στους πόρους, ανάλογα με τις παραμετροποιήσεις που έχουν. Για να γίνει κατανοητό, μια πολιτική πρόσβασης που βασίζεται σε κανόνες μπορεί να απαγορέψει σε ένα επαληθευμένο χρήστη να προσπελάσει δεδομένα μια ημέρα αργίας ή εκτός του ωραρίου εργασίας του, η αν προσπαθήσει να μπει από χώρα διαφορετική από αυτή που διαμένει.

Οι πολιτικές πρόσβασης και οι μηχανισμοί ελέγχου πρόσβασης συμβάλλουν στη διατήρηση της ασφάλειας και της εμπιστευτικότητας των δεδομένων στον χώρο του cloud. Με τη χρήση αυτών των μηχανισμών, περιορίζεται ο κίνδυνος παραβίασης των δεδομένων και των υπηρεσιών που φιλοξενούνται στο νέφος.

3.2.5 Παρακολούθηση και ανίχνευση απειλών (Monitoring and Threat Detection)

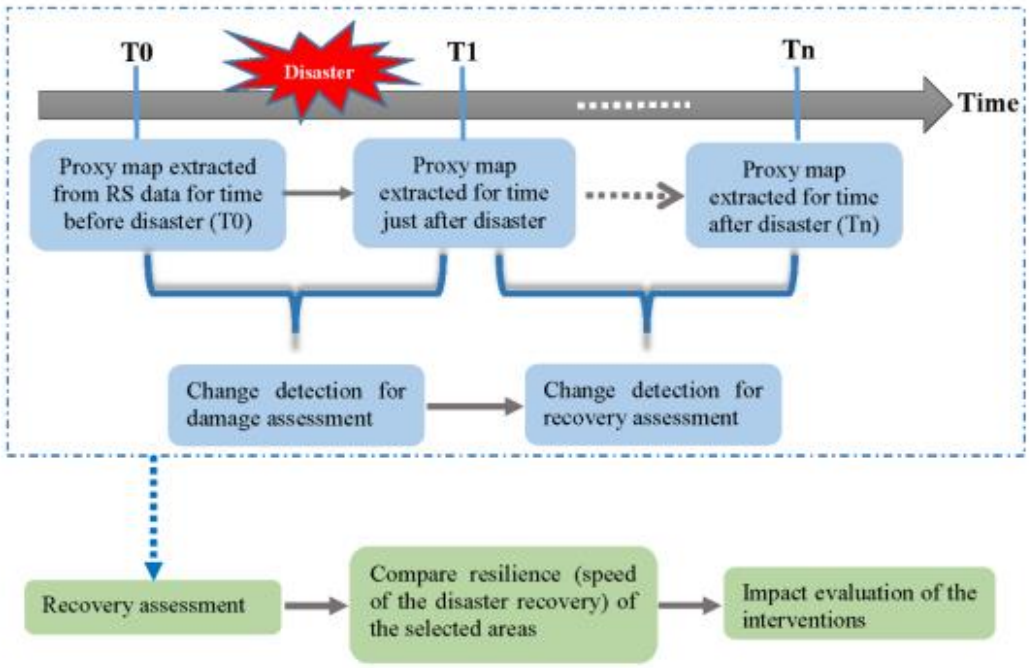
Οι μηχανισμοί παρακολούθησης και ανίχνευσης απειλών παρακολουθούν συνεχώς και σε πραγματικό χρόνο την λειτουργία του νέφους. Στόχος τους είναι να εντοπίσουν έγκαιρα την ύποπτη δραστηριότητα και ανταποκριθούν σε μια ενδεχόμενη κακόβουλη επίθεση. Με την χρήση προηγμένων αλγορίθμων και μοντέλων μηχανικής μάθησης, ανιχνεύονται απειλές όπως DDoS επιθέσεις, εκτέλεση κακόβουλου λογισμικού και προσπάθειες μη εξουσιοδοτημένης πρόσβασης. Οι υπηρεσίες παρακολούθησης και ανίχνευσης απειλών αποτελούν σημαντικό μέρος της ασφάλειας στον χώρο του cloud, καθώς όσο γρηγορότερα γίνει αντιληπτή μια ασυνήθιστη συμπεριφορά, τόσο έγκαιρη θα είναι και η αντιμετώπιση της και τόσο μικρότερη θα είναι η έκταση της ζημιάς που θα προκληθεί.

Για την ανίχνευση απειλών, χρησιμοποιούνται προηγμένοι αλγόριθμοι και ML μοντέλα. Αυτά τα μοντέλα έχουν τη δυνατότητα να αναγνωρίζουν συμπεριφορές και πρότυπα που σχετίζονται με κακόβουλες επιθέσεις. Με την μελέτη και ανάλυση αυτών των δεδομένων και τη σύγκρισή τους με γνωστά μοτίβα, οι μηχανισμοί ανίχνευσης απειλών μπορούν να εντοπίσουν κακόβουλες συμπεριφορές, όπως DDoS επιθέσεις, κακόβουλο λογισμικό, εξουθενωτικές προσπάθειες πρόσβασης και άλλες πιθανές μορφές επιθέσεων.

Η παρακολούθηση και ανίχνευση απειλών συμβάλλει στην άμεση αντίδραση σε απειλές και κακόβουλες επιθέσεις, περιορίζοντας τις επιπτώσεις τους και εξασφαλίζοντας την ακεραιότητα και την αξιοπιστία του νέφους. Επιπλέον, αποτελεί σημαντικό εργαλείο για τον εντοπισμό και την αντιμετώπιση αδικαιολόγητων συμπεριφορών και ανωμαλιών που μπορεί να οφείλονται σε απρόσμενα προβλήματα ή επιθέσεις στο νέφος.

3.2.6 Αποκατάσταση μετά από επίθεση (Post-Attack Recovery)

Η αποκατάσταση μετά από επίθεση αποσκοπεί στην αποκατάσταση των υπηρεσιών και των δεδομένων έπειτα από ένα περιστατικό ασφαλείας. Αυτό περιλαμβάνει την απομόνωση της επίθεσης, την επαναφορά των δεδομένων χρησιμοποιώντας τα αντίγραφα ασφαλείας και την ανασυγκρότηση των πληγέντων συστημάτων.



Εικόνα 9 *– Ανάκαμψη συστήματος cloud μετά από επίθεση*

Η αποκατάσταση μετά από επίθεση αποτελεί σημαντικό στάδιο στη διαχείριση ασφάλειας στον τομέα του cloud. Όταν μια επίθεση λάβει χώρα και προκαλέσει διαταραχές ή ζημιές στις υπηρεσίες και τα δεδομένα, η αποκατάσταση αποσκοπεί στην επαναφορά του συστήματος σε μια ασφαλή και λειτουργική κατάσταση.

Η διαδικασία αποκατάστασης συνήθως περιλαμβάνει τα εξής στάδια:

- Απομόνωση της επίθεσης: Η πρώτη ενέργεια είναι να απομονωθεί η επίθεση και να περιοριστεί η επίδρασή της στο σύστημα. Αυτό μπορεί να περιλαμβάνει την απομάκρυνση του κακόβουλου λογισμικού, ή την απενεργοποίηση των λογαριασμών που σχετίζονται με το περιστατικό.

- Επαναφορά από αντίγραφα ασφαλείας: Ένα σημαντικό μέρος της αποκατάστασης είναι η επαναφορά των δεδομένων από τα αντίγραφα ασφαλείας. Οι πάροχοι υπηρεσιών cloud

διατηρούν συνήθως αντίγραφα ασφαλείας των δεδομένων τους, τα οποία μπορούν να χρησιμοποιηθούν για την ανάκαμψη των πληγέντων πόρων.

- Ανασυγκρότηση πληγέντων συστημάτων: Μετά την επαναφορά των δεδομένων, οι πόροι που επηρεάστηκαν και τα συστήματα πρέπει να ανασυγκροτηθούν. Αυτό περιλαμβάνει την επαναφορά των ρυθμίσεων, των εφαρμογών και των υπηρεσιών που επλήγησαν από την επίθεση.

Ο συνδυασμός αυτών των διαδικασιών συμβάλλει στην επαναφορά των υπηρεσιών και των δεδομένων μετά από μια επίθεση, επαναφέροντας το σύστημα σε ένα ασφαλές και λειτουργικό περιβάλλον. Είναι σημαντικό να διατηρείται ένα επαρκές σύστημα αντιγράφων ασφαλείας και να υπάρχουν σχέδια αποκατάστασης μετά από επιθέσεις, προκειμένου να περιοριστούν οι επιπτώσεις και να ελαχιστοποιηθεί ο χρόνος ανάκαμψης.

3.2.7 Αυτόματη ενημέρωση και διόρθωση του λογισμικού

Οι παρόχοι υπηρεσιών cloud πρέπει να εγκαθιστούν συνεχώς ενημερώσεις και νέες εκδόσεις στα λογισμικά που χρησιμοποιούν, αφού κάθε νέα έκδοση περιλαμβάνει παραμετροποιήσεις ικανές να αντιμετωπίσουν γνωστές απειλές και να διορθώσουν κενά ασφάλειας και πιθανές ευπάθειες των συστημάτων.

Η αυτόματη ενημέρωση και διόρθωση του λογισμικού αποτελεί σημαντική πρακτική στον τομέα του cloud, αφού επιτρέπει στους παρόχους να διατηρούν τις υπηρεσίες τους ενημερωμένες και ασφαλείς. Η διαδικασία αυτή περιλαμβάνει τα παρακάτω:

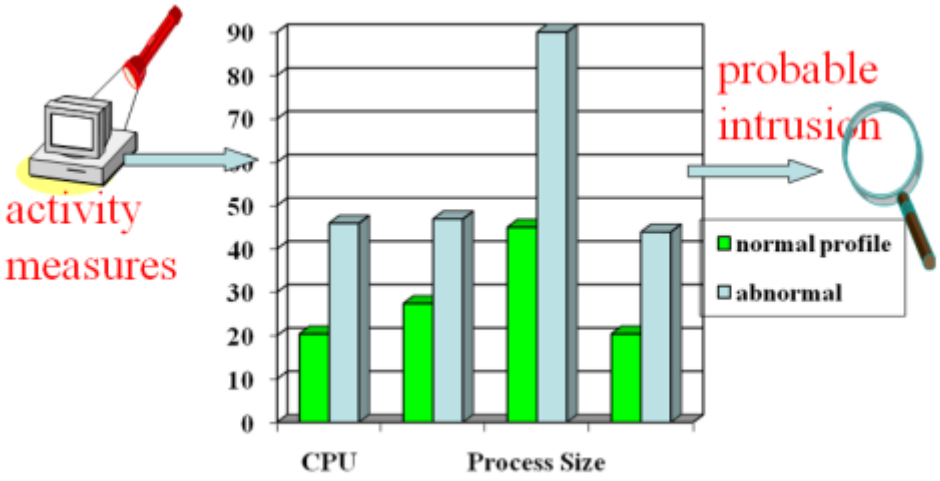
- Συνεχής ενημέρωση: Οι παρόχοι cloud πραγματοποιούν συνεχή ενημέρωση των λογισμικών που χρησιμοποιούν για την παροχή των υπηρεσιών τους. Αυτό σημαίνει ότι τα λογισμικά αναβαθμίζονται και ενημερώνονται με νέες διαθέσιμες εκδόσεις, διορθώσεις γνωστών σφαλμάτων και παραμετροποιήσεις ασφαλείας, προκειμένου να αντιμετωπίζονται συνηθισμένες απειλές και να βελτιώνεται η γενικότερη απόδοση.

- Ευθυγράμμιση με πρότυπα ασφάλειας: Οι παρόχοι υπηρεσιών cloud ενημερώνουν το λογισμικό τους για να συμβαδίζει με τα πρότυπα ασφάλειας και τις βέλτιστες πρακτικές του κλάδου. Αυτό περιλαμβάνει την εφαρμογή απαραίτητων μέτρων ασφαλείας για τη προστασία του δικτύου, την αντιμετώπιση γνωστών ευπαθειών και την υιοθέτηση ενημερωμένων πρωτοκόλλων και αλγορίθμων κρυπτογράφησης.

- Εκτέλεση διορθωτικών ενεργειών: Αν εντοπιστούν κενά ασφαλείας ή ευπάθειες, οι παρόχοι cloud πρέπει άμεσα να προβούν σε διορθωτικές ενέργειες. Αυτές μπορεί να περιλαμβάνουν την εκτέλεση ενημερώσεων ή τη λήψη διορθωτικών πακέτων, την αναδιάταξη της υποδομής ή την αλλαγή των παραμετροποιήσεων ασφαλείας.

3.2.8 Ανίχνευση βασισμένη σε ανωμαλίες (Anomaly Based Detection).

Η ανίχνευση που βασίζεται σε ανωμαλίες (Anomaly Based Detection) συγκρίνει τις γνώριμες δραστηριότητες και συνήθειες των χρηστών στα υπάρχοντα αποθηκευμένα προφίλ ή τη κίνηση των δικτύων για να εντοπίσει τυχόν ασυνήθιστη συμπεριφορά που μπορεί να οφείλεται σε εισβολή. Πιο συγκεκριμένα, στη τεχνική αυτή συλλέγονται δεδομένα που σχετίζονται με την συμπεριφορά των νόμιμων χρηστών ή ενός δικτύου για κάποιο χρονικό διάστημα, και έπειτα τα δεδομένα αυτά αναλύονται προκειμένου να κατασκευαστούν στατιστικά μοντέλα για την τυπική συμπεριφορά των εν λόγω χρηστών ή του δικτύου. Με αυτό τον τρόπο, στη περίπτωση που παρατηρηθούν ενέργειες που αποκλίνουν ή διαφέρουν σημαντικά από τα στατιστικά αυτά μοντέλα, το σύστημα ανίχνευσης απειλών (IDS – Intrusion Detection System) προειδοποιεί ότι γίνεται εισβολή, προκειμένου να ξεκινήσουν άμεσα οι ενέργειες ελέγχου και αντιμετώπισης.



Εικόνα 10 - *Σύστημα ανίχνευσης εισβολής με βάση την εμφάνιση ανωμαλιών*

3.3 Αυθεντικοποίηση και εξουσιοδότηση

Όπως ήδη έχει αναφερθεί, η αυθεντικοποίηση και η εξουσιοδότηση είναι δύο σημαντικές έννοιες που αφορούν στην ασφάλεια και στην προστασία των πόρων στο υπολογιστικό νέφος.

Η αυθεντικοποίηση έχει να κάνει με την επαλήθευση της ταυτότητας ενός χρήστη, η εξουσιοδότηση, από την άλλη πλευρά, αφορά στην διαδικασία παραχώρησης και διαχείρισης των κατάλληλων δικαιωμάτων πρόσβασης στους χρήστες, με βάση την ταυτότητά τους και τις απαιτήσεις τους. Κατά την εξουσιοδότηση, οι πάροχοι υπηρεσιών cloud καθορίζουν τα δικαιώματα πρόσβασης για κάθε χρήστη ή ομάδα χρηστών, περιορίζοντας τις δυνατότητες που έχουν στο νέφος, διασφαλίζοντας έτσι τη προστασία από κακόβουλη χρήση των πόρων.

Για την αυθεντικοποίηση και την εξουσιοδότηση στο υπολογιστικό νέφος, συχνά χρησιμοποιούνται μηχανισμοί όπως πιστοποιητικά, πρωτόκολλα ασφαλούς επικοινωνίας (όπως το SSL - Secure Sockets Layer / TLS - Transport Layer Security), ταυτοποίηση πολλών παραγόντων (MFA) και πολιτικές πρόσβασης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στους πόρους του νέφους.

Οι διαδικασίες αυθεντικοποίησης και εξουσιοδότησης είναι κρίσιμες για την διασφάλιση της ασφάλειας, της εμπιστοσύνης και της αποτελεσματικής λειτουργίας των υπηρεσιών νέφους.

3.4 (Άπο) κρυπτογράφηση δεδομένων

Η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων αποτελούν κρίσιμα μέτρα ασφαλείας στο υπολογιστικό νέφος. Αυτές οι τεχνικές διασφαλίζουν το απόρρητο των δεδομένων αποτρέποντας την μη εξουσιοδοτημένη πρόσβαση και τις παρεμβολές, εξασφαλίζοντας την εμπιστευτικότητα και την ιδιωτικότητα των πληροφοριών που αποθηκεύονται, μεταδίδονται και επεξεργάζονται στο νέφος.

Η κρυπτογράφηση δεδομένων, όπως αναφέρθηκε και νωρίτερα, είναι η διαδικασία μετατροπής κανονικών δεδομένων σε μορφή που είναι ακατανόητη από μη εξουσιοδοτημένους χρήστες. Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν μαθηματικές λειτουργίες για να μετατρέψουν τα δεδομένα σε μια μορφή που είναι δύσκολο να κατανοηθεί χωρίς το απαραίτητο κλειδί. Υπάρχουν δύο βασικοί τύποι κρυπτογράφησης:

- Κρυπτογράφηση Συμμετρικού Κλειδιού: Σε αυτήν τη μέθοδο, τα ίδια κλειδιά χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Ο αποστολέας και ο παραλήπτης πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί. Η κρυπτογράφηση συμμετρικού κλειδιού είναι γρήγορη και αποτελεσματική, αλλά απαιτεί να υπάρχει ένα ασφαλές και απομονωμένο κανάλι επικοινωνίας για τη διανομή του κλειδιού.

- Κρυπτογράφηση Δημόσιου Κλειδιού: Σε αυτήν τη μέθοδο, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Ένα κλειδί, γνωστό ως δημόσιο κλειδί, χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ενώ ένα διαφορετικό κλειδί, γνωστό ως ιδιωτικό κλειδί, χρησιμοποιείται για την αποκρυπτογράφηση. Το δημόσιο κλειδί μπορεί να κατανεμηθεί ευρέως, ενώ το ιδιωτικό κλειδί παραμένει μυστικό. Η κρυπτογράφηση δημόσιου κλειδιού παρέχει μεγαλύτερη ασφάλεια και ευελιξία, αλλά είναι πιο αργή σε σχέση με την κρυπτογράφηση συμμετρικού κλειδιού.

Η αποκρυπτογράφηση είναι η αντίστροφη διαδικασία της κρυπτογράφησης και αφορά στη μετατροπή των κρυπτογραφημένων δεδομένων πίσω στην αρχική τους αναγνώσιμη μορφή. Η αποκρυπτογράφηση γίνεται χρησιμοποιώντας το αντίστοιχο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση.

Η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων στο υπολογιστικό νέφος παρέχουν πολλά πλεονεκτήματα, αλλά και προκλήσεις που πρέπει να ληφθούν υπόψιν. Στα πλεονεκτήματα αξίζει να αναφερθεί πως με τη κρυπτογράφηση επιτυγχάνεται η απόκρυψη ευαίσθητων πληροφοριών, ακόμη και στη περίπτωση που κάποιος κακόβουλα αποκτήσει πρόσβαση στο νέφος, και η προστασία των δεδομένων από τροποποιήσεις και αλλοιώσεις κατά τη μετάδοση ή την αποθήκευσή τους. Στις προκλήσεις θα πρέπει να αναφερθεί πως η (από)κρυπτογράφηση σα διαδικασία επιβαρύνει το σύστημα με επιπλέον υπολογιστικό κόστος, το οποίο ενδεχομένως να επηρεάσει την γενικότερη απόδοσή του, η ανάγκη να προστατευτεί το κλειδί από διαρροή και

να παραμείνει μυστικό, και η επιλογή του κατάλληλου αλγορίθμου ανάλογα με τις ανάγκες και του εκάστοτε παρόχου.

3.5 Παρακολούθηση και ανίχνευση παραβάσεων

Καθώς οι εφαρμογές και τα δεδομένα μεταφέρονται και αποθηκεύονται στο νέφος, είναι σημαντικό να διασφαλίζεται η έγκαιρη ανίχνευση και η αντιμετώπιση πιθανών παραβιάσεων της ασφάλειας.

Η παρακολούθηση περιλαμβάνει τη συλλογή και την ανάλυση δεδομένων από διάφορες πηγές στο νέφος, προκειμένου να εντοπιστούν ενδεχόμενες παραβάσεις ή ανωμαλίες. Αυτό μπορεί να περιλαμβάνει την παρακολούθηση των αρχείων καταγραφής συμβάντων (log files), ή την παρακολούθηση της δραστηριότητας των χρηστών, τις συσκευές τους και άλλα.

Για να επιτευχθεί αποτελεσματική παρακολούθηση και ανίχνευση παραβάσεων, χρησιμοποιούνται ειδικά λογισμικά ασφάλειας. Ορισμένα παραδείγματα ειδικών λογισμικών που χρησιμοποιούνται σε τέτοιες περιπτώσεις περιλαμβάνουν τα συστήματα SIEM (Security Information and Event Management), τα IDS (Intrusion Detection Systems), τα IPS (Intrusion Prevention Systems) και τα HIDS (Host-based Intrusion Detection Systems). Αυτά τα λογισμικά προσφέρουν προηγμένες δυνατότητες παρακολούθησης και ανίχνευσης παραβάσεων σε πραγματικό χρόνο, καθώς και την ικανότητα αντίδρασης σε παραβιάσεις. Τα τελευταία χρόνια τα συστήματα αυτά έχουν εξελιχθεί έτσι ώστε ο εντοπισμός απειλών και η απόκριση σε περιστατικά να γίνεται εξυπνότερα και ταχύτερα χρησιμοποιώντας τεχνητή νοημοσύνη.

Τα ειδικά λογισμικά ασφάλειας απλοποιούν τις ροές εργασιών που σχετίζονται με την ασφάλεια, αφού παρέχουν τις απαραίτητες λειτουργίες για την παρακολούθηση, ανάλυση και ανίχνευση πιθανών παραβάσεων, και λαμβάνουν αποτελεσματικά μέτρα ασφάλειας για την προστασία του υπολογιστικού νέφους και των δεδομένων του.

Κεφάλαιο 4 – Ιδιωτικότητα στις υπηρεσίες νέφους

4.1 Προκλήσεις και απειλές που σχετίζονται με την ιδιωτικότητα

4.1.1 Ο όρος της ιδιωτικότητας

Το θέμα της ιδιωτικότητας, από ηθικής, κοινωνικής και νομικής πλευράς, έχει απασχολήσει φιλοσόφους, επιστήμονες και δικηγόρους σε διάφορες χρονικές περιόδους και σε παγκόσμιο επίπεδο. Το δικαίωμα στην ιδιωτικότητα αναγνωρίστηκε από την παγκόσμια διακήρυξη ανθρωπίνων δικαιωμάτων, την Ευρωπαϊκή σύμβαση για τα ανθρώπινα δικαιώματα και σε διάφορες εθνικές νομοθεσίες.

Ο όρος της ιδιωτικότητας δεν έχει ένα μοναδικό ορισμό και έχει διαφορετική έννοια για κάθε άτομο. Σε κάθε νομικό κείμενο προσεγγίζεται με διαφορετικό τρόπο, και δεν υπάρχει ένας κοινά αποδεκτός ορισμός. Αυτό επιβεβαιώνει την ευρύτητα και την έλλειψη στατικότητας της έννοιας αυτής.

Μια κλασική προσέγγιση αναφέρεται στο άρθρο "The Right to Privacy" των S. Warren και L. Brandeis το 1890, όπου χρησιμοποιήσαν τη φράση "The Right to be left alone" για να περιγράψουν την ιδιωτικότητα του ατόμου. Αυτό το άρθρο ήταν αντίδραση στην αυξανόμενη δημοσιότητα προσωπικών στοιχείων λόγω της εμφάνισης φορητών φωτογραφικών μηχανών και της δημοσίευσής τους σε έντυπα μέσα της εποχής. Σύμφωνα με αυτήν την προσέγγιση, η ιδιωτικότητα περιλαμβάνει την προστασία ιδιωτικών συζητήσεων, την έκφραση σκέψεων και συναισθημάτων, καθώς και τη διασφάλιση των δικαιωμάτων ζωής και ιδιοκτησίας.

Ο Οργανισμός για την οικονομική συνεργασία και ανάπτυξη (OECD - Organisation for Economic Co-operation and Development) όρισε ότι η ιδιωτικότητα αφορά σε οποιαδήποτε πληροφορία σχετίζεται με ένα ταυτοποιημένο ή ταυτοποιήσιμο άτομο (αντικείμενο των δεδομένων).

Η Γενικά Αποδεκτές Αρχές Ιδιωτικότητας (GAPP - Generally Accepted Principles and Practices) που δημιούργησαν το Αμερικανικό Ίδρυμα των πιστοποιημένων δημόσιων λογιστών (AICPA- American Institute of Certified Public Accountants) και το Καναδικό Ίδρυμα Ορκωτών Λογιστών (CICA- Canadian Institute of Chartered Accountants) παρέχει έναν άλλο δημοφιλή ορισμό: "Τα δικαιώματα και οι υποχρεώσεις των ατόμων και των οργανισμών με σεβασμό στη συλλογή, χρήση, διατήρηση και αποκάλυψη των προσωπικών πληροφοριών."

Συνολικά, η ιδιωτικότητα απασχολεί τους φιλοσόφους, τους επιστήμονες και τους δικηγόρους από ηθικής, κοινωνικής και νομικής πλευράς. Έχει αναγνωριστεί ως δικαίωμα σε διεθνή έγγραφα, όπως η Παγκόσμια Διακήρυξη Ανθρωπίνων Δικαιωμάτων (Universal Declaration of Human Rights) και η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα (European Convention on Human Rights), καθώς και σε εθνικές νομοθεσίες που εφάρμοσαν αυτά τα διεθνή έγγραφα σε εθνικό επίπεδο. Παρά το γεγονός ότι δεν υπάρχει ένας μοναδικός αποδεκτός ορισμός, η έννοια της ιδιωτικότητας είναι ευρεία και ευέλικτη.

4.1.2 Προκλήσεις

Η ιδιωτικότητα των δεδομένων αποτελεί ένα από τα κύρια ζητήματα και τη μεγαλύτερη πρόκληση στον τομέα του υπολογιστικού νέφους. Καθώς τα δεδομένα αποθηκεύονται και επεξεργάζονται σε απομακρυσμένους διακομιστές και υπηρεσίες cloud, υπάρχουν πολλές απειλές που μπορούν να θέσουν σε κίνδυνο την ιδιωτικότητα των δεδομένων. Ορισμένες από αυτές τις προκλήσεις και απειλές για τα αντικείμενα των δεδομένων περιλαμβάνουν:

- Ανεπιθύμητη παρακολούθηση: Υπάρχει ο κίνδυνος οι παρόχοι cloud ή άλλοι χρήστες του υπολογιστικού νέφους να παρακολουθούν τα δεδομένα τους χωρίς την έγκρισή τους. Αυτό μπορεί να παραβιάσει την ιδιωτικότητά τους και να αποκαλύψει ευαίσθητες πληροφορίες.

- Κακόβουλη χρήση από εσωτερικούς χρήστες: Οι εργαζόμενοι ή οι administrators των παρόχων cloud μπορεί να έχουν πρόσβαση στα δεδομένα των αντικειμένων και να τα χρησιμοποιήσουν κακόβουλα. Αυτό ισοδυναμεί με παραβίαση της ιδιωτικότητας και κατάχρηση των δεδομένων.

- Αποκάλυψη δεδομένων λόγω κενών ασφάλειας: Οι επιθέσεις στον υπολογιστικό νέφος μπορούν να οδηγήσουν σε γνωστοποίηση δεδομένων λόγω κενών στην ασφάλεια του συστήματος. Αυτό μπορεί να συμβεί λόγω ευπαθειών του λογισμικού ή ανεπαρκών μέτρων προστασίας των δεδομένων.

- Διασπορά δεδομένων: Τα δεδομένα που αποθηκεύονται στο υπολογιστικό νέφος ενδέχεται να αποθηκευτούν σε διάφορες τοποθεσίες και να είναι διάσπαρτα σε πολλούς φυσικούς διακομιστές. Μια τέτοια κατάσταση δυσχεράνει τον έλεγχο και την προστασία των δεδομένων, ειδικά όταν η τοποθεσία στην οποία αποθηκεύονται τα δεδομένα δεν υπόκειται στον έλεγχο ή τους νόμους της χώρας που διαμένει το αντικείμενο των δεδομένων.

Για την αντιμετώπιση αυτών των προκλήσεων και απειλών, είναι σημαντικό να ληφθούν κατάλληλα μέτρα προστασίας των δεδομένων από τη πλευρά του χρήστη. Το αντικείμενο των δεδομένων θα πρέπει να επιλέξει με σωστά κριτήρια τον πάροχο cloud στον οποίο θα αποθηκεύσει τα δεδομένα του και να εφαρμόσει τεχνικές κρυπτογράφησης ή άλλα μέτρα ασφαλείας από μόνος του για να είναι επαρκώς προστατευμένος.

4.2 Τεχνικές προστασίας της ιδιωτικότητας

Έχουν προταθεί διάφορα μέτρα ασφάλειας και τεχνικές για να αποτραπεί η διαρροή και παραβίαση δεδομένων στο νέφος. Μία από αυτές τις τεχνικές είναι η κρυπτογράφηση των δεδομένων προτού αποθηκευτούν στο νέφος και κατά την μετάδοσή τους στο δίκτυο. Η χρήση αποτελεσματικών αλγορίθμων κρυπτογράφησης και η προστασία των κλειδιών στο νέφος είναι κρίσιμες παράμετροι σε αυτήν την περίπτωση όπως αναφέρθηκε και νωρίτερα.

Στις επόμενες σελίδες θα αναλυθούν και θα εξεταστούν οι σημαντικότερες τεχνικές και μέθοδοι για την προστασία της ιδιωτικότητας στο υπολογιστικό νέφος. Ειδικότερα, θα εξεταστούν οι τεχνικές:

- Ανωνυμοποίησης των δεδομένων
- Περιορισμού πρόσβασης στα δεδομένα
- Προστασίας από Account Hijacking.
- Διαγραφής των δεδομένων

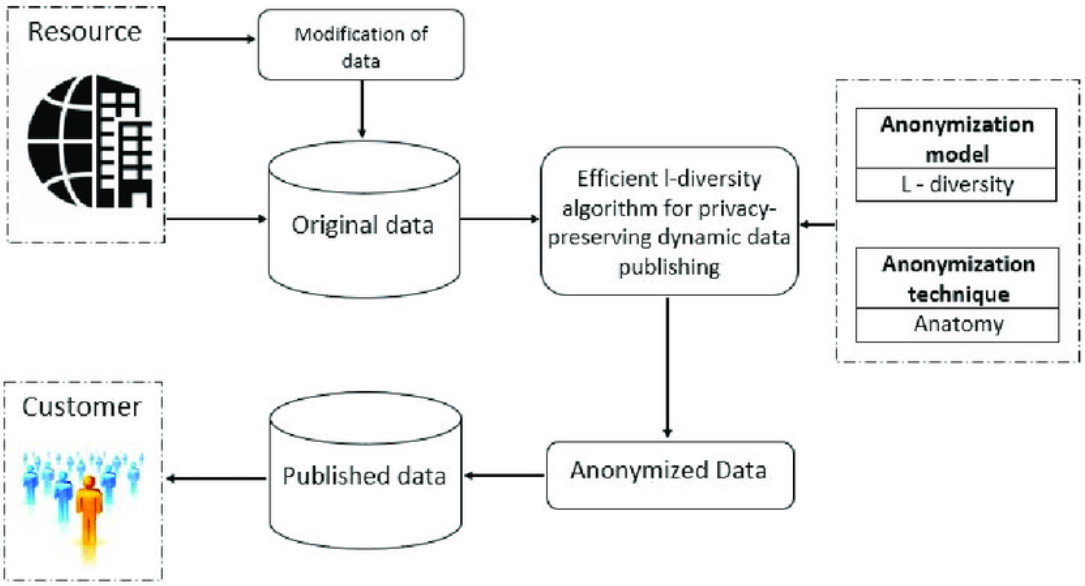
4.3 Ανωνυμοποίηση δεδομένων

Η ανωνυμοποίηση δεδομένων στο cloud αποτελεί μια τεχνική που χρησιμοποιείται για την προστασία της ιδιωτικότητας και τη διασφάλιση του απορρήτου των προσωπικών δεδομένων που αποθηκεύονται και επεξεργάζονται στο νέφος.

Η ανωνυμοποίηση έχει οριστεί ως μια διαδικασία η οποία περιλαμβάνει την απόκρυψη ή την απομάκρυνση των αναγνωριστικών στοιχείων που μπορούν να συσχετιστούν με συγκεκριμένα άτομα ή οντότητες. Η απομάκρυνση των αναγνωριστικών εξασφαλίζει ότι τα δεδομένα παραμένουν ανώνυμα και δεν μπορούν να συσχετιστούν με συγκεκριμένους χρήστες ή οντότητες. Τα δεδομένα τροποποιούνται με τρόπο τέτοιο, ώστε το αντικείμενο των δεδομένων να μη μπορεί πλέον να αναγνωριστεί ούτε άμεσα ούτε έμμεσα, ούτε από τον υπεύθυνο επεξεργασίας ούτε από οποιονδήποτε άλλο. Η ανωνυμοποίηση επιτρέπει τη μεταφορά της πληροφορίας ως ένα βαθμό, ενώ παράλληλα μειώνει το κίνδυνο μιας ακούσιας γνωστοποίησης της.

Η ανωνυμοποίηση των δεδομένων στο υπολογιστικό νέφος έχει τα εξής πλεονεκτήματα: Αρχικά, διασφαλίζει ότι οι προσωπικές πληροφορίες παραμένουν ανώνυμες και δεν μπορούν να αποκαλυφθούν σε μη εξουσιοδοτημένα άτομα ούτε να συσχετιστούν με κάποια οντότητα. Έπειτα, εμποδίζει την αποκάλυψη ευαίσθητων πληροφοριών, όπως είναι τα προσωπικά δεδομένα ή εμπιστευτικές πληροφορίες μιας επιχείρησης. Την ίδια στιγμή όμως, τα δεδομένα αυτά μπορούν να επεξεργασθούν και να αναλυθούν για στατιστικούς σκοπούς χωρίς να αποκαλυφθεί η ταυτότητα ή να επηρεαστεί το αντικείμενο των δεδομένων. Τέλος, η ανωνυμοποίηση συμμορφώνεται με τους κανονισμούς προστασίας δεδομένων.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι η ανωνυμοποίηση δεδομένων δεν εξαλείφει κάθε πιθανότητα ανάκτησης των προσωπικών πληροφοριών, καθώς σε ορισμένες περιπτώσεις είναι δυνατή η συσχέτιση ανωνύμων δεδομένων. Επομένως, πρέπει να ληφθούν υπόψιν οι κατάλληλες τεχνικές και τα κατάλληλα μέτρα προστασίας ώστε να διασφαλιστεί η ιδιωτικότητα και η ασφάλεια των δεδομένων στο cloud.



Εικόνα 11- *Προτεινόμενη μέθοδος ανωνυμοποίησης δεδομένων στο cloud*

4.4 Περιορισμός και έλεγχος πρόσβασης στα δεδομένα

Ο έλεγχος πρόσβασης αποτελεί ένα άλλο σημαντικό μέτρο προστασίας της ιδιωτικότητας στο υπολογιστικό νέφος. Ο έλεγχος πρόσβασης δίνει στους χρήστες συγκεκριμένα δικαιώματα πρόσβασης σε δεδομένα. Αυτό εξασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να αποκτήσουν πρόσβαση στα δεδομένα και να τα επεξεργαστούν. Οι πολιτικές πρόσβασης μπορούν να οριστούν σε επίπεδο ρόλων ή σε επίπεδο χρηστών και να ελέγχονται από τους διαχειριστές.

4.5 Διαγραφή δεδομένων

Η διαγραφή δεδομένων στο cloud ρυθμίζεται από διάφορες νομοθεσίες, ανάλογα με τη χώρα και την περιοχή. Οι πιο γνωστοί κανονισμοί που έχουν να κάνουν με προστασία προσωπικών δεδομένων είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) στην Ευρωπαϊκή Ένωση και ο Νόμος περί Προστασίας των Προσωπικών Πληροφοριών (Personal Information Protection Act - PIPA) στον Καναδά.

Ο GDPR ισχύει για τα προσωπικά δεδομένα που επεξεργάζονται εταιρείες ή οργανισμοί που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση ή παρέχουν υπηρεσίες σε πολίτες της Ευρωπαϊκής Ένωσης. Ο κανονισμός απαιτεί από τις εταιρείες να λαμβάνουν μέτρα για την ασφάλεια και προστασία των προσωπικών δεδομένων, καθώς και να διασφαλίζουν το δικαίωμα των ατόμων για διαγραφή των δεδομένων τους. Σύμφωνα με τον GDPR, οι παρόχοι cloud υπηρεσιών θεωρούνται υπεύθυνοι για την επεξεργασία των δεδομένων και υπόκεινται στις απαιτήσεις του κανονισμού.

Στον Καναδά, ο νόμος PIPA ισχύει για την προστασία των προσωπικών πληροφοριών σε πολυάριθμους ιδιωτικούς τομείς. Οι οργανισμοί που επεξεργάζονται προσωπικά δεδομένα στον Καναδά πρέπει να συμμορφώνονται με τον PIPA και να παρέχουν το δικαίωμα στα άτομα να αιτούνται τη διαγραφή των προσωπικών τους δεδομένων όποτε αυτά το επιθυμούν.

Είναι σημαντικό να σημειωθεί ότι η νομοθεσία περί προστασίας δεδομένων διαφέρει από χώρα σε χώρα και μπορεί να υπάρχουν και άλλοι τοπικοί νόμοι που επηρεάζουν τη διαγραφή δεδομένων στο cloud. Συνιστάται η εξέταση της νομοθεσίας της κάθε χώρας και η αναζήτηση συμβουλών από ένα νομικό ειδικό προκειμένου να διασφαλιστεί η πλήρης κατανόηση των απαιτήσεων και των υποχρεώσεων των ατόμων σχετικά με τη διαγραφή των δεδομένων τους στο cloud.

4.6 Προστασία από Account Highjacking

Ως account hijacking ορίζεται ο έλεγχος των διαδικτυακών λογαριασμών ενός χρήστη από κάποιον μη εξουσιοδοτημένο. Πρόκειται για μια μορφή κλοπής ταυτότητας κατά την οποία ο κακόβουλος χρήστης υποδύεται κάποιον άλλο με σκοπό να συνδεθεί στο λογαριασμό του. Για την προστασία από Account Hijacking, μπορούν να εφαρμοστούν διάφορα μέτρα ασφαλείας στο δίκτυο του νέφους. Αυτά τα μέτρα περιλαμβάνουν τη χρήση συστημάτων ανίχνευσης εισβολής (IDS) στο cloud, που θα επιτηρούν την κυκλοφορία του δικτύου για την ανίχνευση κακόβουλων δραστηριοτήτων. Τα συστήματα ανίχνευσης εισβολής, μαζί με άλλα συστήματα ασφαλείας δικτύου, πρέπει να σχεδιάζονται με γνώμονα την αποτελεσματικότητα του νέφους. Τα συστήματα αυτά βασίζονται κατά κύριο λόγο στις εικονικές μηχανές και χρησιμοποιούν αισθητήρες που βασίζονται στο Snort, ένα γνωστό σύστημα ανίχνευσης εισβολής. Το Snort είναι ένα ελεύθερο και ανοιχτού κώδικα σύστημα ανίχνευσης και πρόληψης εισβολών (Intrusion Detection and Prevention System - IDPS) που χρησιμοποιείται για την ανίχνευση και αντιμετώπιση επιθέσεων σε δίκτυα. Ο βασικός στόχος του Snort είναι να εντοπίζει δραστηριότητες που υποδηλώνουν παραβίαση της ασφάλειας και επιθέσεις από εσωτερικούς ή εξωτερικούς εισβολείς. Τα συστήματα ανίχνευσης εισβολών παρακολουθούν την κατάσταση και τα φορτία των εικονικών μηχανών και μπορούν να κάνουν ενέργειες, όπως εκκίνηση, διακοπή και επαναφορά, ανά πάσα στιγμή.

Για να αντιμετωπιστεί η απειλή του Account Hijacking, μπορεί να χρησιμοποιηθεί και MFA για απομακρυσμένη πρόσβαση. Επιπλέον, η πρόσβαση του χρήστη σε υπηρεσίες και εφαρμογές νέφους πρέπει να εγκρίνεται από τους διαχειριστές του νέφους. Ακόμα, πρέπει να ελέγχονται όλες οι δραστηριότητες των χρηστών με αυξημένα δικαιώματα, καθώς και τα συμβάντα ασφάλειας πληροφοριών που προκαλούνται από αυτές, για να αντιμετωπιστεί αυτή η απειλή.

4.7 Νομοθεσία

Η προστασία των προσωπικών δεδομένων αποτελεί σημαντικό θέμα στη σύγχρονη ψηφιακή εποχή, καθώς η ανάπτυξη τεχνολογιών και η ανάδυση του υπολογιστικού νέφους έχουν επιφέρει σημαντικές αλλαγές στον τρόπο που συλλέγονται, χρησιμοποιούνται και προστατεύονται τα προσωπικά δεδομένα. Στην ενότητα

αυτή θα εξετάσουμε τις κύριες νομοθετικές πράξεις που διέπουν την προστασία των προσωπικών δεδομένων σε παγκόσμιο επίπεδο, με έμφαση στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, τον Νόμο Προστασίας Δεδομένων των Ηνωμένων Πολιτειών και άλλες σημαντικές νομοθεσίες που επηρεάζουν την προστασία των δεδομένων στο υπολογιστικό νέφος.

4.7.1 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) τέθηκε σε ισχύ από την Ευρωπαϊκή Ένωση το 2018. Ο GDPR θεσπίζει ένα ενιαίο πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Θα εξεταστούν οι βασικές αρχές και απαιτήσεις του GDPR, όπως η αρχή της νομιμότητας της επεξεργασίας, η αρχή της διαφάνειας, οι υποχρεώσεις των υπευθύνων επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι μια νομοθετική πράξη που θεσπίστηκε από την Ευρωπαϊκή Ένωση με στόχο την προστασία των προσωπικών δεδομένων των πολιτών. Ο GDPR αποτελεί μια σημαντική νομοθεσία, ιδίως όσον αφορά στον τομέα του υπολογιστικού νέφους, αφού οι υπηρεσίες που βασίζονται στο υπολογιστικό νέφος συχνά εμπλέκουν την επεξεργασία και αποθήκευση μεγάλου όγκου προσωπικών δεδομένων.

Ένας από τους κύριους στόχους του GDPR είναι να διασφαλιστεί ότι οι πολίτες έχουν έλεγχο και διαφάνεια σχετικά με την επεξεργασία των προσωπικών τους δεδομένων. Ο κανονισμός απαιτεί από τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα να λαμβάνουν τη συγκατάθεση των ατόμων και να ενημερώνουν για τον τρόπο που θα χρησιμοποιηθούν τα δεδομένα τους. Αυτό είναι ιδιαίτερα σημαντικό στο υπολογιστικό νέφος, καθώς οι πληροφορίες μπορεί να μεταφέρονται και να αποθηκεύονται σε διάφορες υπηρεσίες και σε διαφορετικές τοποθεσίες.

Επιπλέον, ο GDPR θέτει υψηλά πρότυπα για την ασφάλεια των προσωπικών δεδομένων. Οι φορείς επεξεργασίας που λειτουργούν στο υπολογιστικό νέφος πρέπει να εφαρμόζουν κατάλληλα μέτρα προστασίας για να αποτρέψουν την απώλεια, την κλοπή ή την μη εξουσιοδοτημένη πρόσβαση στα δεδομένα. Αυτό περιλαμβάνει την υιοθέτηση κρυπτογράφησης, την εφαρμογή αυστηρών ελέγχων πρόσβασης και την εκπαίδευση του προσωπικού για τις πρακτικές ασφαλείας. Ακόμη, ο GDPR προβλέπει ότι σε περιπτώσεις παραβίασης της ασφάλειας των δεδομένων, οι υπεύθυνοι επεξεργασίας πρέπει να ειδοποιούνται εντός εύλογου χρονικού διαστήματος. Αυτό βοηθά στην ταχεία αντίδραση σε πιθανές παραβιάσεις και στην προστασία των δεδομένων των πολιτών. Τέλος, ο GDPR θεσπίζει ότι οι πολίτες έχουν το δικαίωμα να ζητούν τη διαγραφή ή την τροποποίηση των προσωπικών τους δεδομένων από τους φορείς επεξεργασίας. Αυτό τους παρέχει έλεγχο και αυτονομία σχετικά με τα δεδομένα τους που επεξεργάζονται στο υπολογιστικό νέφος.

Δικαιώματα του Πολίτη

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) έχει εισάγει βελτιώσεις στις διατάξεις που αφορούν τα δικαιώματα των ατόμων σε σχέση με την πρόσβαση και την προστασία των προσωπικών δεδομένων τους.

- Δικαίωμα στην πληροφόρηση και πρόσβαση: Οι χρήστες έχουν το δικαίωμα να ενημερώνονται για την επεξεργασία των προσωπικών τους δεδομένων και να ζητούν πρόσβαση σε αυτά.

- Δικαίωμα στη διόρθωση: Οι χρήστες μπορούν να ζητούν την διόρθωση τυχόν ανακριβειών στα προσωπικά τους δεδομένα.

- Δικαίωμα στη διαγραφή: Οι χρήστες έχουν το δικαίωμα να ζητούν τη διαγραφή των προσωπικών τους δεδομένων υπό προϋποθέσεις.

- Δικαίωμα στην περιορισμένη επεξεργασία: Οι χρήστες μπορούν να ζητούν τον περιορισμό της επεξεργασίας των προσωπικών τους δεδομένων σε συγκεκριμένες περιπτώσεις.

- Δικαίωμα στη φορητότητα δεδομένων: Οι χρήστες μπορούν να ζητούν τη μεταφορά των προσωπικών τους δεδομένων σε μια άλλη οντότητα ή υπηρεσία.

Οι παραπάνω πτυχές του GDPR αποτελούν σημαντικά βήματα προς την ενίσχυση των δικαιωμάτων και την προστασία των προσωπικών δεδομένων στον τομέα του υπολογιστικού νέφους.

Υποχρεώσεις των φορέων-Παρόχων

Οι πάροχοι cloud αναλαμβάνουν ευθύνη για την προστασία των προσωπικών δεδομένων που αποθηκεύονται και επεξεργάζονται μέσω των υπηρεσιών τους, επομένως έχουν και ορισμένες υποχρεώσεις όσον αφορά στην προστασία των δεδομένων. Οι βασικές υποχρεώσεις τους περιλαμβάνουν:

- Συμμόρφωση με τον νομοθετικό πλαίσιο: Οι πάροχοι cloud πρέπει να συμμορφώνονται με τις νομοθετικές διατάξεις περί προστασίας δεδομένων που ισχύουν στις δικαιοδοσίες όπου λειτουργούν.

- Συμβάσεις επεξεργασίας δεδομένων: Οι πάροχοι cloud πρέπει να συνάπτουν συμβάσεις επεξεργασίας δεδομένων με τους πελάτες τους, καθορίζοντας τους όρους και τις προϋποθέσεις για την επεξεργασία των προσωπικών δεδομένων τους.

- Τεχνικά μέτρα ασφαλείας: Οι πάροχοι cloud πρέπει να λαμβάνουν κατάλληλα τεχνικά μέτρα για την προστασία των προσωπικών δεδομένων που αποθηκεύονται και επεξεργάζονται στις υπηρεσίες τους. Αυτά τα μέτρα περιλαμβάνουν την κρυπτογράφηση των δεδομένων, τον έλεγχο πρόσβασης και την προστασία από απώλεια, κλοπή ή καταστροφή.

- Ενημέρωση και εκπαίδευση: Οι πάροχοι cloud πρέπει να ενημερώνουν τους χρήστες τους για τις πρακτικές που ακολουθούν σχετικά με την προστασία των δεδομένων και να τους παρέχουν την απαραίτητη εκπαίδευση για την ασφαλή χρήση των υπηρεσιών τους.

- Παροχή εργαλείων διαχείρισης δεδομένων: Οι πάροχοι cloud πρέπει να παρέχουν εργαλεία και δυνατότητες διαχείρισης δεδομένων, όπως οι ρυθμίσεις απορρήτου και οι επιλογές διαγραφής δεδομένων, που επιτρέπουν στους χρήστες να ελέγχουν τη χρήση και την προστασία των προσωπικών τους δεδομένων.

Στο νέο κανονισμό GDPR υπάρχουν ενισχυμένες υποχρεώσεις για τους φορείς επεξεργασίας:

- Απαιτήσεις ενημέρωσης: Οι φορείς επεξεργασίας πρέπει να παρέχουν διαφάνεια και πληροφόρηση σχετικά με την επεξεργασία των προσωπικών δεδομένων.

- Απαιτήσεις συγκατάθεσης: Οι φορείς επεξεργασίας πρέπει να λαμβάνουν σαφή συγκατάθεση από τους χρήστες για την επεξεργασία των προσωπικών τους δεδομένων.

- Ανώτατη αρχή ευθύνης: Οι φορείς επεξεργασίας φέρουν την ευθύνη να λαμβάνουν τα αναγκαία μέτρα για την προστασία των προσωπικών δεδομένων και την αποφυγή παραβιάσεων ασφαλείας.

- Διοργανωτικές απαιτήσεις: Οι φορείς επεξεργασίας πρέπει να θεσπίζουν εσωτερικές διαδικασίες και πολιτικές που ασφαλίζουν τη συμμόρφωσή τους προς τον GDPR.

Ανεξάρτητα από το αν οι φορείς επεξεργασίας βρίσκονται εντός ή εκτός της Ευρωπαϊκής Ένωσης, ο GDPR επηρεάζει οποιονδήποτε φορέα που επεξεργάζεται προσωπικά δεδομένα ευρωπαίων πολιτών. Επομένως, ανεξάρτητα από την παγκόσμια τους τοποθεσία, οι φορείς επεξεργασίας πρέπει να συμμορφώνονται με τις απαιτήσεις του GDPR για να διασφαλίσουν την προστασία των προσωπικών δεδομένων.

Κεφάλαιο 5 – Συμπεράσματα

Η παρούσα εργασία είχε ως βασικό αντικείμενο μελέτης την προστασία και την ασφάλεια της ιδιωτικότητας στον τομέα του υπολογιστικού νέφους. Η εμφάνιση του υπολογιστικού νέφους τα τελευταία χρόνια είχε σημαντική επίδραση σε πολλούς τομείς των πληροφοριακών συστημάτων, αφού κατάφερε να κάνει πιο ελκυστικό το λογισμικό (software) που προσφέρεται ως υπηρεσία και να διαμορφώσει τον τρόπο με τον οποίο σχεδιάζεται και πωλείται το υπολογιστικό υλικό (hardware). Οι μεταβολές αυτές που έφερε το υπολογιστικό νέφος επηρεάζουν πολλούς ανθρώπους που το χρησιμοποιούν καθημερινά, χωρίς ενδεχομένως να το συνειδητοποιούν, αλλά και επιχειρήσεις που αποφασίζουν να εγκαταλείψουν τις παραδοσιακές πληροφοριακές εφαρμογές που ήταν πολύπλοκες στη διαχείρισή τους και αρκετά δαπανηρές, για να χρησιμοποιήσουν πλέον

πληροφοριακά συστήματα που συνεργάζονται με το υπολογιστικό νέφος. Το υπολογιστικό νέφος παρέχει πολλά πλεονεκτήματα σε ό,τι αφορά την αποθήκευση, την πρόσβαση και τη διαχείριση δεδομένων. Ωστόσο, υπάρχουν και ορισμένοι κίνδυνοι και αδυναμίες που πρέπει να ληφθούν υπόψιν όταν πρόκειται για την ασφάλεια των δεδομένων στο υπολογιστικό νέφος.

Η προστασία της ιδιωτικότητας στο υπολογιστικό νέφος αποτελεί σημαντικό ζήτημα που απαιτεί την εφαρμογή κατάλληλων τεχνικών και μέτρων προστασίας. Οι προαναφερθείσες τεχνικές, όπως η ενίσχυση της κρυπτογραφίας, ο έλεγχος πρόσβασης, η ανωνυμοποίηση δεδομένων, η παρακολούθηση και ανίχνευση παραβάσεων και οι πολιτικές και διαδικασίες, συμβάλλουν στην προστασία της ιδιωτικότητας και τη διασφάλιση του απορρήτου των δεδομένων στο υπολογιστικό νέφος. Ωστόσο, είναι σημαντικό να σημειωθεί ότι οι τεχνικές προστασίας από μόνες τους δεν αρκούν. Η συνεχής εκπαίδευση των χρηστών, η κατανόηση των προκλήσεων και απειλών που αφορούν στην ιδιωτικότητα, καθώς και η συμμόρφωση προς τους κανονισμούς και τις πρακτικές ασφάλειας είναι εξίσου σημαντικές πτυχές που πρέπει να ληφθούν υπόψιν.

Τέλος, η συνεχής εξέλιξη της τεχνολογίας και η εμφάνιση νέων προκλήσεων στον τομέα της ιδιωτικότητας επιβάλλουν τη διαρκή αξιολόγηση και ενημέρωση σχετικά με τις τεχνικές προστασίας, προκειμένου να διασφαλιστεί η αποτελεσματική προστασία των δεδομένων και της ιδιωτικότητας στο υπολογιστικό νέφος. Σχετικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας στο υπολογιστικό νέφος ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) αποτελεί το βασικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων, ιδίως στο πλαίσιο του υπολογιστικού νέφους. Μέσω του GDPR, θεσπίζονται πρότυπα για τη συλλογή, την επεξεργασία, την αποθήκευση και την προστασία των προσωπικών δεδομένων, ενισχύοντας τα δικαιώματα και την ιδιωτικότητα των πολιτών στο ψηφιακό περιβάλλον.

Στον τομέα του cloud computing, της τεχνητής νοημοσύνης και της ασφάλειας των δεδομένων, υπάρχουν αρκετές προκλήσεις που αναμένεται να αντιμετωπιστούν μελλοντικά.

Πρώτον, η επέκταση του cloud computing θα απαιτεί ακόμα πιο αποτελεσματικά και αξιόπιστα συστήματα διαχείρισης των πόρων. Η αυξανόμενη ζήτηση για υπηρεσίες cloud θα απαιτεί από τους πάροχους να επενδύσουν σε υποδομές μεγάλης κλίμακας και να βελτιώσουν την απόδοση και την ανεκτικότητα σε σφάλματα.

Δεύτερον, η τεχνητή νοημοσύνη απαιτεί αυξημένη υπολογιστική ισχύ και αποθηκευτικούς πόρους. Οι αλγόριθμοι μηχανικής μάθησης και άλλες τεχνικές τεχνητής νοημοσύνης χρειάζονται μεγάλες ποσότητες δεδομένων και υπολογιστική ισχύ για να εκπαιδευτούν και να λειτουργήσουν αποτελεσματικά. Οι πάροχοι cloud θα πρέπει να αναβαθμίσουν τις υποδομές τους για να υποστηρίξουν αυτές τις απαιτήσεις.

Τρίτον, η ασφάλεια των δεδομένων αποτελεί μια τεράστια πρόκληση. Καθώς οι οργανισμοί αποθηκεύουν και επεξεργάζονται ολοένα και περισσότερα ευαίσθητα δεδομένα στο cloud, η ανάγκη για αποτελεσματικές τεχνικές ασφάλειας γίνεται όλο και πιο επιτακτική. Είναι ανάγκη να ληφθούν προηγμένα

μέτρα ασφάλειας για την προστασία των δεδομένων από απειλές όπως την κακόβουλη πρόσβαση, τις επιθέσεις και τις διαρροές.

Η ασφάλεια στο υπολογιστικό νέφος είναι ένα σύνθετο θέμα και εξαρτάται από πολλούς παράγοντες, όπως η σωστή διαμόρφωση των υπηρεσιών, η χρήση κρυπτογράφησης, η προστασία πρόσβασης, οι διαδικασίες ελέγχου, η παρακολούθηση κίνησης δεδομένων κ.ά. Οι πάροχοι cloud υπηρεσιών και οι χρήστες πρέπει να λάβουν σοβαρά υπόψιν την ασφάλεια και να υιοθετούν συνεχώς βελτιώσεις για να αντιμετωπίσουν τους κινδύνους ασφαλείας που ενδέχεται να υπάρχουν.

Τέλος, η πολιτική και νομική ρύθμιση αποτελεί επίσης πρόκληση. Οι οργανισμοί και οι πάροχοι cloud θα πρέπει να συμμορφώνονται με τους νομικούς κανονισμούς για την προστασία της ιδιωτικότητας, τη μεταφορά δεδομένων και άλλα ζητήματα που αφορούν την ασφάλεια και την προστασία των δεδομένων. Οι προκλήσεις στο cloud computing, την τεχνητή νοημοσύνη και την ασφάλεια των δεδομένων είναι πολυποίκιλες και απαιτούν συνεχή προσαρμογή και καινοτομία για να διασφαλιστεί η αξιοπιστία, η απόδοση και η προστασία των υπηρεσιών και των δεδομένων στο μέλλον.

5.1 Μελλοντικές προκλήσεις

Ορισμένες από τις κύριες προκλήσεις ασφαλείας που αναμένεται να αντιμετωπιστούν στο cloud περιλαμβάνουν:

1. Νέες επιθέσεις και ευπάθειες μηδενικής ημέρας (zero day attacks): Οι κακόβουλοι χρήστες θα δημιουργούν συνεχώς νέες μεθόδους επιθέσεων και θα αναζητούν ευπάθειες μηδενικές ημέρας (zero-day vulnerabilities) που δεν έχουν γίνει γνωστές ακόμη ούτε έχουν ανιχνευτεί ή διορθωθεί.

2. Ανθρώπινο λάθος: Ο ανθρώπινος παράγοντας εξακολουθεί να είναι μια σημαντική πρόκληση στην ασφάλεια. Οι ανθρώπινοι χρήστες μπορεί να κάνουν λάθη όπως χρήση αδύναμων κωδικών ασφαλείας, ανοικτή πρόσβασης σε δεδομένα, ή να πέσουν θύματα απάτης.

3. Ασφάλεια πολυμετοχικού cloud: Πολλοί οργανισμοί χρησιμοποιούν πολυμετοχικά cloud, όπου συνδυάζουν δημόσια, ιδιωτικά και υβριδικά cloud. Αυτό δημιουργεί προκλήσεις στην ενοποίηση των μέτρων ασφαλείας και στον έλεγχο κάθε ενός περιβάλλοντος.

4. Επιθέσεις στις εικονικές μηχανές: Η χρήση εικονικών μηχανών ανοίγει νέους τρόπους επιθέσεων.

Οι παρόχοι cloud και οι χρήστες πρέπει να επικεντρωθούν στην ασφάλεια, να ενημερώνονται για τις τελευταίες απειλές και να υιοθετούν κατάλληλες προσεγγίσεις για να προστατεύουν τα δεδομένα και τις εφαρμογές τους στο cloud.

Αναφορές – Βιβλιογραφία

1 A., Lavender & Elisha, Oderinde. (2019). The Use of Biometrics in Multifactor Authentication (MFA) for Cloud Computing Data Storage. International Journal of Computer Applications. 178. 30-37. 10.5120/ijca2019919025.

2 Abdulsalam, Yunusa & Hedabou, Mustapha. (2021). Security and Privacy in Cloud Computing: Technical Review. Future Internet. 14. 11. 10.3390/fi14010011.

3 Ahmad, Sultan & Afzal, Mohammad. (2018). A Review of Assured Data Deletion Mechanism in Cloud Computing. International Journal of Engineering and Technology(UAE). 7. 10.14419/ijet.v7i4.5.20101.

4 Annappaiah, Dinesha & Agrawal, V.K.. (2012). Multi-level Authentication Technique for Accessing Cloud Services. 10.1109/ICCCA.2012.6179130.

5 Firdhous, Mohamed & Husieen, Naseer. (2018). Data Security Implementations in Cloud Computing: A Critical Review. 1-5. 10.1109/ICITR.2018.8736153.

6 BRUMA, Lidia. (2020). Data Security Methods in Cloud Computing. Informatica Economica. 24. 48-60. 10.24818/issn14531305/24.1.2020.05.,

7 Kire. (2016). Security Techniques for Data Protection in Cloud Computing. International Journal of Grid and Distributed Computing. 9. 49-56. 10.14257/ijgdc.2016.9.1.05.

8 Akram, Waseem. (2019). A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography).

9 Alenizi, Bayan & Humayun, Mamoona & Jhanjhi, Noor. (2021). Security and Privacy Issues in Cloud Computing. Journal of Physics: Conference Series. 1979. 012038. 10.1088/1742-6596/1979/1/012038.

10 Ali, Mohammed & Barnawi, Ahmed & Bashar, Abul. (2012). Modeling and Simulation Strategies for Performance Evaluation of Cloud Computing Systems.

11 Association, Information & Sen, Jaydip. (2015). Security and Privacy Issues in Cloud Computing. 10.4018/978-1-4666-6539-2.ch074.

12 Ayache, Meryeme & Erradi, Mohamed & Freisleben, Bernd. (2015). Access control policies enforcement in a cloud environment: Openstack. 26-31. 10.1109/ISIAS.2015.7492740.

13 Bairagi, Swati & Bang, Ankur. (2015). Cloud Computing: History, Architecture, Security Issues.

14 Balani, Zina & Varol, Hacer. (2020). Cloud Computing Security Challenges and Threats. 1-4. 10.1109/ISDFS49300.2020.9116266.

15 Batman, Ayse Necibe. (2019). European Cloud Service Data Protection Certification. 10.1007/978-94-6265-279-8_14.

16 Bentil, Felix & Lartey, Isaac. (2021). Cloud Cryptography -A Security Aspect. Volume 10.

17 Bhagat, Babita & Khobragade, Shrutika & Arudkar, Archana. (2023). The Evolution of Cloud Computing.

18 Bhardwaj, Akashdeep & Goundar, Sam. (2020). Cloud Computing Security Services to Mitigate DDoS Attacks. 10.5772/intechopen.92683.

19 Bhargav, A. & Manhar, Advin. (2020). A Review on Cryptography in Cloud Computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 225-230. 10.32628/CSEIT206639.

20 Bk, Jeevitha & Thriveni, J. & K R, Venugopal. (2016). Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey. International Journal of Computer Applications. 156. 16-27. 10.5120/ijca2016912513.

21 Brohi, Sarfraz & Bamiah, Mervat. (2013). Challenges and Benefits for Adopting the Paradigm of Cloud Computing.

22 Brugman, Jonathon & Khan, Mohammed & Kasera, Sneha & Parvania, Masood. (2019). Cloud Based Intrusion Detection and Prevention System for Industrial Control Systems Using Software Defined Networking. 98-104. 10.1109/RWS47064.2019.8971825.

23 Chagarlamudi, Gnana. (2020). Challenges and threats in cloud security. International Journal of Cloud Computing. 1. 1.

24 Chandra Jadala, Dr. (2019). Authentication and Authorization Mechanism for Cloud Security. 10.35940/ijeat.F8473.088619.

25 Chiba, Zouhair & Abghour, Noreddine & Moussaid, Khalid & Omri, Amina & Rida, Mohamed. (2018). A Review of Intrusion Detection Systems in Cloud Computing. 10.4018/978-1-5225-5736-4.ch012.

26 Contreras Mojica, Diana & Wilkinson, Sean & Balan, Nipun & James, Philip. (2021). Assessing post-disaster recovery using sentiment analysis: The case of L'Aquila, Italy. Earthquake Spectra. 38. 875529302110364. 10.1177/87552930211036486.

27 Dai, Xue & Wang, Zhao & Zhang, Yan. (2013). Data Security and Privacy Protection of Cloud Computing. Advanced Materials Research. 846-847. 1570-1573. 10.4028/www.scientific.net/AMR.846-847.1570.

28 Darwish, Marwan. (2018). Privacy and Security of Cloud Computing: A Comprehensive Review of Techniques and Challenges.

29 David, Tolu & Akande,. (2020). Privacy and Security in Cloud Computing.

30 Dhasaratham, M & Singh, R. (2018). A Survey on Data Anonymization Using Mapreduce on Cloud with Scalable Two-Phase Top-Down Approach. International Journal of Engineering & Technology. 7. 254. 10.14419/ijet.v7i2.20.14773.

31 Eldred, Mike & Adams, Carl & Good, Alice. (2019). Impact of EU Data Protection Laws on Cloud Computing: Capturing Cloud-Computing Challenges and Fault Lines. 10.4018/978-1-5225-7501-6.ch097.

32 George, Reenu & Sivan, Sabitha. (2013). Data anonymization and integrity checking in cloud computing. 1-5. 10.1109/ICCCNT.2013.6726813.

33 Gill, Sajid & Abdur Razzaq, Mirza & Ahmad, Muneer & Almansour, Fahad & Ul Haq, Ikram & Jhanjhi, Noor & Zaib, Malik & Masud, Mehedi. (2021). Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study. Intelligent Automation and Soft Computing. 31. 117-128. 10.32604/iasc.2022.016597.

34 Huang, Michelle. (2020). Privacy and Data Protection in the Digital Era: The Global v. National Scope.

35 kaur, Sandeep & Kaur, Gaganpreet & Shabaz, Dr. Mohammad. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. Security and Communication Networks. 2022. 1-9. 10.1155/2022/7540891.

36 Kertész, Attila & Váradi, Szilvia. (2014). Legal Aspects of Data Protection in Cloud Federations. 10.1007/978-3-642-38586-5_15.

37 Kertész, Attila & Váradi, Szilvia. (2014). Legal Aspects of Data Protection in Cloud Federations. 10.1007/978-3-642-38586-5_15.

38 Laskey, Kathryn & Laskey, Kenneth. (2009). Service oriented architecture. Wiley Interdisciplinary Reviews: Computational Statistics. 1. 101 - 105. 10.1002/wics.8.

39 Manning, Colin. (2016). Challenges Posed by Big Data to European Data Protection Law. SSRN Electronic Journal. 10.2139/ssrn.2728624.

40 Mathur, Priya & Gupta, Amit & Vashishtha, Prateek. (2019). Comparative Study of Cryptography for Cloud Computing for Data Security. Recent Advances in Computer Science and Communications. 13. 10.2174/2666255813666190911114909.

41 Mehmood, Yasir & Shibli, Awais & Habiba, Umme & Masood, Rahat. (2013). Intrusion Detection System in Cloud Computing: Challenges and opportunities. Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013. 59-66. 10.1109/NCIA.2013.6725325.

42 Mohammad, Abdulghafour. (2022). Distributed Authentication and Authorization Models in Cloud Computing Systems: A Literature Review. Journal of Cybersecurity and Privacy. 2. 107-123. 10.3390/jcp2010008.

43 Morol, Md. Kishor & Das, Shuvra Smaran. (2022). Data Security and Privacy in Cloud Computing Platforms: A Comprehensive Review. International Journal of Current Science Research and Review. 05. 10.47191/ijcsrr/V5-i5-09.

44 Mothomela, Dimpho. (2020). An Evaluation of Multifactor Authentication Schemes in Cloud Data Security AN EVALUATION OF MULTIFACTOR AUTHENTICATION SCHEMES IN CLOUD DATA SECURITY.

45 Muthumayil, Buvana & Muthumayil, K & Rajinikannan, M & Thangaiyan, Jayasankar & Prof, Asst. (2021). Optimize Cryptography Algorithm for Efficient Data Security on Cloud Computing. 12. 459-464.

46 Nizamuddin, Nishara & Pandey, Reeta. (2015). Enhancing Security in Public Clouds using Data Anonymization Techniques. International Journal of Computer Applications. 128. 33-36. 10.5120/ijca2015906428.

47 Pai, Vaikunth & Aithal, Sreeramana. (2016). Cloud Computing Security Issues - Challenges and Opportunities. International Journal of Management, Technology, and Social Sciences. 33-42. 10.47992/IJMTS.2581.6012.0004.

48 Pandey, Dr-Ashish & Boddu, Raja & Tiwari, Mohit & Tiwari, Tripti. (2021). AN ANALYSIS OF DATA SECURITY AND PRIVACY IN CLOUD COMPUTING.

49 Raj, Anushree & D'Souza, Rio. (2019). Big Data Anonymization in Cloud using k-Anonymity Algorithm using Map Reduce Framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 50-56. 10.32628/CSEIT19516.

50 Russo, Barbara & Valle, Laura & Bonzagni, Guido & Locatello, Davide & Pancaldi, Marta & Tosi, Davide. (2018). Cloud Computing and the New EU General Data Protection Regulation. IEEE Cloud Computing. 5. 58-68. 10.1109/MCC.2018.064181121.

51 S, Priya & Ponmagal, Dr. (2022). IDS Based threat monitoring in Cloud Computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 108-114. 10.32628/CSEIT228110.

52 Salomoni, Davide & Campos Plasencia, Isabel & Gaido, Luciano & Donvito, Giacinto & Fuhrmann, Patrick & Marco de Lucas, Jesus & Lopez Garcia, Alvaro & Orviz Fernandez, Pablo & Blanquer, Ignacio & Moltó, Germán & Plociennik, M. & Owsiak, Michal & Urbaniak, M. & Hardt, M. & Ceccanti, Andrea & Wegh, B. & Gomes, Jose & David, Mario & Alves, Luís & Viljoen, M.. (2017). INDIGO-DataCloud: Project Achievements.

53 Shahzadi, Sonia & Iqbal, Muddesar & Qayyum, Zia & Dagiuklas, Tasos. (2017). Infrastructure as a Service (IaaS): A Comparative Performance Analysis of Open-Source Cloud Platforms. 10.1109/CAMAD.2017.8031522.

54 Somani, Gaurav & Gaur, Manoj & Sanghi, Dheeraj & Conti, Mauro & Buyya, Rajkumar. (2015). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. Computer Communications. 107. 10.1016/j.comcom.2017.03.010.

55 Spalevic, Zaklina & Vićentijević, Kosana. (2022). GDPR and challenges of personal data protection. The European Journal of Applied Economics. 19. 55-65. 10.5937/EJAE19-36596.

56 Suliman, Mohammed. (2021). A Brief Analysis of Cloud Computing Infrastructure as a Service(IaaS). 6. 1409-1412.

57 Sun, Yunchuan & Zhang 张均胜, Junsheng & Xiong, Yongping & Zhu, Guangyu. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014. 1-9. 10.1155/2014/190903.

58 Surbiryala, Jayachander & Rong, Chunming. (2019). Cloud Computing: History and Overview. 1-7. 10.1109/CloudSummit47114.2019.00007.

59 Temuujin, Odsuren & Ahn, Jinhyun & Im, Dong-Hyuk. (2019). Efficient L-Diversity Algorithm for Preserving Privacy of Dynamically Published Datasets. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2936301.

60 Verma, Amandeep & Kaushal, Sakshi. (2018). Cloud Computing Security Issues and Challenges: A Survey. 445-454. 10.1007/978-3-642-22726-4_46.

61 Vidović, Marina. (2016). EU Data Protection Reform: Challenges for Cloud Computing. Croatian Yearbook of European Law and Policy. 12. 171-206. 10.3935/cyelp.12.2016.252.

62 Vranaki, Asma. (2016). Cloud Investigations by European Data Protection Authorities: An Empirical Account. 10.4337/9781783479924.00045.

63 Yang, Zhanpeng & Feng, Qiaobin & Jiang, Jinglan & Chen, Qiyu. (2020). Fine-grained outsourced data deletion in cloud storage. Journal of Physics: Conference Series. 1656. 012025. 10.1088/1742-6596/1656/1/012025.

64 Zharova, Anna. (2015). The salient features of personal data protection laws with special reference to cloud technologies. A comparative study between European countries and Russia. Applied Computing and Informatics. 12. 10.1016/j.aci.2015.07.001.

65 Zhou, Minqi & Zhang, Rong & Xie, Wei & Qian, Weining & Zhou, Aoying. (2010). Security and Privacy in Cloud Computing: A Survey. Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference On. 105 - 112. 10.1109/SKG.2010.19.