Πανεπιστήμιο Θεσσαλίας
Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών:
«Μηχανική Λογισμικού για Διαδικτυακές & Φορητές Εφαρμογές»

Μεταπτυχιακή Διπλωματική Εργασία

Διασφάλιση ποιότητας υπηρεσιών υπολογιστικού νέφους (SLA)

ΛΑΜΠΡΟΥ ΦΙΛΙΤΣΑ

Επιβλέπων Καθηγητής: Σάββας Ηλίας

Λάρισα, 2023

Περίληψη

Η ασφάλεια των δεδομένων είναι σταθερά ένα σημαντικό ζήτημα στην τεχνολογία των πληροφοριών. Στο περιβάλλον υπολογιστικού νέφους, γίνεται ιδιαίτερα σοβαρό επειδή τα δεδομένα βρίσκονται σε διαφορετικά σημεία ακόμη και σε όλο τον κόσμο. Η ασφάλεια των δεδομένων και η προστασία του απορρήτου είναι οι δύο κύριοι παράγοντες ανησυχίας των χρηστών σχετικά με την τεχνολογία cloud. Αν και πολλές τεχνικές σχετικά με τα θέματα του cloud computing έχουν διερευνηθεί τόσο σε ακαδημαϊκούς όσο και σε βιομηχανίες, η ασφάλεια δεδομένων και η προστασία της ιδιωτικής ζωής γίνονται πιο σημαντικές για τη μελλοντική ανάπτυξη της τεχνολογίας cloud computing στην κυβέρνηση, τη βιομηχανία και τις επιχειρήσεις. Τα θέματα ασφάλειας δεδομένων και προστασίας απορρήτου σχετίζονται τόσο με το υλικό όσο και με το λογισμικό στην αρχιτεκτονική του cloud. Αυτή η μελέτη έχει σκοπό να επικεντρωθεί με βάση τον τρόπο που αναπτύσσονται τα κεφάλαια και να εξηγήσει τι είναι το cloud computing, κάνοντας και μια ιστορική αναδρομή για να παρατηρήσουμε την εξέλιξή του. Στη συνέχεια, θα ασχοληθούμε με την αρχιτεκτονική του cloud computing και θα αναφέρουμε τα πλεονεκτήματα και τα μειονεκτήματα που εντοπίζονται κατά τη χρήση του. Θα γίνει αναφορά σχετικά με τη νομοθεσία που υπάρχει για τη χρήση του, τους τρόπους προστασίας των δεομένων και τις μελλοντικές εξελίξεις.

Λέξεις κλειδιά: Cloud computing, προστασία δεδομένων, SLA

Abstract

Data security is consistently an important issue in information technology. In the cloud computing environment, it becomes especially serious because the data resides in different places even around the world. Data security and privacy protection are the two main concerns of users regarding cloud technology. Although many techniques related to cloud computing issues have been explored in both academics and industries, data security and privacy are becoming more important for the future development of cloud computing technology in government, industry and enterprises. Data security and privacy concerns relate to both hardware and software in the cloud architecture. This study is intended to focus, based on how the chapters are developed and explain what cloud computing is, also taking a historical look back to observe its evolution. Next, we will deal with the architecture of cloud computing and mention the advantages and disadvantages found when using it. A reference will be made regarding the legislation that exists for its use, the ways of data protection and future developments.

Keywords: Cloud computing, data privacy, SLA

Περιεχόμενα

Κεφάλαιο 1: Υπολογιστικό Νέφος

1.1 Εισαγωγή

Ζούμε και λειτουργούμε στον κόσμο των υπολογιστών και του διαδικτύου. Το Διαδίκτυο έχει αλλάξει δραστικά τον κόσμο των υπολογιστών από την έννοια του παράλληλου υπολογισμού, στον κατανεμημένο υπολογισμό, μετά στον υπολογισμό πλέγματος και τώρα στο υπολογιστικό νέφος. Το cloud computing είναι ένα νέο κύμα στον τομέα της πληροφορικής. Κάποιοι το βλέπουν ως ένα αναδυόμενο πεδίο στην επιστήμη των υπολογιστών. Αποτελείται από ένα σύνολο πόρων και υπηρεσιών που προσφέρονται μέσω του Διαδικτύου. Ως εκ τούτου, το υπολογιστικό σύννεφο, ονομάζεται επίσης και Internet computing (Rajaraman, 2014). Η λέξη «σύννεφο» είναι μια μεταφορά για την περιγραφή του ιστού ως ενός χώρου όπου η πληροφορική έχει προεγκατασταθεί και υπάρχει ως υπηρεσία. Λειτουργικά συστήματα, εφαρμογές, αποθήκευση, δεδομένα και ικανότητα επεξεργασίας υπάρχουν όλα στον Ιστό, έτοιμα για κοινή χρήση μεταξύ των χρηστών.

Το cloud computing έχει κάνει μια σημαντική ανακάλυψη στον τομέα της πληροφορικής. Με την εμφάνισή του, έφερε πραγματικά επανάσταση στην πληροφορική. Έχει παίξει σημαντικό ρόλο στην τροφοδοσία για αυξανόμενες απαιτήσεις για αποθήκευση και υποδομή. Η εξαιρετική ικανότητα του cloud είναι ότι παρέχει πόρους, όπως υλικό και λογισμικό μέσω δικτύου. Εκεί υπάρχει αριθμός πόρων στο cloud computing που μπορούν να προσληφθούν με βάση την αμοιβή ανά χρήση (Rajaraman, 2014). Σε γενικές γραμμές μπορούμε να διακρίνουμε το σύννεφο ως:

- ✓ Ιδιωτικό σύννεφο: Αυτός ο τύπος cloud λειτουργεί για μια καθορισμένη οργάνωση ή επιχείρηση, π.χ. σύννεφο για μια συγκεκριμένη οργάνωση.
- ✓ Δημόσιο σύννεφο: Τα δημόσια σύννεφα είναι εύκολα διαθέσιμα από Google, Amazon, Microsoft κ.λπ. Το δημόσιο cloud παρέχει υποδομές και υπηρεσίες προς το κοινό ή οποιονδήποτε οργανισμό. Οι πόροι μοιράζονται σε εκατοντάδες ή χιλιάδες άτομα.
- ✓ Σύννεφο κοινότητας: Σε ένα σύννεφο κοινότητας οι υπηρεσίες παρέχουν υποδομή σε οργανισμούς με παρόμοια ενδιαφέροντα.
- ✓ Υβριδικό σύννεφο: Αυτός ο τύπος σύννεφου είναι ένα μείγμα ιδιωτικού και δημόσιου. Αν και τα σύννεφα είναι ανακατεμένα, ακόμα το καθένα έχει την ατομική του ταυτότητα και επομένως βοηθά πολλαπλά στην ανάπτυξη.

Ο κύριος στόχος του υπολογιστικού νέφους είναι η καλύτερη χρήση των κατανεμημένων πόρων και η επίλυση προβλημάτων υπολογισμού μεγάλης κλίμακας. Για παράδειγμα, το cloud computing μπορεί να εστιάσει τη δύναμη χιλιάδων υπολογιστών σε ένα πρόβλημα, να κινητοποιήσει ερευνητές να κάνουν τη δουλειά τους πιο γρήγορα. Έτσι, το cloud computing μπορεί να θεωρείται ως ένα κατανεμημένο σύστημα που προσφέρει υπολογιστικές υπηρεσίες μέσω υπολογιστή σε ένα δίκτυο επικοινωνίας, συνήθως το Διαδίκτυο (TCP/IP). Πόροι στο σύννεφο είναι διαφανείς στους χρήστες και δεν χρειάζεται να γνωρίζουμε την ακριβή τοποθεσία των πόρων αυτών (Almorsy, Grundy & Müller, 2016). Μπορούν να μοιραστούν μεταξύ τους μεγάλους αριθμούς χρηστών, που θα έπρεπε να έχουν δυνατότητα πρόσβασης σε εφαρμογές και δεδομένα από οπουδήποτε και ανά πάσα στιγμή.

1.2 Τι είναι το υπολογιστικό νέφος

Το cloud computing, ένας όρος που συχνά συγκρίνεται με το ηλεκτρονικό εμπόριο, είναι μια από τις πιο αινιγματικές τεχνικές έννοιες στην ιστορία. Υπάρχουν δύο λόγοι για αυτό: πρώτον, το cloud computing είναι εξαιρετικά προσαρμόσιμο και μπορεί να χρησιμοποιηθεί σε πολλά σενάρια εφαρμογών, και δεύτερον, διαφημίζεται έντονα από εταιρείες για προώθηση επιχειρήσεων (Rajaraman, 2014). Το Hyper Cycle του Ομίλου Gartner, που δημοσιεύτηκε το 2008, σημείωσε ότι το cloud computing γνώριζε ταχεία ανάπτυξη. Ο John McCarthy αναφέρθηκε στις θεμελιώδεις αρχές του cloud computing στην ομιλία του στο MIT Centennial το 1961, δηλώνοντας ότι «Το βοηθητικό πρόγραμμα υπολογιστών θα μπορούσε να γίνει η βάση μιας νέας και σημαντικής βιομηχανίας». Ωστόσο, ο όρος "υπολογιστικό σύννεφο" όπως τον γνωρίζουμε σήμερα πιθανότατα εισήχθη για πρώτη φορά από τον Eric Schmidt κατά τη διάρκεια της ομιλίας του σχετικά με τις στρατηγικές μηχανών αναζήτησης σε ένα συνέδριο το 2006.

Το cloud computing έχει πλέον πολλούς ορισμούς και μεταφορές. Από την άποψή μας, το cloud computing είναι μια υπολογιστική τεχνολογία στην οποία οι υπηρεσίες πληροφορικής παρέχονται από τεράστιες υπολογιστικές μονάδες χαμηλού κόστους συνδεδεμένες σε δίκτυα IP (Almorsy, Grundy & Müller, 2016). Το cloud computing έχει τις ρίζες του στο σχεδιασμό πλατφόρμας μηχανών αναζήτησης. Το cloud computing έχει 5 κύρια τεχνικά χαρακτηριστικά:

- ✓ Υπολογιστικοί πόροι μεγάλης κλίμακας

- ✓ Υψηλή ελαστικότητα και επεκτασιμότητα
- ✓ Κοινό σύνολο πόρων (εικονικοί και φυσικοί πόροι)
- ✓ Δυναμικός προγραμματισμός πόρων
- ✓ Γενικού σκοπού

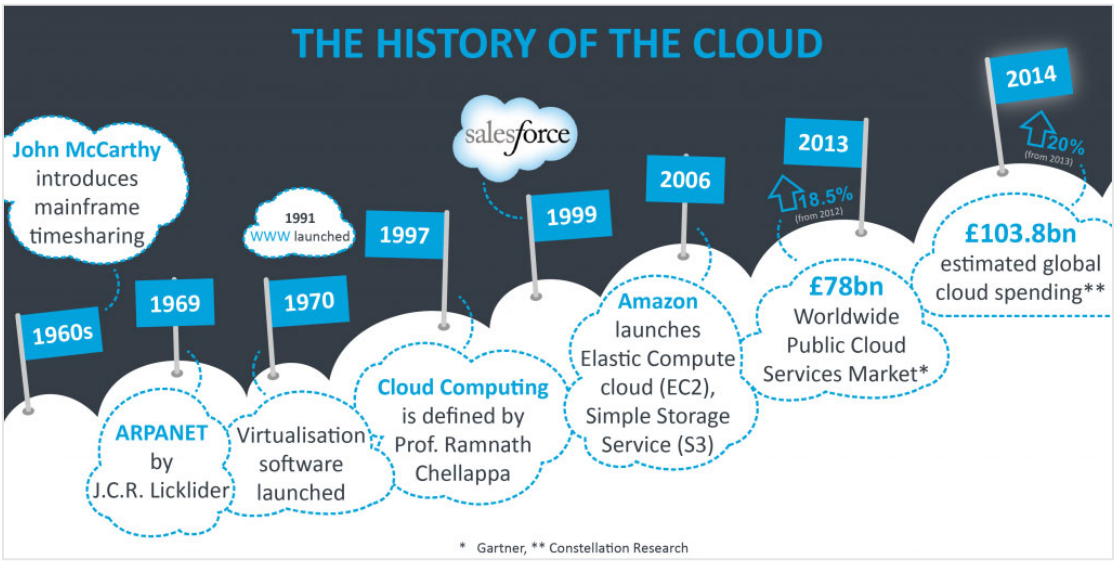
Εν ολίγοις, μπορούμε να σκεφτούμε το cloud computing ως παροχή υπολογιστικών υπηρεσιών, συμπεριλαμβανομένων διακομιστών, μέσων αποθήκευσης, βάσεων δεδομένων, δικτύων, λογισμικού, αναλυτικών στοιχείων και νοημοσύνης, όπου κάθε διαδικασία διεξάγεται μέσω Διαδικτύου για την παροχή ταχύτερης καινοτομίας, ευελιξίας πόρων και οικονομίες κλίμακας.

1.3 Ιστορική αναδρομή

Με την ανοδική εξέλιξη του Διαδικτύου, υπάρχει αυξημένη πίεση στην υπάρχουσα υποδομή αποθήκευσης και υπολογιστικών συστημάτων. Οι παροχείς υπηρεσιών Διαδικτύου έχουν ξεκινήσει να χρησιμοποιούν χαμηλότερης ποιότητας υλικά στους υπολογιστές που αποτελούν τη βάση τους (Kim, 2009). Αυτό έχει οδηγήσει στην ανάπτυξη διαφόρων τεχνολογιών λογισμικού που επιτρέπουν την ευέλικτη λειτουργία των υπολογιστών. Αυτή η εξέλιξη έχει οδηγήσει στην εμφάνιση τριών κυρίων παρόχων υπολογιστικού νέφους που βασίζονται σε τεχνολογίες αφαίρεσης πόρων: η Amazon, η Google και η Microsoft. Πιο συγκεκριμένα, η Amazon χρησιμοποιεί την τεχνολογία εικονικού διακομιστή και έχει δημιουργήσει υπηρεσίες όπως το Elastic Compute Cloud (EC2), το Amazon S3 (υπηρεσία αποθήκευσης αντικειμένων) και το SimpleDB (υπηρεσία αποθήκευσης δεδομένων δομής) που βασίζονται στην τεχνολογία Xen. Αυτές οι υπηρεσίες λειτουργούν κατόπιν αιτήματος και παρέχουν μια οικονομική λύση, καθιστώντας την Amazon πρωτοπόρο στην κατηγορία της υποδομής ως υπηρεσία (IaaS).

Από την άλλη πλευρά, η προσέγγιση της Google βασίζεται στη χρήση περιβάλλοντος άμμος (sandbox) για την υποστήριξη του τεχνικού μοντέλου τους. Η Google έχει δημοσιεύσει πολλές έρευνες από το 2003 έως το 2006, παρουσιάζοντας ένα είδος πλατφόρμας ως υπηρεσία (PaaS) για το cloud computing. Αυτή η πλατφόρμα, γνωστή ως Google App Engine (GAE), έγινε διαθέσιμη για το κοινό το 2008 (Qian et al., 2009).Το Microsoft Azure κυκλοφόρησε τον Οκτώβριο του 2008 και χρησιμοποιεί το Windows Azure Hypervisor (WAH) ως την υποκείμενη υποδομή του cloud, με το .NET

ως μέσο εφαρμογής. Το Azure προσφέρει επίσης υπηρεσίες όπως αποθήκευση αντικειμένων BLOB και υπηρεσία SQL. Είναι δύσκολο να αποφασίσουμε ποιο είναι καλύτερο, αλλά εμφανώς ο εικονικός διακομιστής προσφέρει μεγαλύτερη ευελιξία και είναι συμβατός με υφιστάμενα λογισμικά και εφαρμογές, ενώ τα sandboxes έχουν περιορισμούς στις γλώσσες προγραμματισμού, αλλά λιγότερη πολυπλοκότητα στην αφαίρεση πόρων. Παρατηρείται ότι, προς το παρόν, ο εικονικός διακομιστής αποτελεί την πιο δημοφιλή τεχνική αφαίρεσης πόρων στον τομέα του cloud computing (Qian et al., 2009). Πέρα από τις δημόσιες υπηρεσίες cloud αυτές, πολλές εταιρείες έχουν πειραματιστεί και ακόμα έχουν εφαρμόσει εσωτερικά συστήματα υπολογιστικού νέφους. Το cloud computing έχει γίνει ήδη βασική στρατηγική για προμηθευτές και παρόχους τηλεπικοινωνιακών υπηρεσιών. Επιπλέον, στις Ηνωμένες Πολιτείες και την Ιαπωνία, το cloud computing έχει γίνει εθνική στρατηγική. Η παρακάτω εικόνα παρουσιάζει την εξέλιξη του υπολογιστικού νέφους μέσα στα χρόνια (Qian et al., 2009).



Εικόνα 1 – History of the cloud

Πηγή: https://cloudcomputing521.wordpress.com/2017/05/01/history-of-cloud-computing

Κεφάλαιο 2: Αρχιτεκτονική υπολογιστικού νέφους & πλατφόρμες

2.1 Αρχιτεκτονική υπολογιστικού νέφους

Οι αλλαγές στις απαιτήσεις των συστημάτων πληροφορικής έχουν προκαλέσει τη δημιουργία του συστήματος απαιτήσεων για το cloud computing. Ο τρόπος που το cloud λειτουργεί και επιδρά στις ανάγκες των εταιρειών καθορίζεται από τις τεχνολογίες που τηρούν τις αυτές απαιτήσεις. Για να κατανοήσουμε αναλυτικά τη δομή του συστήματος cloud, πρέπει να μελετήσουμε τα βασικά στοιχεία που διαμορφώνουν τη συμπεριφορά του σύμφωνα με τον καθορισμένο ορισμό (Albini & Rajnai, 2018). Επιπλέον, είναι επικερδές να αξιολογήσουμε την αναγκαιότητα κάθε μέρους του.

Κατακόρυφη δομή: Όσον αφορά την κατακόρυφη δομή, βάσει του ορισμού του cloud, τα κύρια χαρακτηριστικά του μπορούν να οργανωθούν γύρω από θέματα όπως η διαθεσιμότητα, η δομή, η χωρητικότητα, η ευελιξία και η δυνατότητα μέτρησης. Στο παρελθόν, η δομή των παραδοσιακών συστημάτων πληροφορικής περιλάμβανε το δίκτυο, το υλικό, το λειτουργικό σύστημα, το επίπεδο βάσης δεδομένων και το επίπεδο εφαρμογής. Αυτό το παραδοσιακό μοντέλο άλλαξε με την εισαγωγή της εικονικοποίησης (virtualization). Η εικονικοποίηση δημιουργεί ένα νέο επίπεδο μεταξύ του υλικού και του λειτουργικού συστήματος, το οποίο επιτρέπει την ευέλικτη αλλαγή μεγέθους των υλικών πόρων. Στο νέο αυτό επίπεδο, τα σημεία επεξεργασίας χρησιμοποιούν μόνο τους πόρους που απαιτούν για την εκτέλεση των λειτουργιών τους. Επιπλέον, αυτό το επίπεδο έχει επιπτώσεις στη διαθεσιμότητα, τη χωρητικότητα και τη δυνατότητα μέτρησης. Ως αποτέλεσμα, η μελέτη αρχίζει με την εξέταση αυτού του επιπέδου.

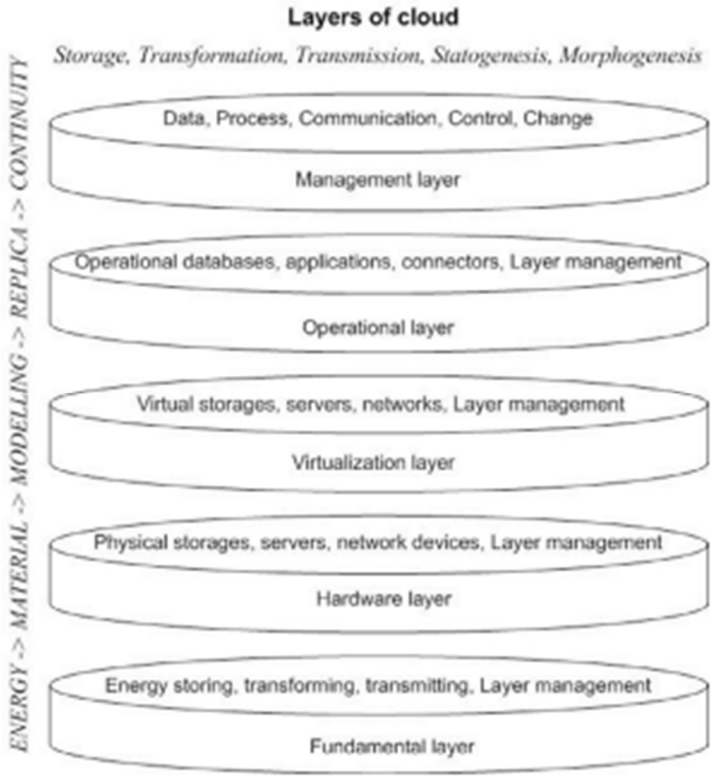
Κατά τη χρήση της εικονικοποίησης, οι φυσικοί πόροι των συστημάτων πληροφορικής, όπως η αποθήκευση δεδομένων, η ικανότητα επεξεργασίας και τα στοιχεία επικοινωνίας μπορούν να οργανωθούν ευέλικτα σε λογικές κατηγορίες πόρων. Έπειτα, αυτές οι λογικές κατηγορίες πόρων μπορούν να αντιστοιχιστούν σε εικονικά σημεία επεξεργασίας. Με αυτόν τον τρόπο, παρατηρούμε μια διάκριση ανάμεσα στους φυσικούς πόρους της πληροφορικής και τους λογικούς πόρους που απαιτούνται. Επιπλέον, οι λογικές κατηγορίες πόρων αποτελούν τη βάση για τη μέτρηση. Αντί να υπάρχουν απομονωμένα, το λειτουργικό σύστημα, τα στοιχεία βάσης δεδομένων, τα στοιχεία εφαρμογής και τα στοιχεία σύνδεσης δεδομένων συμπιέζονται σε ένα ενιαίο

επίπεδο, το οποίο αποκαλείται ως το επίπεδο λειτουργίας, σύμφωνα με την έρευνα των Albini & Rajnai (2018). Αυτό το επίπεδο λειτουργίας λειτουργεί ως πλατφόρμα για την εκτέλεση των επιχειρηματικών διαδικασιών. Πάνω από αυτό το επίπεδο, το διαχειριστικό επίπεδο εμπλουτίζεται με στοιχεία διαχείρισης cloud. Το επίπεδο του υλικού βρίσκεται κάτω από το εικονικό επίπεδο, το οποίο δημιουργεί τους φυσικούς πόρους της πληροφορικής. Επιπλέον, τα ενεργειακά στοιχεία που παράγουν μηχανολογικούς πόρους και μηχανολογικούς πόρους για το επίπεδο υλικού πρέπει να λαμβάνονται υπόψη, καθώς αποτελούν κρίσιμο στοιχείο για την λειτουργία του cloud. Αυτό το βασικό στρώμα αποτελεί τη θεμελιώδη βάση για τη σχεδίαση του cloud. Επιπλέον, καθένα από αυτά τα στρώματα αντιστοιχεί σε ένα θεωρητικό επίπεδο μοντελοποίησης, όπως ενέργεια, υλικό, αφαίρεση και συνέχεια.

Οριζόντια δομή: Προκειμένου να εδραιωθεί η διαδικασία οργάνωσης της οριζόντιας δομής, πρέπει να οργανωθούν οι βασικές συνιστώσες γύρω από φιλοσοφικές αφηρημένες κατηγορίες. Αυτές οι κατηγορίες περιλαμβάνουν τα ακόλουθα στοιχεία: το "αντικείμενο", που αναφέρεται σε ό,τι εκτελεί μια υπηρεσία ή υποστηρίζει μια λειτουργία. Σύμφωνα με το πρότυπο της πληροφορικής, αυτό μπορεί να είναι η επεξεργασία ή ο μετασχηματισμός. Το δεύτερο στοιχείο είναι η "ιδιοκτησία," που καθορίζει τον τρόπο με τον οποίο λειτουργεί η συνολική διαδικασία. Για παράδειγμα, στον τομέα της πληροφορικής, αυτό μπορεί να περιλαμβάνει δεδομένα ή αποθήκευση. Το τρίτο στοιχείο, η "σχέση," εκφράζει την εξωτερική σύνδεση. Σύμφωνα με το πρότυπο της πληροφορικής, αυτό μπορεί να είναι η επικοινωνία ή η μετάδοση. Αυτό το στατικό τρίπτυχο αντικατοπτρίζει μια γενική προσέγγιση. Συμπληρώνοντας αυτές τις αφηρημένες κατηγορίες με την πρωτογενή και δευτερεύουσα μεταβολή του συστήματος, δημιουργείται ένα δυναμικό μοντέλο. Οι τρεις αφηρημένες κατηγορίες συνθέτουν ένα σύνολο, και τα στοιχεία που περιγράφουν τη μεταβολή προσδίδουν κίνηση στο σύστημα. Συνεπώς, όλα τα στοιχεία είναι απαραίτητα.

Η δομή που δημιουργήθηκε βασίζεται στις προαναφερθείσες κάθετες και οριζόντιες εκτιμήσεις, καθώς και στα υποχρεωτικά στοιχεία. Όλα τα στοιχεία της δομής του πίνακα είναι υποχρεωτικά, και η απουσία οποιουδήποτε στοιχείου θα οδηγήσει στην αδυναμία επίτευξης των απαιτήσεων του cloud. Για αυτόν τον λόγο, αυτή η υποδομή μπορεί να αναφέρεται ως "αρχιτεκτονική" (Albini & Rajnai, 2018). Η αρχιτεκτονική του cloud μπορεί να διακριθεί σε πέντε κύρια στρώματα, λόγω της αρχής της διασύνδεσης. Κάθε ένα από αυτά τα στρώματα αντιπροσωπεύει ένα επίπεδο σκέψης

και λειτουργίας ανθρώπινης φύσης, συμπεριλαμβανομένων της εκδήλωσης της ενέργειας, της αναπαράστασης του υλικού κόσμου, του μοντελοποιητικού στρώματος της ανθρώπινης σκέψης, του αντιγράφου της πραγματικότητας και της συνέχειας. Επιπλέον, η κύρια αποστολή κάθε στρώματος είναι να διασφαλίσει την ασφάλεια και τη λειτουργία του επιπέδου λογισμικού.



Εικόνα 2 – Αρχιτεκτονική Νέφους

Ας δούμε αναλυτικά κάθε επίπεδο με ποιον τρόπο διαμορφώνεται:

Θεμελιώδες στρώμα (Fundamental Layer)

Το βασικό στρώμα αρχιτεκτονικής του cloud είναι το χαμηλότερο επίπεδο και αντιστοιχεί στη διαχείριση της φυσικής ενέργειας. Αυτό το επίπεδο εξυπηρετεί το υλικό επίπεδο που βρίσκεται πάνω από αυτό. Σε αυτό το στρώμα, οι φυσικοί πόροι μετατρέπονται σε μηχανικούς πόρους, χρησιμοποιώντας μηχανολογικές και κτιριακές λύσεις. Στοιχεία αυτού του στρώματος περιλαμβάνουν αποθήκευση ενέργειας, μετατροπείς ενέργειας, διαμεσολαβητές ενέργειας και εργαλεία διαχείρισης επιπέδων (Albini & Rajnai, 2018).

Στρώμα υλικού (Hardware Layer)

Το υλικό επίπεδο χρησιμοποιεί τις υπηρεσίες του κατώτερου θεμελιώδους επιπέδου και εξυπηρετεί το επίπεδο εικονικοποίησης που βρίσκεται πάνω από αυτό. Αυτό το στρώμα αντιστοιχεί στη λογική αναπαράσταση της φυσικής εκδήλωσης. Σε αυτό το στρώμα, οι μηχανικοί πόροι μετατρέπονται σε φυσικούς πόρους πληροφορικής μέσω συσκευών υλικού πληροφορικής. Στοιχεία αυτού του στρώματος περιλαμβάνουν αποθηκευτικούς χώρους φυσικών δεδομένων, φυσικούς διακομιστές, φυσικά δίκτυα και συσκευές δικτύου, καθώς και εργαλεία διαχείρισης επιπέδων.

Επίπεδο εικονικοποίησης (Virtualization Layer)

Το στρώμα εικονικοποίησης εκμεταλλεύεται τις υπηρεσίες του κατώτερου υλικού επιπέδου και υπηρετεί το επίπεδο λειτουργίας που βρίσκεται από πάνω. Αυτό το στρώμα αντιστοιχεί στην ανθρώπινη σκέψη σχετικά με τη μοντελοποίηση. Καλύπτει τους φυσικούς πόρους πληροφορικής και δημιουργεί ευέλικτες εικονικές ομάδες πόρων πληροφορικής. Επιπλέον, επιτρέπει τη δημιουργία εικονικών υπηρεσιών για μέτρηση. Στοιχεία αυτού του στρώματος περιλαμβάνουν εικονικές αποθήκες δεδομένων, κέντρα εικονικών πόρων, εικονικά δίκτυα και συσκευές εικονικού δικτύου, καθώς και εργαλεία διαχείρισης για την πλατφόρμα εικονικοποίησης (Albini & Rajnai, 2018).

Λειτουργικό στρώμα (Operational Layer)

Το επίπεδο λειτουργίας εκμεταλλεύεται τις υπηρεσίες του αν?οκείμενου επιπέδου εικονικοποίησης και παρέχει λειτουργικές παραμέτρους για το επίπεδο διαχείρισης που βρίσκεται από πάνω. Αυτό το στρώμα αντιστοιχεί στην απεικόνιση της πραγματικότητας στην ανθρώπινη σκέψη. Η πλατφόρμα του αποτελείται από το λειτουργικό σύστημα. Επιχειρηματικές διαδικασίες εκτελούνται σε αυτό το στρώμα, με τα υπόλοιπα επίπεδα να επωμίζονται την ευθύνη για τη διασφάλιση της συνεχούς και βιώσιμης λειτουργίας του. Στοιχεία αυτού του επιπέδου είναι παρόμοια με αυτά της παραδοσιακής προσέγγισης ενός συμβατικού λειτουργικού συστήματος δικτύου: διαχείριση βάσεων δεδομένων, επεξεργασία εφαρμογών, στοιχεία επικοινωνίας και διαχείριση επιπέδων.

Επίπεδο διαχείρισης (Management Layer)

Το επίπεδο διαχείρισης αποτελεί το υψηλότερο στρώμα του cloud. Παρόλο που όλα τα επίπεδα παρέχουν δεδομένα που εμπλέκονται με αυτό το επίπεδο με έμμεσο τρόπο, η

βάση του βρίσκεται απευθείας στο λειτουργικό επίπεδο. Αυτό το στρώμα αντιστοιχεί στη διασφάλιση της συνεχούς λειτουργίας και βιωσιμότητας. Τα στοιχεία που απαρτίζουν το στρώμα διαχείρισης περιλαμβάνουν εργαλεία διαχείρισης δεδομένων, συστήματα διαχείρισης των σημείων επεξεργασίας, συστήματα διαχείρισης υπηρεσιών δικτύου και διαχείριση συστημάτων υποστήριξης αποφάσεων (Albini & Rajnai, 2018).

2.2 Υπηρεσίες υπολογιστικού νέφους

Σε μια αγορά όπου προσφέρονται βοηθητικά προγράμματα πληροφορικής, είναι δυνατό να βρούμε μια ευρεία ποικιλία υπηρεσιών cloud. Αυτές οι υπηρεσίες cloud είναι συσκευασμένες με διεπαφές προγραμματισμού εφαρμογών (API) και είναι προσβάσιμες μέσω του δικτύου. Οι υπηρεσίες cloud αντιπροσωπεύουν κάθε είδους ικανότητα πληροφορικής που προσφέρεται από τον πάροχο υπηρεσιών cloud (CSP) στους πελάτες υπηρεσιών cloud (CSC). Συνήθεις κατηγορίες υπηρεσιών cloud περιλαμβάνουν την υποδομή ως υπηρεσία (IaaS), την πλατφόρμα ως υπηρεσία (PaaS) και το λογισμικό ως υπηρεσία (SaaS) (Rashid & Chaturvedi, 2019).

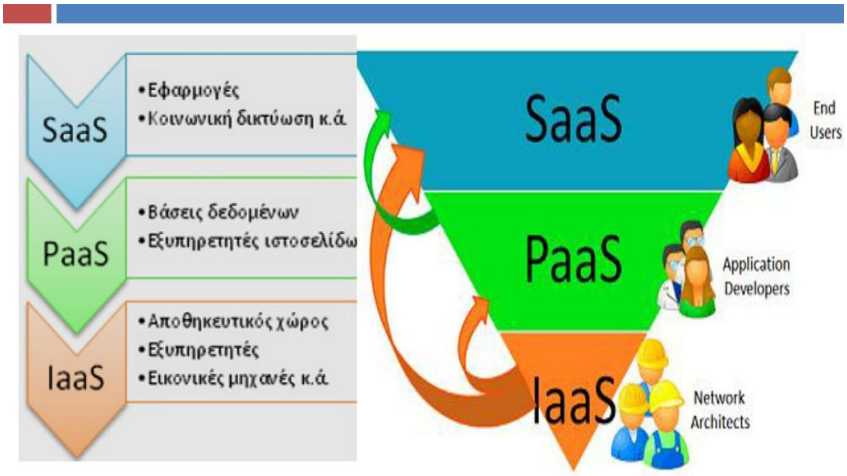
Infrastructure-as-a-service (IaaS): Το IaaS είναι η πιο βασική μορφή cloud υπηρεσιών. Παρέχει τεράστιους υπολογιστικούς πόρους, όπως χωρητικότητα αποθήκευσης, υπολογιστική ισχύ και δίκτυο. Επιτρέπει την απομακρυσμένη πρόσβαση σε αυτούς τους υπολογιστικούς πόρους. Τα κύρια πλεονεκτήματά του περιλαμβάνουν την πληρωμή βάσει της χρήσης, καθώς και ασφάλεια και αξιοπιστία. Είναι επίσης γνωστό ως "hardware-as-a-service" (Rashid & Chaturvedi, 2019). Ένα παράδειγμα IaaS είναι το Amazon Elastic Compute Cloud.

Platform-as-a-service (PaaS): Το PaaS υποστηρίζει ένα σύνολο προγραμμάτων εφαρμογών που συνδέονται με εφαρμογές cloud. Αναπτύχθηκε λόγω της αναγκαιότητας για αποδοτικότερο cloud computing και ανάπτυξη εφαρμογών στο web. Πολλές μεγάλες εταιρείες αποσκοπούν στην κυριαρχία στον τομέα του cloud computing, ανάλογα με τον τρόπο που η Microsoft επικράτησε στην αγορά των προσωπικών υπολογιστών (PC) (Rashid & Chaturvedi, 2019). Παραδείγματα PaaS περιλαμβάνουν το Google App Engine και το Microsoft Azure.

Software-as-a-service (SaaS): Το SaaS προσφέρει μια υπηρεσία που μπορεί να χρησιμοποιηθεί άμεσα από τον τελικό χρήστη. Αυτό είναι λογισμικό που αναπτύσσεται και προσφέρεται μέσω του Διαδικτύου. Πρόκειται για υπηρεσία όπου πληρώνεται

ανάλογα με τη χρήση. Στοχεύει να αντικαταστήσει τις εφαρμογές που εκτελούνται σε τοπικούς υπολογιστές. Ένα χαρακτηριστικό παράδειγμα SaaS είναι το Salesforce.com. Αυτά τα μοντέλα υπηρεσιών βοηθούν στην κατηγοριοποίηση όχι μόνο του cloud computing αλλά και των συγκεκριμένων προσφορών, προϊόντων και παρόχων (Rashid & Chaturvedi, 2019). Καθώς η τεχνολογία του cloud computing εξελίσσεται, πολλοί τύποι υπηρεσιών εισάγονται και επικαλύπτονται με αυτές τις αρχιτεκτονικές.

Στην εικόνα που ακολουθεί, παρουσιάζονται σχηματικά όλες οι υπηρεσίες που αναφέρθηκαν.



Εικόνα 3 – Μοντέλα Υπηρεσιών Νέφους

2.3 Cloud Πλατφόρμες

Το cloud computing είναι ένα μοντέλο που παρέχει υπηρεσίες υπολογιστικής φύσης παρόμοιες με τα παραδοσιακά βοηθητικά προγράμματα. Αυτό επιτρέπει στους χρήστες να αξιοποιούν υπηρεσίες βάσει των δικών τους αναγκών, χωρίς να χρειάζεται να ανησυχούν για το πού φιλοξενούνται οι υπηρεσίες ή τον τρόπο παράδοσής τους. Οι Amazon Web Services (AWS) και η Google Cloud Platform ανήκουν στους κύριους παροχείς υπηρεσιών cloud. Το AWS προσφέρει μια ευρεία γκάμα υπηρεσιών που καλύπτουν κατηγορίες όπως Υπολογισμός, Αποθήκευση, Παράδοση Περιεχομένου, Βάσεις Δεδομένων, Δικτύωση, Analytics και άλλες. Αντίθετα, το Google Cloud Platform επικεντρώνεται στη διαχείριση υποδομής, προσφέροντας διακομιστές,

διαμόρφωση δικτύων και υπηρεσίες σε κατηγορίες όπως Υπολογισμός, Αποθήκευση και Βάσεις Δεδομένων, Δικτύωση, Μεγάλα Δεδομένα και Μηχανική Εκμάθηση (Hyseni & Ibrahimi, 2017).

Στο παρελθόν, διεξήχθησαν δύο συγκρίσεις ανάμεσα στις πλατφόρμες υπολογιστικού νέφους που προσφέρονται από την Amazon και την Google, το 2014 και το 2016. Ο κύριος στόχος αυτών των συγκρίσεων ήταν να βοηθήσει τους χρήστες στην επιλογή της κατάλληλης πλατφόρμας υπολογιστικού νέφους ανάλογα με τις ανάγκες τους. Κατά τη διάρκεια αυτών των συγκρίσεων, αξιολογήθηκαν διάφοροι παράγοντες, συμπεριλαμβανομένων των κατηγοριών υπηρεσιών, των διαθέσιμων υπηρεσιών και των τιμών ανά μονάδα εικονικής μηχανής. Η σκοπιμότητα τέτοιων ερευνών ήταν να προσφέρει μια συνοπτική προεπισκόπηση των υπηρεσιών που παρέχουν και οι δύο παροχοί, ενώ παράλληλα βοηθά τους χρήστες και τους παρόχους υπηρεσιών cloud στη λήψη ενημερωμένων αποφάσεων (Hyseni & Ibrahimi, 2017). Ακολουθεί αναφορά στις κυριότερες πλατφόρμες με τη σχετική ανάλυση.

Amazon Web Servises: Ένα άτομο ή μια οργάνωση, είτε πρόκειται για δημόσιο, ιδιωτικό ή κυβερνητικό φορέα, μπορεί να αποκτήσει υπηρεσίες AWS (Amazon Web Services) σε μορφή υπολογιστικών πόρων κατ' απαίτηση, υπό το μοντέλο χρέωσης pay-as-you-go. Διαχειριστές Ιστού που βασίζονται στο cloud προσφέρουν πολλές διαφορετικές επιλογές, παρέχοντας πλαισιώσεις και συσκευές που εξυπηρετούν τις ανάγκες επεξεργασίας. Από την πλευρά της Amazon, το Amazon Elastic Compute Cloud παρέχει αυτές τις ευκολίες, επιτρέποντας στους πελάτες να έχουν διαρκή πρόσβαση σε μια εικονική συστοιχία υπολογιστών μέσω του Διαδικτύου.

Με αυτή τη λειτουργία, ο πελάτης αποκτά χαρακτηριστικά σαν να διαθέτει δικό του υψηλής ποιότητας υλικό, καθώς και εξοπλισμό (CPU και GPU για επεξεργασία, RAM για ανάγκες μνήμης, σκληρός δίσκος, SSD για αποθήκευση δεδομένων), με διάφορες επιλογές πλαισίων εργασίας και προ-κατασκευασμένων εφαρμογών, όπως CRM, βάσεις δεδομένων, και διακομιστές φιλοξενίας ιστοσελίδων, μεταξύ άλλων. Οι διακομιστές AWS σε παγκόσμιο επίπεδο διαχειρίζονται με ασφάλεια μέσω του συστήματος αντιγράφων ασφαλείας της Amazon. Το κόστος απόκτησης των υπηρεσιών τους ποικίλει ανάλογα με τις επιλογές του χρήστη (Kamal et al., 2020). Όσον αφορά το λειτουργικό σύστημα, τον σχεδιασμό του προγράμματος και τα χαρακτηριστικά οργάνωσης που καθορίζονται από τον πάροχο, απαιτούν την επιλογή

επιπέδου προσβασιμότητας, τη διασφάλιση της ασφάλειας και τη χρήση συγκεκριμένων εργαλείων διαχείρισης.

Ένας πελάτης έχει τη δυνατότητα να πληρώσει για να αποκτήσει έναν αποκλειστικό εικονικό υπολογιστή από τις υπηρεσίες AWS (Amazon Web Services), ή έναν αποκλειστικό φυσικό υπολογιστή, ή ακόμη και έναν συνδυασμό των δύο. Η καίρια πτυχή της συμφωνίας με το AWS είναι ότι προσφέρει ασφάλεια στον πελάτη. Οι υπηρεσίες του AWS είναι διαθέσιμες σε διάφορες γεωγραφικές τοποθεσίες σε όλο τον κόσμο (Kamal et al., 2020). Το AWS έχει εξυπηρετήσει περισσότερες από ενενήντα διοικήσεις μέχρι το 2017, καλύπτοντας διάφορους τομείς, όπως διαχείριση βάσεων δεδομένων, αποθήκευση, διαχείριση εφαρμογών, και εξοπλισμός που χρησιμοποιείται στη μηχανική και το Διαδίκτυο των πραγμάτων (IoT), μεταξύ άλλων. Το κυρίαρχο σύνολο προϊόντων περιλαμβάνει τα AS3 και EC2. Οι τελικοί χρήστες δεν αναλαμβάνουν το μεγαλύτερο μέρος της διαχείρισης απευθείας, αλλά χρησιμοποιούν τα API για την ενσωμάτωση των υπηρεσιών στις δικές τους εφαρμογές με σκοπό την επίτευξη των στόχων τους. Επιπλέον, το AWS έχει επεκταθεί στο πεδίο του HTTP και χρησιμοποιεί το δομικό στυλ REST και τη σύμβαση SOAP. Η Amazon προωθεί το AWS σε υποστηρικτές ως μέθοδο για την πιο γρήγορη και οικονομικά αποτελεσματική απόκτηση επεκταμένης κλίμακας πόρων από τον σχεδιασμό και τη συντήρηση ενός πραγματικού φυσικού κέντρου δεδομένων. Το κόστος χρέωσης των υπηρεσιών διαμορφώνεται ανάλογα με τη χρήση, και κάθε διαχείριση εκτιμά τη χρήση με διαφορετικούς τρόπους. Το AWS αποτελεί έναν ολοκληρωμένο πάροχο υπηρεσιών cloud, ενώ η Microsoft και η Google ακολουθούν το πρότυπο του AWS (Kamal et al., 2020).

Microsoft Azure Cloud: Το Microsoft Azure Cloud αναφέρεται στη διαχείριση ενός υπολογιστικού νέφους που παρέχεται από τη Microsoft για την εκτέλεση διάφορων εργασιών, όπως ανάλυση, ανάπτυξη, και διαχείριση εφαρμογών. Αυτό το υπολογιστικό νέφος διαχειρίζεται από κέντρο δεδομένων που ανήκει στη Microsoft. Προσφέρει λύσεις που καλύπτουν τις κατηγορίες SaaS (Λογισμικό ως Υπηρεσία), PaaS (Πλατφόρμα ως Υπηρεσία) και IaaS (Υποδομή ως Υπηρεσία), και υποστηρίζει πολλές γλώσσες προγραμματισμού, μηχανές, και δομές. Επιπλέον, παρέχει συγκεκριμένα πλαίσια και εργαλεία ανάπτυξης της Microsoft. Το Microsoft Azure ξεκίνησε τον Οκτώβριο του 2008 ως το έργο "Project Red Dog."

Το Microsoft Azure έχει επενδύσει σημαντικά ποσά χρημάτων στον τομέα του cloud computing, προσφέροντας διάφορες λύσεις cloud σε κλίμακα που έχουν δαπανήσει εκατομμύρια εκατομμύρια δολάρια. Αυτές οι λύσεις αποσκοπούν στην υποστήριξη των χρηστών και στην ικανοποίηση των απαιτήσεών τους. Το Microsoft Azure επιτρέπει στους αναπτυσσόμενους να χρησιμοποιούν τις υπηρεσίες του σε ένα δίκτυο με εκτεταμένους πόρους, χωρίς αρχική σημαντική επένδυση και με περιορισμένα λειτουργικά έξοδα. Το Cloud Computing είναι η υπολογιστική ισχύς που είναι διαθέσιμη στο δίκτυο και συνδέει διάφορες μηχανές, σε πολλές κατηγορίες υποδομής όπως ιδιωτικές, δημόσιες, και υβριδικές υποδομές.

Google Cloud Platform: Όπως δηλώνει το όνομα του, το GCP (Google Cloud Platform) παρέχεται από την Google και αποτελεί μια συλλογή διαχειριστών υπολογιστικού νέφους. Λειτουργεί στην ίδια πλατφόρμα που χρησιμοποιεί η Google για την εκτέλεση των υπηρεσιών τελικού πελάτη της, όπως το YouTube και η Αναζήτηση της Google. Μέσω αυτής της πλατφόρμας, ο πελάτης μπορεί να διεκπεραιώσει εύκολα διάφορες διοικητικές εργασίες στο cloud, όπως αποθήκευση δεδομένων, υπολογισμός πληροφοριών, ανάλυση δεδομένων και μηχανική μάθηση. Για τη διαδικασία εγγραφής απαιτείται λεπτομέρεια κάρτας χρέωσης ή εναλλακτικώς καθολικός τρόπος πληρωμής. Το GCP παρέχει στους χρήστες ένα στάδιο διαχείρισης και συνθηκών εγγραφής χωρίς την ανάγκη ύπαρξης διακομιστή. Η Google παρουσίασε το App Engine τον Απρίλιο του 2008, το οποίο λειτούργησε ως πλαίσιο για τη δημιουργία και διαχείριση εφαρμογών web σε φάρμες διακομιστών που εποπτεύει η Google.

Κύριως ασχολήθηκε με την διαχείριση κατανεμημένων υπολογιστών. Με την αυξανόμενη δημοτικότητά του, παρατηρήθηκε ότι συνήθως χρησιμοποιείται τον Νοέμβριο του 2011, και ως αποτέλεσμα, η Google συμμετείχε στην εισαγωγή διάφορων διαχειριστών cloud σε αυτό το στάδιο. Το Google Cloud Platform αντιπροσωπεύει μια επιχειρηματική μονάδα της Google που συνδυάζει το πλαίσιο ανοιχτού cloud GCP με τη χρήση του G Suite, βιομηχανίας προσαρμογών του Android και του Chrome OS, καθώς και διεπαφές προγραμματισμού εφαρμογών (API) που επικεντρώνονται στην τεχνητή νοημοσύνη (AI) και τη διαχείριση χαρτογράφησης. (Kamal et al., 2020)

Κεφάλαιο 3: Πλεονεκτήματα και μειονεκτήματα του Υπολογιστικού Νέφους

3.1 Πλεονεκτήματα του Υπολογιστικού Νέφους

Υπάρχουν ορισμένα βασικά πλεονεκτήματα σχετικά με τη χρήση και την αποθήκευση στο cloud, τα οποία καθιστούν ελκυστική την προοπτική της χωρητικότητας στο cloud. Τα κύρια από αυτά περιλαμβάνουν:

- *Απλούστερη διαχείριση*: Η υποστήριξη για προγραμματισμό, γενική υποδομή και υλικό που χρησιμοποιείται για την αποθήκευση αποθεμάτων βελτιώνεται σημαντικά με τη χρήση ενός cloud service. Οι εφαρμογές που βασίζονται σε cloud είναι συνήθως πολύ λιγότερο απαιτητικές όσον αφορά τη ρύθμιση και τη διαχείριση σε σύγκριση με αντίστοιχες εγκαταστάσεις (Abdalla & Varol, 2019). Συχνά, από πλευράς του χρήστη, το μόνο που απαιτείται για τη διαχείριση της χωρητικότητας είναι ένα πρόγραμμα περιήγησης στον ιστό, με την πολυπλοκότητα της διαχείρισης να ανατίθεται στον πάροχο υπηρεσιών.
- *Οικονομική αποδοτικότητα:* Η αποθήκευση στο cloud αποτελεί εξαιρετική λύση για την ελαχιστοποίηση των δαπανών κατοχής. Η εξάλειψη της ανάγκης για δαπανηρά συστήματα και το βάρος της συντήρησής τους από τον πελάτη, οδηγεί τις επιχειρήσεις σε σημαντικές εξοικονομήσεις, οι οποίες αντισταθμίζουν το κόστος της αποθήκευσης στο cloud. Επιπλέον, τα τέλη που σχετίζονται με τη δυνατότητα απόκτησης υψηλής διαθεσιμότητας και την ευελιξία που απαιτεί μια εταιρεία είναι πολύ πιο ανταγωνιστικά σε σχέση με την εξοικονόμηση. Κατά βάση, οι οικονομίες κλίμακας που πετυχαίνονται μέσω των server farms δυσκολα μπορούν να ταιριαστούν από άλλους εκτός από τους μεγάλους οργανισμούς.
- *Η τεχνική αποθήκευσης πληροφοριών σε απομακρυσμένους διακομιστές cloud είναι γνωστή ως cloud storage.* Η αποθήκευση στο cloud ξεχωρίζει θετικά από άλλες παραδοσιακές πρακτικές αποθήκευσης, με ένα μέρος της αιτιολόγησης να περιλαμβάνει τα εξής:
    - ✓ Οι εταιρείες δεν χρειάζεται πλέον να εγκαταστήσουν φυσικό αποθηκευτικό υλικό στο δικό τους χώρο εργασίας ή στο δικό τους κέντρο δεδομένων.

- ✓ Οι ρουτίνες συντήρησης που περιλαμβάνουν τη δημιουργία αντιγράφων ασφαλείας και την απόκτηση επιπλέον αποθηκευτικών μέσων απομακρύνονται από τον πελάτη, επιτρέποντάς του να επικεντρωθεί στις βασικές του δραστηριότητες.
- ✓ Οι εταιρείες αμείβουν μόνο για τον πραγματικό χώρο αποθήκευσης που χρησιμοποιούν.

- *Ατέλειες και ενημερώσεις χαμηλής επίδρασης:* Η υπηρεσία cloud computing συνήθως προσφέρει οικονομικές εναλλακτικές λύσεις στην αποθήκευση υλικού. Αυτό οδηγεί σε συνεχή λειτουργία κατά τη διάρκεια προγραμματισμένων ή απρογραμμάτιστων προβλημάτων (Abdalla & Varol, 2019). Αυτό ισχύει επίσης για τις αναβαθμίσεις του υλικού, οι οποίες δεν επηρεάζουν πλέον τον τελικό χρήστη.
- *Απλοποιημένη διάθεση:* Οι λύσεις αποθήκευσης στο cloud απελευθερώνουν τη χωρητικότητα σε τοπικό επίπεδο και παρέχουν ευέλικτες λύσεις αποθήκευσης που βασίζονται στο cloud ανάλογα με τις ανάγκες, εξαλείφοντας την ανάγκη για επιπλέον τοπικό αποθηκευτικό χώρο.
- *Δυνατότητα κέντρου δεδομένων:* Με τη χρήση δημόσιων cloud υπηρεσιών, ο πελάτης κατανέμει την υποδομή και τη διαχείριση σε οργανισμούς που εξειδικεύονται σε αυτόν τον τομέα. Συνεπώς, ο πελάτης δαπανά λιγότερο χρόνο στη διαχείριση της υποδομής, απελευθερώνοντας χρόνο για να επικεντρωθεί στις πυρήνας του δραστηριότητές του.
- *Εκτίμηση χρήσης:* Ο πελάτης πληρώνει μόνο για τους πόρους που πραγματικά χρησιμοποιεί. Αυτό επιτρέπει στον πελάτη να προσθέτει περισσότερες υπηρεσίες cloud όταν χρειάζεται, χωρίς την ανάγκη αγοράς φυσικού εξοπλισμού. Συνεπώς, προσφέρεται στον πελάτη η ευελιξία να πληρώσει μόνο ό,τι απαιτείται, όταν απαιτείται.
- *Ελαστικότητα*: Ο πελάτης διαθέτει πρακτικά ατελείωτη αποθηκευτική χωρητικότητα και μπορεί να προσαρμόσει δυναμικά τους υπολογιστικούς πόρους που χρειάζεται για να αντιμετωπίσει διακυμάνσεις στις απαιτήσεις του. Αυτό επιτρέπει στον πελάτη να αντιδρά σε απρόβλεπες αυξήσεις της κίνησης σε πραγματικό χρόνο, χωρίς την ανάγκη για ακριβές υλικό ή διακομιστές σε σταθερή λειτουργία. Αντίθετα, όταν ο πελάτης λειτουργεί με συγκεκριμένες ρυθμίσεις, είτε σε περιβάλλον cloud είτε μη cloud, πρέπει να διασφαλίσει ότι

διαθέτει επίσημα ή νοικιάζει τους απαιτούμενους πόρους για να ανταποκριθεί στα συγκεκριμένα πρότυπα χρήσης. (Abdalla & Varol, 2019).

3.2 Μειονεκτήματα του Υπολογιστικού Νέφους

Εκτός από τα πλεονεκτήματα, υπάρχουν επίσης αρκετά ανεπιθύμητα χαρακτηριστικά και κινδύνοι που σχετίζονται με τη χρήση χώρου αποθήκευσης στο cloud. Αν και το cloud computing αυξάνει την επιρροή του, εξακολουθούν να υφίστανται ανησυχίες (Avram, 2014). Μερικές κοινές προκλήσεις περιλαμβάνουν:

- *Προστασία των Δεδομένων*: Η διασφάλιση της ασφάλειας των δεδομένων αποτελεί κρίσιμο παράγοντα που πρέπει να αντιμετωπίζεται πάντοτε με σοβαρότητα. Οι επιχειρήσεις είναι αντίθετες στο να εμπιστεύονται την ασφάλεια των επιχειρηματικών τους δεδομένων σε τρίτους παροχείς. Έχουν φόβους ότι μπορεί να χάσουν δεδομένα στον ανταγωνισμό ή να παραβιαστεί η εμπιστευτικότητα των δεδομένων των πελατών τους. Σε πολλές περιπτώσεις, η πραγματική τοποθεσία αποθήκευσης δεν αποκαλύπτεται, προσθέτοντας περαιτέρω ανησυχίες σχετικά με την ασφάλεια του οργανισμού. Σε παραδοσιακά μοντέλα, οι επιχειρήσεις διαθέτουν φυσικά τείχη προστασίας γύρω από τα κέντρα δεδομένων (που ανήκουν σε αυτές) για την προστασία αυτών των ευαίσθητων πληροφοριών (Avram, 2014). Στο μοντέλο cloud, οι παροχείς υπηρεσιών είναι κυρίως υπεύθυνοι για την ασφάλεια των δεδομένων και οι επιχειρήσεις πρέπει να εμπιστεύονται αυτούς.
- *Ανάκτηση δεδομένων και διαθεσιμότητα:* Όλες οι επιχειρηματικές εφαρμογές είναι υποχρεωμένες να τηρούν αυστηρά τις συμφωνίες επιπέδου υπηρεσιών (SLA). Οι επιχειρησιακές ομάδες διαδραματίζουν κρίσιμο ρόλο στη διαχείριση αυτών των SLA και στον χρόνο εκτέλεσης των εφαρμογών. Σε παραγωγικά περιβάλλοντα, οι επιχειρησιακές ομάδες υποστηρίζουν: τη δημιουργία αντιγράφων ασφαλείας δεδομένων, την κατάλληλη ομαδοποίηση και αντιμετώπιση των αποτυχιών, την παρακολούθηση του συστήματος (παρακολούθηση συναλλαγών, παρακολούθηση αρχείων καταγραφής και άλλα), καθώς και την ανάκτηση δεδομένων από καταστροφικές καταστάσεις, τη διαχείριση της χωρητικότητας και της απόδοσης, καθώς και τη συντήρηση (Runtime Governance). Εάν οι υπηρεσίες αυτές είναι αντιμέτωπες με

προβλήματα λειτουργίας από έναν πάροχο cloud, οι ζημίες και ο αντίκτυπος θα μπορούσαν να έχουν καταστροφικές επιπτώσεις.

- *Ικανότητες διαχείρισης:* Αν και υπάρχουν πολλοί πάροχοι υπηρεσιών cloud, η διαχείριση της υποδομής και της πλατφόρμας βρίσκεται ακόμα σε αρχικό στάδιο. Χαρακτηριστικά όπως η δυναμική κλιμάκωση, η διαχείριση δυναμικών πόρων και η κατανομή πόρων αποτελούν κρίσιμες απαιτήσεις για πολλές επιχειρήσεις. Υπάρχουν μεγάλες ευκαιρίες για βελτίωση των δυνατοτήτων επεκτασιμότητας και φορτίου που προσφέρονται μέχρι σήμερα.
- *Κανονισμοί και Περιορισμοί Συμμόρφωσης*: Σε ορισμένες ευρωπαϊκές χώρες, υπάρχουν κυβερνητικοί κανονισμοί που δεν επιτρέπουν τη μεταφορά προσωπικών δεδομένων των πελατών και άλλων ευαίσθητων πληροφοριών εκτός της χώρας ή της πολιτείας. Για να συμμορφωθούν με αυτούς τους κανονισμούς, οι πάροχοι υπηρεσιών cloud πρέπει να δημιουργήσουν μια υποδομή αποθήκευσης δεδομένων αποκλειστικά εντός της συγκεκριμένης χώρας ή πολιτείας (Avram, 2014). Ωστόσο, η δημιουργία μιας τέτοιας υποδομής δεν είναι πάντα εφικτή και αποτελεί μεγάλη πρόκληση για τους παρόχους cloud. Με το cloud computing, η επίκρατη δραστηριότητα μετακινείται στη διεπαφή, που είναι το σημείο αλληλεπίδρασης μεταξύ των παρόχων υπηρεσιών και των πολλαπλών ομάδων χρηστών υπηρεσιών. Οι υπηρεσίες cloud απαιτούν επιδεξιότητες σε τομείς όπως η διανομή, η αξιολόγηση των κινδύνων, και η διαπραγμάτευση υπηρεσιών, πράγματα στα οποία πολλές επιχειρήσεις δεν είναι εξοπλισμένες να χειριστούν.

Κάποια από τα συχνά εντοπιζόμενα μειονεκτήματα που συχνά καταγράφονται λόγω της συνεχούς χρήσης του υπολογιστικού νέφους περιλαμβάνουν:

- ✓ Διαρροές και πρόσβαση σε δεδομένα χωρίς άδεια μεταξύ εικονικών συσκευών που λειτουργούν στον ίδιο διακομιστή.
- ✓ Σφάλματα εκ μέρους του προμηθευτή cloud στον χειρισμό της σωστής διαχείρισης και αποθήκευσης ευαίσθητων δεδομένων (Ali, Khan & Vasilakos, 2015).
- ✓ Μερικές φορές η υπηρεσία cloud μπορεί να μην είναι διαθέσιμη για εκτεταμένες χρονικές περιόδους λόγω σφαλμάτων και σφαλμάτων συστήματος.

- ✓ Οι χάκερ μπορεί να παραβιάσουν και να εισέλθουν σε εφαρμογές πελάτη που φιλοξενούνται στο cloud, και έτσι να έχουν πρόσβαση και να διανέμουν ευαίσθητα δεδομένα.
- ✓ Ζητήματα αξιοπιστίας.
- ✓ Πιθανή αδυναμία διατήρησης της ακεραιότητας των δεδομένων (βεβαιωθείτε ότι οι αποθηκευμένες πληροφορίες είναι «σωστές»).
- ✓ Περιορισμένες ρυθμίσεις: Οι προμηθευτές λύσεων δημόσιου νέφους έχουν μια τυπική διάταξη διαμορφώσεων θεμελίων που ανταποκρίνονται στις ανάγκες του συνολικού πληθυσμού. Σε ορισμένες περιπτώσεις, απαιτείται εξαιρετικά εξειδικευμένο υλικό για την αντιμετώπιση κλιμακούμενων υπολογιστικών ζητημάτων (Ali, Khan & Vasilakos, 2015). Σε περιπτώσεις όπως αυτή, η χρήση λύσεων δημόσιου cloud είναι συχνά αδύνατη, με την αιτιολογία ότι η απαιτούμενη λειτουργικότητα είναι απλή και δεν προσφέρεται από τον προμηθευτή.

3.3 *Βασικά χαρακτηριστικά του υπολογιστικού νέφους*

Το cloud computing, το grid computing, οι υπολογιστές υψηλής απόδοσης (High Performance Computing - HPC) ή οι υπερυπολογιστές, καθώς και τα κέντρα δεδομένων των υπολογιστών, όλοι ανήκουν στον παράλληλο υπολογισμό. Οι υπολογιστές υψηλής απόδοσης επικεντρώνονται στην επιστημονική πληροφορική, η οποία είναι εντατική και, ως εκ τούτου, παρέχει υψηλή απόδοση επεξεργασίας και χαμηλή καθυστέρηση. Ο υπολογισμός πλέγματος βασίζεται στα κέντρα HPC (High Performance Computing) (Kim, 2009). Πολλά συνδεδεμένα κέντρα HPC σχηματίζουν ένα μεγάλο πλέγμα που ακολουθεί μια ισχυρή βάση. Το cloud computing, που βασίζεται στα κέντρα δεδομένων, είναι πολύ πιο διαδεδομένο από τον υπολογισμό πλέγματος, καθώς το κέντρο δεδομένων δεν αποσκοπεί απλά στην υψηλή απόδοση επεξεργασίας και τη χαμηλή καθυστέρηση. Αντίθετα, είναι περισσότερο ισορροπημένο από τα κέντρα HPC (Gong et al., 2010). Ορισμένα από τα χαρακτηριστικά του cloud computing περιλαμβάνουν:

Εννοιολογικά χαρακτηριστικά – προσανατολισμένο στις υπηρεσίες*:* Το cloud computing και οι υπηρεσίες του συχνά βασίζονται σε αρχές που είναι παρόμοιες με τον παραδοσιακό υπολογισμό πλέγματος, αλλά είναι πιο πρακτικές και προσανατολισμένες

στην απλοποίηση της χρήσης του υπολογισμού. Η αφαίρεση και η προσβασιμότητα είναι δύο βασικά χαρακτηριστικά που συμβάλλουν στην απλοποίηση της χρήσης του cloud. Οι χρήστες δεν χρειάζεται να έχουν λεπτομερείς γνώσεις της υποκείμενης αρχιτεκτονικής του cloud για να το χρησιμοποιήσουν.

Οι υπηρεσίες του cloud computing διαχωρίζονται συνήθως σε τρεις κύριες κατηγορίες:

- **Infrastructure-as-a-Service (IaaS)**: Σε αυτήν την κατηγορία, παρέχονται υπολογιστικοί πόροι όπως χωρητικότητα αποθήκευσης, ισχύς επεξεργασίας και υποδομή δικτύου. Οι χρήστες μπορούν να εκμεταλλευτούν αυτούς τους πόρους όπως τους χρειάζονται.
- **Platform-as-a-Service (PaaS)**: Σε αυτήν την κατηγορία, οι υποδομές είναι αφαιρεμένες, και παρέχεται ένα περιβάλλον ανάπτυξης λογισμικού. Οι προγραμματιστές μπορούν να αναπτύξουν και να τρέξουν εφαρμογές χωρίς να ανησυχούν για την υποκείμενη υποδομή.
- **Software-as-a-Service (SaaS)**: Σε αυτήν την κατηγορία, παρέχονται λογισμικές εφαρμογές προς χρήση μέσω του διαδικτύου. Οι χρήστες δεν χρειάζεται να εγκαταστήσουν το λογισμικό στους δικούς τους υπολογιστές, αλλά μπορούν να το χρησιμοποιήσουν απευθείας μέσω της περιήγησής τους.

Αυτές οι κατηγορίες καλύπτουν ένα ευρύ φάσμα απαιτήσεων και αναγκών, επιτρέποντας στους χρήστες να επιλέγουν τον τύπο υπηρεσίας που ταιριάζει καλύτερα στον σκοπό τους.

Τεχνικά χαρακτηριστικά – χαλαρή ζεύξη: Η χαλαρή σύζευξη είναι πράγματι ένα σημαντικό τεχνικό χαρακτηριστικό του cloud computing. Επιτρέπει τη διάχωρση των υποδομών και την ανεξαρτησία των μερών, ενισχύοντας την ευελιξία και την απόδοση των υπηρεσιών cloud. Αυτό σημαίνει ότι η συμπεριφορά ή η απόδοση ενός τμήματος της υποδομής cloud δεν επηρεάζει αναγκαστικά τα υπόλοιπα τμήματα, και οι πελάτες μπορούν να χρησιμοποιούν τις υπηρεσίες ανεξάρτητα μεταξύ τους. Συγχρόνως, αυτό επιτρέπει την αποτελεσματική διαχείριση των καθυστερήσεων, καθώς εξαρτήσεις δεδομένων και καθολικοί συγχρονισμοί είναι αρκετά περίπλοκοι για να υποστηρίξουν την υψηλή καθυστέρηση μεταξύ των υπολογιστικών κόμβων. Η χρήση υψηλής ταχύτητας δικτύων όπως το InfiniBand είναι σημαντική για την διασφάλιση της αποδοτικής επικοινωνίας μεταξύ των διαφορετικών τμημάτων της υποδομής cloud. Αυτές οι τεχνικές λεπτομέρειες συμβάλλουν στη δημιουργία ενός αποδοτικού και

αξιόπιστου συστήματος cloud computing που επιτρέπει την ευέλικτη παροχή υπηρεσιών στους χρήστες.

Τεχνικά χαρακτηριστικά – ισχυρή ανοχή σε σφάλματα: Η ανοχή σε σφάλματα αποτελεί σημαντικό πεδίο στην επιστήμη της πληροφορικής, και είναι αναγκαία για τη διασφάλιση της αξιοπιστίας και της διαθεσιμότητας συστημάτων, ιδίως σε υψηλής απόδοσης και κρίσιμες εφαρμογές. Οι μέθοδοι ανοχής σε σφάλματα στοχεύουν στη δυνατότητα ενός συστήματος να συνεχίσει να λειτουργεί, ακόμη και αν παρουσιαστούν σφάλματα, εξασφαλίζοντας έτσι την ευστάθεια και την ασφάλειά του. Ο έλεγχος των σφαλμάτων σε διάφορα επίπεδα και σε διάφορες μορφές είναι αναγκαίος. Αυτό μπορεί να περιλαμβάνει τόσο την ανίχνευση όσο και την αποκατάσταση σφαλμάτων. Οι προηγμένες μέθοδοι συχνά απαιτούν χρήση εξειδικευμένου υλικού και λογισμικού για την επίτευξη αυτών των στόχων. Επιπλέον, σε παράλληλα υπολογιστικά συστήματα, όπου η διαχείριση των σφαλμάτων μπορεί να είναι ακόμα πιο προκλητική, οι μέθοδοι ανοχής σε σφάλματα παίζουν κρίσιμο ρόλο. Η έρευνα και η ανάπτυξη σε αυτόν τον τομέα συνεχίζεται, καθώς οι απαιτήσεις για αξιοπιστία και ανοχή σε σφάλματα συνεχώς εξελίσσονται με την αύξηση της πολυπλοκότητας των συστημάτων υπολογιστών και των εφαρμογών.

***Οικονομικά χαρακτηριστικά – επιχειρηματικό μοντέλο*:** Το επιχειρηματικό μοντέλο είναι πράγματι ένα κρίσιμο στοιχείο διάκρισης μεταξύ του grid computing και του cloud computing. Και τα δύο μοντέλα υπολογιστικής υποδομής εστιάζουν στην παροχή υπολογιστικών υπηρεσιών, αλλά έχουν διαφορετικές κατευθύνσεις σε ό,τι αφορά την παροχή αυτών των υπηρεσιών και τον τρόπο επιχειρηματικής αλληλεπίδρασης. Στο grid computing, όπως αναφέρατε, η έρευνα και η ακαδημαϊκή κοινότητα ήταν συχνά υπεύθυνες για την ανάπτυξη και τη λειτουργία των πλεγμάτων. Αυτό οδήγησε το grid computing να έχει συχνά ακαδημαϊκό ή κυβερνητικό χαρακτήρα με έμφαση στην έρευνα και την επιστημονική κοινότητα. Τα κίνητρα δεν ήταν πάντα το κέρδος ή η επιχειρηματική απόδοση, αλλά η εξυπηρέτηση ερευνητικών αναγκών και της κοινότητας. Αντίθετα, το cloud computing υποστηρίζεται κυρίως από μεγάλες εταιρείες του ιδιωτικού τομέα που προσφέρουν υπηρεσίες cloud για κερδοσκοπικούς λόγους. Το επιχειρηματικό μοντέλο του cloud computing εστιάζει στην παροχή άμεσα χρήσιμων υπηρεσιών για τους χρήστες, συχνά με βάση τη χρήση. Οι χρήστες του cloud computing μπορούν να είναι τόσο τελικοί χρήστες (π.χ., άτομα που χρησιμοποιούν υπηρεσίες SaaS για προσωπική χρήση) όσο και επαγγελματίες που παρέχουν υπηρεσίες

σε άλλους χρησιμοποιώντας την υπολογιστική υποδομή του cloud. Συνοψίζοντας, το grid computing είναι συχνά πιο επικεντρωμένο στην έρευνα και την ακαδημαϊκή κοινότητα, ενώ το cloud computing εστιάζει περισσότερο στην επιχειρηματική προοπτική και την παροχή υπηρεσιών κοινής ωφέλειας σε ευρύτερες κοινότητες, συμπεριλαμβανομένων τόσο των τελικών χρηστών όσο και των διαμεσολαβητών.

Χαρακτηριστικά εμπειρίας χρήστη – ευκολία χρήσης: Η εμπειρία χρήστη είναι σημαντικό κριτήριο στην αξιολόγηση και την επιτυχία μιας εφαρμογής, ανεξάρτητα από το πεδίο της υπολογιστικής υποδομής που χρησιμοποιείται. Στον τομέα του cloud computing, η εμπειρία χρήστη παίζει έναν σημαντικό ρόλο, καθώς οι υπηρεσίες προσφέρονται σε άτομα και επιχειρήσεις που εξαρτώνται από αυτές για την αποτελεσματική εκτέλεση των καθημερινών τους εργασιών. Ο σχεδιασμός της εμπειρίας χρήστη είναι κρίσιμος, διότι επηρεάζει την ευκολία χρήσης και την αποτελεσματικότητα των χρηστών όταν αλληλεπιδρούν με τις υπηρεσίες του cloud. Η δημιουργία μιας φιλικής προς τον χρήστη περιβάλλοντος και η εξασφάλιση ότι οι χρήστες μπορούν να αποκτούν πρόσβαση σε απαραίτητες υπηρεσίες είναι θεμελιώδεις για την επιτυχία του cloud computing. Επιπλέον, οι πτυχές όπως η χρηστικότητα, η αξιοποίηση, η πολύτιμη διαφοροποίηση και η επιθυμητή εμπειρία παίζουν ρόλο στον τρόπο που οι παροχείς cloud προσφέρουν τις υπηρεσίες τους. Οι πελάτες πρέπει να βρίσκουν Ceιρίες τοποθεσίες που να ανταποκρίνονται στις ανάγκες τους και να προσφέρουν μια ικανοποιητική εμπειρία. Συνολικά, η εμπειρία χρήστη παίζει κεντρικό ρόλο στην επιτυχία του cloud computing και θα πρέπει να λαμβάνεται υπόψη κατά την ανάπτυξη και την παροχή υπηρεσιών στον χώρο της υπολογιστικής υποδομής.

Κεφάλαιο 4: Νομοθεσία σχετικά με το cloud computing

4.1 Service-level Agreement (SLA)

Παρακάτω γίνεται προσπάθεια να παρουσιάσουμε την ουσία του cloud computing και τα διάφορα μοντέλα υπηρεσιών που παρέχει. Δίνεται μια σύντομη επεξήγηση για τα βασικά σημεία που σχετίζονται με τις υπηρεσίες αυτές:

Cloud Computing: Το cloud computing αναφέρεται στη χρήση απομακρυσμένων υπολογιστικών πόρων και υπηρεσιών μέσω του διαδικτύου. Αυτό αντικαθιστά την ανάγκη για τοπικούς υπολογιστές και διακομιστές σε επιχειρήσεις.

Μοντέλα υπηρεσιών: Το cloud computing προσφέρει διάφορα μοντέλα υπηρεσιών. Τα πιο κοινά είναι: Υλικό ως Υπηρεσία (IaaS), Πλατφόρμα ως Υπηρεσία (PaaS), Λογισμικό ως Υπηρεσία (SaaS).

Ελαστικότητα και Χαμηλό κόστος: Ένα από τα βασικά πλεονεκτήματα του cloud computing είναι η δυνατότητα προσαρμογής των πόρων κατάλληλα για τη ζήτηση. Οι πόροι πληρώνονται με βάση τη χρήση, καθιστώντας το πιο οικονομικό για πολλές επιχειρήσεις.

- ✓ **Επιχειρηματικό Μοντέλο**: Η μετάβαση στο cloud computing μπορεί να επηρεάσει το επιχειρηματικό μοντέλο μιας επιχείρησης. Παρέχει ευελιξία στον τρόπο που οι επιχειρήσεις παρέχουν και χρησιμοποιούν τις υπηρεσίες τους.
- ✓ **Τιμή**: Το cloud computing μπορεί να προσφέρει υψηλή απόδοση σε χαμηλότερο κόστος σε σύγκριση με την παραδοσιακή υποδομή. Αυτή η οικονομική αποδοτικότητα είναι ένα από τα σημαντικά πλεονεκτήματα.

Η μετάβαση στο cloud computing έχει αλλάξει τον τρόπο που οι επιχειρήσεις αντιλαμβάνονται και χρησιμοποιούν την υπολογιστική υποδομή. Προσφέρει ευελιξία και δυνατότητα πρόσβασης σε πόρους και υπηρεσίες χωρίς την ανάγκη για μεγάλες επενδύσεις σε υλικό και λογισμικό. Η περιγραφή σχετικά με τη Συμφωνία Επιπέδου Υπηρεσιών (SLA) και την σημασία της στον χώρο του cloud computing είναι πολύ κατατοπιστική. Οι SLA είναι σημαντικές για να εξασφαλίζεται η αποδοτική παροχή υπηρεσιών και η διατήρηση της αξιοπιστίας στον χώρο του cloud computing. Εδώ είναι μερικά κύρια σημεία που επισημαίνονται στους κανονισμούς:

- **Είδη SLA**: Υπάρχουν διάφορα είδη SLA που καθορίζουν την απόδοση και τη συμπεριφορά των cloud υπηρεσιών. Αυτά μπορεί να περιλαμβάνουν όρους για τον μέσο χρόνο μεταξύ αποτυχιών (MTBF), τον μέσο χρόνο για την επισκευή (MTTR), ρυθμούς δεδομένων, απόδοση και άλλα μετρήσιμα χαρακτηριστικά.

- **Επιβολή και Ανταμοιβές/Ποινές**: Οι SLA συχνά περιλαμβάνουν κανόνες για την επιβολή ανταμοιβών ή ποινών. Αυτό διευκολύνει τη διασφάλιση της συμμόρφωσης με τις συμφωνίες και τη διόρθωση τυχόν παραβιάσεων.

- **Διατήρηση και Τροποποίηση**: Είναι σημαντικό να διατηρείται και να επικαιροποιείται η SLA για να ανταποκρίνεται σε νέες ανάγκες και προδιαγραφές. Οι εμπλεκόμενοι φορείς πρέπει να συναντώνται τακτικά για την αξιολόγηση και την ενημέρωση της SLA.

- **Επίσημη ή Ατύπη Συμφωνία**: Οι SLA μπορεί να είναι επίσημες ή ατύπες, ανάλογα με τον χαρακτήρα των σχέσεων μεταξύ των ενδιαφερομένων. Οι επίσημες SLA συνήθως είναι νομικά δεσμευτικές συμφωνίες.

Οι SLA είναι καίριες για τη διαχείριση και την αξιοπιστία στον τομέα του cloud computing, καθώς βοηθούν στην εξασφάλιση ότι οι υπηρεσίες παραμένουν σταθερές και αξιόπιστες για τους χρήστες.

4.2 SLA στο cloud computing

Σίγουρα, η διανομή λογισμικού σε ένα εκατομμύριο χρήστες μέσω ενός κέντρου δεδομένων στο πλαίσιο του cloud computing είναι πολύ διαφορετική από την παραδοσιακή διανομή λογισμικού σε προσωπικούς υπολογιστές. Υπάρχουν πολλές προκλήσεις που πρέπει να αντιμετωπίσουν οι πάροχοι cloud κατά την παράδοση λογισμικού ως υπηρεσία, συμπεριλαμβανομένων των προκλήσεων που σχετίζονται με τη διαχείριση πόρων και την καθορισμό των SLA:

- **Διαχείριση Πόρων**: Στην περίπτωση του cloud, οι πόροι πρέπει να κατανέμονται αυτόματα και δυναμικά για να ανταποκρίνονται στις απαιτήσεις των χρηστών. Αυτό απαιτεί προηγμένη διαχείριση πόρων και ευφυείς αλγόριθμους.

- **Εξατομικευμένη Παροχή**: Κάθε χρήστης ή ομάδα χρηστών μπορεί να έχει διαφορετικές ανάγκες. Οι πάροχοι cloud πρέπει να είναι σε θέση να παρέχουν εξατομικευμένες λύσεις που ικανοποιούν αυτές τις ανάγκες.

- **Μέτρηση Απόδοσης**: Τα SLA πρέπει να περιλαμβάνουν συγκεκριμένες παραμέτρους απόδοσης που μπορούν να μετρηθούν και να παρακολουθηθούν. Αυτό βοηθά στην αξιολόγηση της ποιότητας των υπηρεσιών και στην διόρθωση πιθανών προβλημάτων.

- **Ενθάρρυνση/Αποθάρρυνση της Υποβολής Αιτημάτων**: Οι SLA μπορούν να περιλαμβάνουν μηχανισμούς ανατροφοδότησης που ενθαρρύνουν ή αποθαρρύνουν την υποβολή αιτημάτων υπηρεσιών, ανάλογα με τη διαθεσιμότητα των πόρων.

- **Συνεχής Επαλήθευση και Ενημέρωση**: Οι SLA πρέπει να είναι ευέλικτες και να ενημερώνονται τακτικά για να ανταποκρίνονται σε αλλαγές και να διασφαλίζουν ότι η ποιότητα των υπηρεσιών παραμένει υψηλή.

Επίσης, η ασφάλεια και η προστασία των δεδομένων είναι σημαντικές προκλήσεις όταν παρέχουμε λογισμικό ως υπηρεσία σε εκατομμύρια χρήστες μέσω ενός κέντρου δεδομένων. Η διαχείριση της ασφάλειας πρέπει να είναι εξαιρετικά αυστηρή για την προστασία των ευαίσθητων δεδομένων των χρηστών. Ο καθορισμός παραμέτρων ποιότητας υπηρεσίας (Quality of Service - QoS) και η χρήση τους σε συμφωνίες επιπέδου υπηρεσίας (SLA) είναι κρίσιμοι για τον επιτυχημένο σχεδιασμό και τη λειτουργία ενός cloud computing περιβάλλοντος. Οι QoS παράμετροι βοηθούν στον καθορισμό των προδιαγραφών που πρέπει να πληρούνται όσον αφορά την απόδοση και την ποιότητα των υπηρεσιών. Αυτό δίνει στους πάροχους cloud τη δυνατότητα να κατανοήσουν τι ακριβώς αναζητούν οι χρήστες και πώς μπορούν να προσφέρουν αυτές τις υπηρεσίες με τον βέλτιστο τρόπο. Ορισμένες προκλήσεις και λύσεις περιλαμβάνουν:

- ✓ Ορισμός κατάλληλων QoS Παραμέτρων: Οι πάροχοι cloud πρέπει να καθορίσουν ποιες QoS παράμετροι είναι σημαντικές για τους χρήστες τους. Αυτές μπορεί να περιλαμβάνουν την απόδοση, τη διαθεσιμότητα, τον χρόνο ανταπόκρισης, την ασφάλεια και πολλά άλλα.

- ✓ Διαφοροποίηση Υπηρεσιών: Ανάλογα με τις QoS απαιτήσεις, οι πάροχοι cloud μπορεί να προσφέρουν διάφορα επίπεδα υπηρεσιών. Παρέχοντας επιλογές, οι χρήστες μπορούν να επιλέξουν αυτό που ταιριάζει καλύτερα στις ανάγκες τους.
- ✓ Συνεχής Παρακολούθηση και Προσαρμογή: Η παρακολούθηση της QoS είναι σημαντική. Οι πάροχοι πρέπει να ελέγχουν την απόδοση και να προσαρμόζουν τις υπηρεσίες τους σε πραγματικό χρόνο για να παραμείνουν συμβατοί με τα SLA.
- ✓ Μηχανισμοί Ανατροφοδότησης: Οι SLA πρέπει να περιλαμβάνουν μηχανισμούς ανατροφοδότησης που επιτρέπουν στους χρήστες να αξιολογήσουν την εμπειρία τους και να καταθέσουν παρατηρήσεις και παράπονα.
- ✓ Αυτόματη Διαχείριση Πόρων: Η αυτοματοποίηση και η δυναμική διαχείριση πόρων είναι κρίσιμες για την εκπλήρωση των SLA, καθώς επιτρέπουν την ανταπόκριση σε μεταβαλλόμενες απαιτήσεις.
- ✓ Οι QoS και οι SLA είναι ουσιώδεις για την επίτευξη υψηλής ποιότητας υπηρεσιών στον κόσμο του cloud computing. Αυτές οι πρακτικές βοηθούν τους πάροχους να κατανοήσουν, να παρακολουθούν και να βελτιώσουν συνεχώς την απόδοση των υπηρεσιών τους και να προσφέρουν μια θετική εμπειρία στους χρήστες τους.

Διαχείριση υπηρεσιών με γνώμονα τον πελάτη, έχει να κάνει με την ικανοποίηση των πελατών, η οποία αποτελεί θεμέλιο παράγοντα για την επιτυχία ενός παρόχου υπηρεσιών υπολογιστών στον κλάδο του cloud computing. Για να επιτύχουν αυτόν τον στόχο, οι πάροχοι υπηρεσιών πρέπει να επικεντρωθούν στην εξατομίκευση, την επικοινωνία, την ασφάλεια, την αξιοπιστία και την εξυπηρέτηση των πελατών τους. Παραθέτουμε μερικούς σημαντικούς παράγοντες που συνδέονται με την ικανοποίηση των πελατών στον χώρο του cloud computing:

- ✓ **Επικοινωνία και Σχόλια**: Οι πάροχοι πρέπει να διατηρούν ανοιχτές γραμμές επικοινωνίας με τους πελάτες τους. Ακούγοντας τα σχόλια, τις ανησυχίες και τις απόψεις των πελατών, μπορούν να προσαρμόσουν τις υπηρεσίες τους για να ανταποκριθούν στις ανάγκες τους.

- ✓ **Ασφάλεια**: Η προστασία των δεδομένων των πελατών είναι θεμελιώδης. Οι πάροχοι πρέπει να λαμβάνουν μέτρα ασφαλείας για να προστατεύσουν τα δεδομένα και την ιδιωτικότητα των χρηστών τους.

- ✓ **Αξιοπιστία**: Η σταθερότητα και η διαθεσιμότητα των υπηρεσιών είναι ζωτικής σημασίας. Οι πελάτες πρέπει να μπορούν να βασίζονται στο ότι οι υπηρεσίες θα είναι διαθέσιμες όταν τις χρειάζονται.

- ✓ **Εξυπηρέτηση Πελατών**: Οι πάροχοι πρέπει να είναι ευγενείς και φιλικοί απέναντι στους πελάτες τους. Ο τρόπος επικοινωνίας και εξυπηρέτησης πελατών πρέπει να είναι υψηλού επιπέδου.

- ✓ **Διαφοροποίηση**: Οι πάροχοι μπορούν να προσφέρουν διάφορα επίπεδα υπηρεσιών για να ικανοποιήσουν διαφορετικές ανάγκες των πελατών. Αυτό επιτρέπει στους πελάτες να επιλέξουν αυτό που ταιριάζει καλύτερα στις ανάγκες τους.

Η διατήρηση της ικανοποίησης των πελατών απαιτεί συνεχείς προσπάθειες και παρακολούθηση της αγοράς, καθώς και την προσαρμογή στις μεταβαλλόμενες ανάγκες και προτιμήσεις των πελατών.

Διαχείριση Υπολογιστικού Κινδύνου: Η διαχείριση κινδύνου είναι κρίσιμη για τους παρόχους υπηρεσιών cloud computing, καθώς υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν την επίτευξη των SLA και, συνεπώς, την ικανοποίηση των πελατών. Όπως αναφέρατε, η διαχείριση κινδύνου περιλαμβάνει διάφορα βήματα:

- ✓ **Καθορισμός του Πλαισίου**: Σε αυτό το βήμα, πρέπει να καθοριστεί το πλαίσιο της διαχείρισης κινδύνου, περιλαμβάνοντας τους στόχους, τις προτεραιότητες και τους περιορισμούς. Αυτό βοηθά στην καθορισμό του εύρους της διαδικασίας.
- ✓ **Προσδιορισμός των Κινδύνων**: Στη συνέχεια, πρέπει να αναγνωριστούν οι κίνδυνοι που μπορεί να αντιμετωπίσει ο πάροχος υπηρεσιών. Αυτό μπορεί να περιλαμβάνει κινδύνους που αφορούν την ασφάλεια, τη διαθεσιμότητα, την απόδοση και άλλες πτυχές της υπηρεσίας.

- ✓ **Αξιολόγηση των Κινδύνων**: Αφού αναγνωρίσουμε τους κινδύνους, πρέπει να τους αξιολογήσουμε ως προς την πιθανότητα εμφάνισής τους και τις συνέπειές τους στον πάροχο και τους πελάτες.
- ✓ **Διαχείριση των Κινδύνων**: Σε αυτό το στάδιο, αναπτύσσονται στρατηγικές για τη διαχείριση κάθε κινδύνου. Αυτό μπορεί να περιλαμβάνει την υιοθέτηση τεχνικών, πολιτικών ή διαδικαστικών μέτρων για τη μείωση των κινδύνων.
- ✓ **Δημιουργία Συστήματος Διαχείρισης Κινδύνου**: Στο τελικό βήμα, δημιουργούμε ένα σύστημα διαχείρισης κινδύνου που θα συνεχίσει να εφαρμόζει και να επανεξετάζει το σχέδιο διαχείρισης κινδύνου καθ' όλη τη διάρκεια της παροχής των υπηρεσιών.

Η διαχείριση κινδύνου συμβάλλει στο να αναγνωρίζονται, να αντιμετωπίζονται και να μειώνονται οι κίνδυνοι που επηρεάζουν την ικανοποίηση των πελατών και την πληροφορική των υπηρεσιών cloud. Καθώς η αγορά εξελίσσεται και νέοι κίνδυνοι εμφανίζονται, η διαχείριση κινδύνου είναι μια συνεχής διαδικασία που πρέπει να ενσωματώνεται στις στρατηγικές διαχείρισης των παρόχων υπηρεσιών cloud.

Αυτόνομη Διαχείριση Πόρων: Η αυτονομία και η δυνατότητα προσαρμογής είναι κρίσιμες για την αποτελεσματική διαχείριση πόρων στο πλαίσιο του cloud computing, καθώς οι απαιτήσεις των χρηστών και οι συνθήκες λειτουργίας μπορεί να αλλάζουν συνεχώς. Αυτό απαιτεί αυτόνομα συστήματα που μπορούν να λαμβάνουν αποφάσεις για την παροχή υπηρεσιών και τη διαχείριση πόρων με βάση την τρέχουσα κατάσταση και τις ανάγκες των χρηστών. Αυτό μπορεί να επιτευχθεί με τη χρήση ευφυών αλγορίθμων και μηχανισμών που επιτρέπουν στα συστήματα να παρακολουθούν συνεχώς την απόδοσή τους και να προσαρμόζουν αυτόματα τη λειτουργία τους. Οι μηχανισμοί και οι ευφυείς αλγόριθμοι είναι σημαντικά για την επίτευξη αυτονομίας στα κέντρα δεδομένων του cloud. Οι προσωπικοί μεσάζοντες μπορούν να εκπροσωπούν τους χρήστες και να αλληλεπιδρούν με τους παρόχους υπηρεσιών για να επιλέξουν τις καλύτερες διαθέσιμες επιλογές. Επιπλέον, οι ευφυείς αλγόριθμοι μπορούν να χρησιμοποιηθούν για τη δυναμική διαχείριση πόρων και την αυτο-διαμόρφωση του συστήματος με βάση την ανάλυση της απόδοσης και την πρόβλεψη των αναγκών.

Η διαχείριση πόρων και η προσαρμογή στις αλλαγές στις απαιτήσεις υπηρεσιών αποτελούν θεμέλιο όλων των επιτυχημένων υπηρεσιών cloud, καθώς επιτρέπουν την

ευελιξία και την ικανοποίηση των χρηστών. Η χρήση της τεχνολογίας και των αλγορίθμων για την αυτονομία και την προσαρμογή είναι απαραίτητη για την αντιμετώπιση των προκλήσεων του cloud computing.

Κατανομή πόρων προσανατολισμένη σε SLA μέσω εικονικοποίησης: Η εικονικοποίηση και η χρήση εικονικών μηχανών (VMs) αποτελούν σημαντικά εργαλεία στον κόσμο του cloud computing. Όπως περιγράψαμε, οι VMs επιτρέπουν την απομόνωση και τη δυνατότητα παραμετροποίησης των εικονικών περιβαλλόντων, καθιστώντας δυνατή την αποτελεσματική κατανομή των πόρων σε αντίθεση με τις παραδοσιακές φυσικές μηχανές.

Οι κυριότερες προτεραιότητες και πλεονεκτήματα που προσφέρουν τα VMs στη διαχείριση πόρων περιλαμβάνουν:

Απομόνηση και ασφάλεια: Κάθε VM λειτουργεί σε ένα απομονωμένο περιβάλλον, δίνοντας τη δυνατότητα να τρέχουν διαφορετικά λειτουργικά συστήματα ή εφαρμογές χωρίς να αλληλεπιδρούν. Αυτό προσφέρει ασφάλεια και επιτρέπει την επίτευξη ορισμένων πολιτικών απομόνωσης.

Ευελιξία: Οι VMs μπορούν να δημιουργηθούν, να εκκινηθούν και να σταματήσουν δυναμικά, ανάλογα με τις ανάγκες. Αυτό επιτρέπει τη δυναμική προσαρμογή της χωρητικότητας πόρων για να ανταποκριθεί στη μεταβαλλόμενη ζήτηση.

Καλύτερη εκμετάλλευση πόρων: Επειδή μπορούν να διαμορφωθούν διάφορες πολιτικές διαχείρισης πόρων για κάθε VM, μπορούμε να εκχωρήσουμε διαφορετικά ποσοστά επεξεργαστικής ισχύος, μνήμης και άλλων πόρων ανάλογα με τις ανάγκες.

Όταν πρόκειται για τη διανομή πόρων προσανατολισμένη στα Service Level Agreements (SLAs), οι VMs μπορούν να είναι πολύ χρήσιμες. Μπορούμε να παραμετροποιήσουμε τις VMs για να πληρούν τις απαιτήσεις των SLAs των διαφόρων πελατών. Επιπλέον, η ευελιξία των VMs μας επιτρέπει να προσαρμόσουμε δυναμικά τη χωρητικότητα σύμφωνα με τη ζήτηση, βοηθώντας έτσι στην τήρηση των SLAs.

Συνολικά, η εικονικοποίηση μέσω VMs έχει αναδειχθεί σε ισχυρό εργαλείο για την αποτελεσματική διαχείριση πόρων στον κόσμο του cloud computing.

Συγκριτική αξιολόγηση και μέτρηση υπηρεσιών: Η ανάπτυξη ενός τυπικού συνόλου δεικτών αναφοράς για την αξιολόγηση των πολιτικών διαχείρισης πόρων στον τομέα του cloud computing είναι αναγκαία για να διευκολυνθεί ο ανταγωνισμός και να επιτραπεί στους χρήστες να επιλέξουν τις καταλληλότερες υπηρεσίες για τις ανάγκες τους. Η Κοινοπραξία Δείκτης Μέτρησης Υπηρεσιών Cloud (CSMIC) αναγνωρίζει τη σημασία των δεικτών μέτρησης (SMIs) για αυτόν τον σκοπό.

Οι SMIs μπορούν να αντιπροσωπεύουν διάφορες απαιτήσεις και παράμετρους που έχουν σημασία για τους χρήστες και τις εφαρμογές τους. Μερικοί δείκτες μέτρησης που θα μπορούσαν να συμπεριληφθούν σε ένα τυπικό σύνολο δεικτών αναφοράς για το cloud computing περιλαμβάνουν:

Διαθεσιμότητα: Αυτός ο δείκτης αξιολογεί τη διαθεσιμότητα των υπηρεσιών στο cloud, επιδιώκοντας να μετρήσει τον χρόνο κατά τον οποίο οι υπηρεσίες είναι διαθέσιμες και λειτουργούν αναλλόλυτα.

Απόδοση: Η απόδοση μπορεί να μετρηθεί με δείκτες όπως η ταχύτητα ανταπόκρισης, ο χρόνος φόρτωσης και άλλες μετρήσιμες παραμέτρους που αφορούν την απόδοση της υπηρεσίας.

Ασφάλεια και αξιοπιστία: Δείκτες σχετικοί με την ασφάλεια των δεδομένων και την αξιοπιστία των υπηρεσιών, συμπεριλαμβανομένων των μέτρων ασφαλείας και των συχνοτήτων αναφορών σφαλμάτων.

Κόστος: Οι δείκτες σχετικοί με το κόστος χρήσης των υπηρεσιών, όπως η τιμή κατανάλωσης πόρων, τα κόστη υπηρεσιών, και άλλοι σχετικοί δείκτες.

Ελαστικότητα: Οι δείκτες που αξιολογούν τη δυνατότητα ευελιξίας και κλιμακοποίησης των υπηρεσιών για να ανταποκριθούν στις μεταβαλλόμενες ανάγκες.

Αυτοί οι δείκτες μπορούν να αναλυθούν περαιτέρω σε προδιαγραφές ώστε να προσφέρουν πληροφορίες σχετικά με τις απαιτήσεις εφαρμογών και υπηρεσιών. Αυτό

θα επιτρέψει στους χρήστες να αξιολογήσουν πιο αποτελεσματικά τις υπηρεσίες των παρόχων cloud και να επιλέξουν ανάλογα.

Μοντελοποίηση Συστήματος και Επαναληπτική Αξιολόγηση: Η χρήση προσομοιώσεων διακριτών γεγονότων είναι μια αποτελεσματική προσέγγιση για την αξιολόγηση της απόδοσης στρατηγικών διαχείρισης πόρων στον χώρο του cloud computing. Αυτές οι προσομοιώσεις μπορούν να αντιπροσωπεύουν το σύστημα με ρεαλιστικά μοντέλα και δεδομένα και να επιτρέπουν την αξιολόγηση της συμπεριφοράς του στον χρόνο και κάτω από διάφορες συνθήκες. Εδώ είναι ορισμένα βήματα που μπορούμε να ακολουθήσουμε κατά τη χρήση προσομοιώσεων για την αξιολόγηση των στρατηγικών διαχείρισης πόρων:

- ✓ **Καθορίστε τα μοντέλα:** Πρέπει να καθορίσουμε τα μοντέλα που θα χρησιμοποιηθούν για την προσομοίωση, συμπεριλαμβανομένων των μοντέλων διαφορετικών τύπων πόρων, πελατών και αιτημάτων υπηρεσιών.
- ✓ **Ορίστε σενάρια:** Δημιουργούμε διάφορα σενάρια που αντιπροσωπεύουν διάφορες καταστάσεις χρήσης και αντίδρασης στις διαφορετικές στρατηγικές διαχείρισης πόρων.
- ✓ **Συλλέξτε πραγματικά δεδομένα:** Συλλέγουμε πραγματικά δεδομένα από το σύστημα, όπως τη ζήτηση πόρων, τη διαθεσιμότητα, την απόδοση, και τις δραστηριότητες των πελατών.
- ✓ **Δημιουργία προσομοιώσεων:** Χρησιμοποιούμε τα μοντέλα και τα δεδομένα για να δημιουργήσουμε προσομοιώσεις όπου μπορούμε να εκτελέσουμε διάφορες στρατηγικές διαχείρισης πόρων.
- ✓ **Αξιολόγηση και σύγκριση:** Συγκρίνουμε τα αποτελέσματα από τις διάφορες προσομοιώσεις για να αξιολογήσουμε την απόδοση των στρατηγικών.
- ✓ **Προσαρμογή και βελτίωση:** Βασιζόμενοι στα αποτελέσματα, μπορούμε να προσαρμόσουμε και να βελτιώσουμε τις στρατηγικές διαχείρισης πόρων και να εξετάσουμε τον τρόπο με τον οποίο επηρεάζουν τη συνολική απόδοση.

Η χρήση προσομοιώσεων μας επιτρέπει να αξιολογήσουμε τις στρατηγικές διαχείρισης πόρων σε ένα ασφαλές και ελεγχόμενο περιβάλλον πριν τις εφαρμόσουμε στον πραγματικό κόσμο. Επίσης, μπορούμε να προβλέψουμε τον τρόπο με τον οποίο οι στρατηγικές θα αντιδράσουν σε μελλοντικές αλλαγές στις απαιτήσεις και τους πόρους.

4.3 SLAs και οι πάροχοι νεφών

Είναι κατανοητό ότι τονίζεται η σημασία της προσαρμοστικότητας και της ευελιξίας όσον αφορά την κατανομή πόρων σε κέντρα δεδομένων Cloud και την ανταπόκριση στις αλλαγές στις απαιτήσεις των πελατών. Αυτό είναι ένα πολύ σημαντικό ζήτημα στον χώρο του cloud computing και είναι απαραίτητο για τη διατήρηση και βελτίωση της ποιότητας των υπηρεσιών. Εδώ είναι μερικά βήματα που μπορούν να βοηθήσουν στην επίτευξη αυτής της στόχευσης:

Δυναμική προσαρμογή: Οι στρατηγικές διαχείρισης πόρων πρέπει να είναι σε θέση να αντιδρούν δυναμικά στις αλλαγές στις απαιτήσεις των πελατών. Αυτό μπορεί να επιτευχθεί μέσω αυτόματης επαναδιαμόρφωσης των πόρων στο κέντρο δεδομένων Ŧ μετακίνηση, επαναδιαμόρφωση και κλιμακούνται όπως απαιτείται.

Αυτόματος εντοπισμός και πρόβλεψη: Χρησιμοποιήστε συστήματα παρακολούθησης και ανάλυσης για την παρακολούθηση των απαιτήσεων των πελατών και την πρόβλεψη των μελλοντικών αλλαγών.

Πολιτικές διαχείρισης: Αναπτύξτε πολιτικές διαχείρισης πόρων που βασίζονται σε πρότυπα SLA και παρέχουν ευελιξία για την προσαρμογή των πόρων.

Διαχείριση αξιοπιστίας και ασφάλειας: Η διατήρηση και βελτίωση της αξιοπιστίας και της ασφάλειας πρέπει να είναι στο επίκεντρο της στρατηγικής, καθώς αυτές είναι κρίσιμες παράμετροι για πολλούς πελάτες.

Επικοινωνία με τους πελάτες: Διατηρήστε ανοιχτές γραμμές επικοινωνίας με τους πελάτες και λαμβάνουμε υπόψη τις ανάγκες και τα αιτήματά τους για τη συνεχή βελτίωση των υπηρεσιών.

Συνεχής εκπαίδευση: Η εκπαίδευση του προσωπικού σχετικά με τις νέες τεχνολογίες και τις τεχνικές διαχείρισης πόρων είναι σημαντική για την επίτευξη των στόχων μας.

Με αυτές τις προσεγγίσεις, ένα κέντρο δεδομένων Cloud μπορεί να είναι πιο ανταγωνιστικό, πιο ευέλικτο και πιο προσανατολισμένο στις ανάγκες των πελατών του. Η προσέγγιση για την υλοποίηση αυτού του ερευνητικού οράματος συνίσταται στο ότι οι στρατηγικές που περιγράφουμε είναι σημαντικές για τη διαχείριση των υπηρεσιών σε ένα περιβάλλον Cloud. Ας αναλύσουμε κάθε ένα από αυτά τα σημεία:

- **Υποστήριξη για διαχείριση υπηρεσιών με γνώμονα τον πελάτη:** Ο προσανατολισμός στον πελάτη είναι κρίσιμος. Η προσαρμογή των υπηρεσιών

στις ανάγκες τους και ο υπολογισμός τους βάσει των προφίλ και των απαιτήσεών τους (QoS) είναι βασικός παράγοντας για την επιτυχία σε ένα περιβάλλον Cloud.

- **Διαχείριση υπολογιστικού κινδύνου:** Η αναγνώριση, αξιολόγηση και διαχείριση των υπολογιστικών κινδύνων είναι ουσιώδης για τη διασφάλιση της ασφάλειας και της αξιοπιστίας των υπηρεσιών. Οι κίνδυνοι μπορεί να πηγάζουν από διάφορες πηγές, όπως κακόβουλη επίθεση, ανεπάρκεια πόρων και πολλά άλλα.
- **Στρατηγικές διαχείρισης πόρων βασισμένες στην αγορά:** Ο συνδυασμός της διαχείρισης υπηρεσιών με γνώμονα τον πελάτη και της υπολογιστικής διαχείρισης κινδύνου μπορεί να διασφαλίσει ότι οι πόροι ανατίθενται αποτελεσματικά και ασφαλώς σύμφωνα με τις ανάγκες της αγοράς και των πελατών.
- **Ενσωμάτωση μοντέλων αυτόνομης διαχείρισης πόρων:** Η αυτοματοποίηση είναι σημαντική για τη διαχείριση πόρων σε ένα περιβάλλον Cloud. Μπορεί να επιτρέπει τη δυναμική εκχώρηση πόρων, ανάλογα με τις αλλαγές στις απαιτήσεις των υπηρεσιών.
- **Χρήση της τεχνολογίας Virtual Machine (VM):** Οι VM παρέχουν ευελιξία και δυνατότητα δυναμικής εκχώρησης πόρων. Η χρήση τους είναι κρίσιμη για την αποτελεσματική διαχείριση πόρων σε ένα κέντρο δεδομένων Cloud.

Συνολικά, αυτές οι στρατηγικές μπορούν να βοηθήσουν στην επίτευξη των απαιτήσεων των πελατών και τη διατήρηση ενός υψηλού επιπέδου απόδοσης και ασφάλειας σε ένα περιβάλλον Cloud.

SLA του Amazon AWS

Είναι σημαντικό να γνωρίζουμε πώς χειρίζεται το AWS το Service Level Agreement (SLA) για τις διάφορες υπηρεσίες τους, όπως το EC2, το S3, το Route 53 και το CloudFront. Το SLA αυτό καθορίζει τα ποσοστά διαθεσιμότητας και τις αποζημιώσεις σε περίπτωση διακοπής των υπηρεσιών. Εδώ είναι μια περίληψη των SLA για κάθε υπηρεσία:

- ✓ **EC2 (Elastic Compute Cloud):**

- Διαθεσιμότητα: Το AWS εγγυάται τουλάχιστον το 99.95% διαθεσιμότητας του EC2 κάθε μήνα. Αυτό σημαίνει ότι οι παρουσίες EC2 θα είναι διαθέσιμες σε αυτό το ποσοστό του χρόνου.
- Αποζημίωση: Αν η διαθεσιμότητα μειωθεί κάτω από 99.95%, ο πελάτης λαμβάνει αποζημίωση. Οι ποσοστώσεις της αποζημίωσης εξαρτώνται από τον χρόνο διακοπής.

✓ **S3 (Simple Storage Service):**

- Διαθεσιμότητα: Το AWS εγγυάται τουλάχιστον το 99.9% διαθεσιμότητας του S3 κατά την ανάγνωση ή την εγγραφή δεδομένων.
- Αποζημίωση: Αν η διαθεσιμότητα μειωθεί, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.

✓ **Route 53 (Amazon DNS):**

- Διαθεσιμότητα: Το AWS εγγυάται το 100% διαθεσιμότητας του Route 53. Αυτό σημαίνει ότι η υπηρεσία θα είναι πάντα διαθέσιμη.
- Αποζημίωση: Σε περίπτωση διακοπής, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τη διάρκεια της διακοπής.

✓ **CloudFront:**

- Διαθεσιμότητα: Το AWS εγγυάται τουλάχιστον το 99.9% διαθεσιμότητας του CloudFront.
- Αποζημίωση: Αν η διαθεσιμότητα μειωθεί κάτω από 99.9%, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.

Αυτές οι πολιτικές SLA διασφαλίζουν ότι οι πελάτες του AWS έχουν πρόσβαση σε υψηλής ποιότητας υπηρεσίες και λαμβάνουν αποζημιώσεις σε περίπτωση διακοπής ή μειωμένης διαθεσιμότητας.

SLA του Microsoft Azure

Το Microsoft Azure προσφέρει διάφορες υπηρεσίες, και το Service Level Agreement (SLA) παίζει σημαντικό ρόλο για να διασφαλίσει τη διαθεσιμότητα και την αξιοπιστία

των υπηρεσιών αυτών. Εδώ είναι μια περίληψη του πώς το Azure χειρίζεται το SLA για τις τέσσερις σημαντικές υπηρεσίες που αναφέρατε:

- ✓ **Virtual Machines (VM) στο Azure:**
    - Διαθεσιμότητα: Το Azure εγγυάται τουλάχιστον το 99.95% διαθεσιμότητας για τις VM. Αυτό σημαίνει ότι οι VM θα είναι διαθέσιμες σε αυτό το ποσοστό του χρόνου.
    - Αποζημίωση: Αν η διαθεσιμότητα μειωθεί κάτω από το 99.95%, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.
- ✓ **Azure Storage:**
    - Διαθεσιμότητα: Το Azure εγγυάται τουλάχιστον το 99.9% διαθεσιμότητας για την ανάγνωση και την εγγραφή δεδομένων στο Azure Storage.
    - Αποζημίωση: Αν η διαθεσιμότητα μειωθεί, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.
- ✓ **Διαχειριστής επισκεψιμότητας (Azure Traffic Manager):**
    - Διαθεσιμότητα: Το Azure εγγυάται το 99.99% διαθεσιμότητας για το Azure Traffic Manager.
    - Αποζημίωση: Σε περίπτωση διακοπής, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.
- ✓ **Azure CDN (Content Delivery Network):**
    - Διαθεσιμότητα: Το Azure CDN εγγυάται τουλάχιστον το 99.99% διαθεσιμότητας.
    - Αποζημίωση: Αν η διαθεσιμότητα μειωθεί κάτω από το 99.99%, ο πελάτης λαμβάνει αποζημίωση ανάλογα με τον χρόνο διακοπής.

Αυτές οι πολιτικές SLA εξασφαλίζουν ότι οι πελάτες του Azure έχουν πρόσβαση σε υψηλής ποιότητας υπηρεσίες και λαμβάνουν αποζημιώσεις σε περίπτωση διακοπής ή μειωμένης διαθεσιμότητας. Αυτό βοηθάει τις επιχειρήσεις να διατηρούν υψηλό επίπεδο υπηρεσιών για τους πελάτες τους.

SLA του νέφους Rackspace

Το Rackspace παρέχει διάφορες υπηρεσίες υπολογιστικής υποδομής, συμπεριλαμβανομένων των Cloud Servers και των υπηρεσιών αποθήκευσης όπως το Cloud Block Storage και το Cloud Files. Τα Service Level Agreements (SLAs) που παρέχει το Rackspace για αυτές τις υπηρεσίες περιλαμβάνουν τα ακόλουθα:

- ✓ **Cloud Servers (επόμενης γενιάς):**
    - **Διαθεσιμότητα Διαχείρισης:** Η εγγύηση υπηρεσίας υπολογίζεται με βάση το ποσοστό επιτυχημένων αιτημάτων στη στοίβα διαχείρισης. Εάν αυτό το ποσοστό είναι κάτω από 99%, ο πελάτης λαμβάνει αποζημίωση.
    - **Εγγύηση Υπηρεσίας Δικτύου:** Το δίκτυο του κέντρου δεδομένων, το HVAC και η ισχύς είναι υποχρεωτικά διαθέσιμα τουλάχιστον στο 99.95% του χρόνου. Εκτός από την προγραμματισμένη συντήρηση, αυτές οι υπηρεσίες πρέπει να είναι διαθέσιμες για τουλάχιστον το 99.95% του χρόνου.
- ✓ **Cloud Block Storage και Cloud Files:**
    - Τα SLAs για αυτές τις υπηρεσίες περιλαμβάνουν εγγυήσεις για τη διαθεσιμότητα και την απόκριση του δικτύου εκτός του κέντρου δεδομένων.
    - Σε περίπτωση που υπάρξουν διακοπές στη διαθεσιμότητα εκτός του κέντρου δεδομένων, αυτές οι διακοπές δεν υπολογίζονται στο SLA.

Είναι σημαντικό να προσέξουμε τις παρεμπίπτουσες συνθήκες, όπως η προγραμματισμένη συντήρηση και η ανακοίνωση προς τους πελάτες. Αυτά τα SLAs στοχεύουν στη διασφάλιση της διαθεσιμότητας και της αξιοπιστίας των υπηρεσιών που παρέχονται από το Rackspace και προσφέρουν αποζημίωση σε περίπτωση παραβάσεων των εγγυήσεων υπηρεσίας. Οι λεπτομέρειες που παρουσιάσατε σχετικά με το SLA του Rackspace για τις υπηρεσίες Cloud Servers προσφέρουν μια καλή εικόνα για τη διαθεσιμότητα και την αξιοπιστία των υπηρεσιών τους. Είναι σημαντικό για τους πελάτες να γνωρίζουν πώς το Rackspace αντιμετωπίζει τις εκτάκτως αναγκαίες καταστάσεις, καθώς και τι προσφέρει σε περίπτωση προβλημάτων.

Σύγκριση με άλλες μεγάλες υπηρεσίες cloud όπως το AWS και το Azure, είναι αλήθεια ότι υπάρχουν διαφορές στα SLA τους. Τα πρότυπα SLA διαφέρουν ανάλογα με τον

πάροχο υπηρεσιών, τις υπηρεσίες που παρέχουν, και τον τρόπο με τον οποίο αξιολογούν τη διαθεσιμότητα. Οι χρήστες πρέπει να εξετάσουν τις ανάγκες και τις απαιτήσεις τους για να αποφασίσουν ποιος πάροχος ταιριάζει καλύτερα στις δικές τους ανάγκες. Σημαντικό είναι να ληφθούν υπόψη και άλλοι παράγοντες πέρα από τα SLA, όπως η τιμή, η ευελιξία, οι υπηρεσίες που προσφέρονται, και η υποστήριξη πελατών. Επίσης, η επικοινωνία και η συνεργασία με τον πάροχο υπηρεσιών σε περίπτωση προβλημάτων είναι σημαντικές. Κάθε πάροχος έχει τα πλεονεκτήματά του και τις μοναδικές χαρακτηριστικές των υπηρεσιών του, και οι χρήστες πρέπει να επιλέξουν βάσει των αναγκών και των προτεραιοτήτων τους. Η αυστηρότητα των SLA είναι σημαντική για την εκτίμηση της αξιοπιστίας και της διαθεσιμότητας μιας υπηρεσίας cloud. Στην περίπτωση του Rackspace, η αυστηρότητα της εγγύησης υπηρεσίας μπορεί να εξαρτάται από το ποιοι πόροι αξιολογούνται, το χρονικό πλαίσιο, και τον τρόπο μέτρησης της απόδοσης.

Εάν η εγγύηση υπηρεσίας βασίζεται στην απόδοση ενός συγκεκριμένου πόρου σε μια σύντομη χρονική περίοδο, όπως το παράδειγμα που δώσατε για τις συναλλαγές μνήμης σε ένα διάστημα 5 λεπτών, τότε αυτή η εγγύηση είναι αυστηρή και απαιτεί υψηλή αξιοπιστία για τον συγκεκριμένο πόρο κατά τη διάρκεια της συγκεκριμένης χρονικής περιόδου. Αυτό είναι σημαντικό για εφαρμογές που απαιτούν σταθερή και υψηλή απόδοση σε σύντομα διαστήματα. Αντίθετα, εάν μια εγγύηση υπηρεσίας μετρά την απόδοση σε μεγαλύτερα χρονικά πλαίσια ή για ομάδες πόρων, τότε η εγγύηση μπορεί να είναι λιγότερο αυστηρή, αλλά πιο κατάλληλη για εφαρμογές με πιο χαλαρές απαιτήσεις στην απόδοση. Οι πάροχοι cloud προσαρμόζουν τα SLA τους για να καλύψουν τις ανάγκες των διαφόρων πελατών. Κρίσιμες εφαρμογές με υψηλές απαιτήσεις ως προς τη διαθεσιμότητα και την ακρίβεια ίσως απαιτούν πιο αυστηρά SLA και επιπλέον μέτρα ασφαλείας. Επομένως, η αυστηρότητα των SLA πρέπει να αντικατοπτρίζει τις απαιτήσεις των εφαρμογών και των επιχειρήσεων που χρησιμοποιούν τις υπηρεσίες cloud.

Κεφάλαιο 5: Ασφάλεια δεδομένων και αποθήκευση

5.1 Περιπτώσεις ακεραιότητας δεδομένων

Η ακεραιότητα των δεδομένων είναι μια από τις βασικές αρχές της ασφάλειας των δεδομένων και της πληροφορικής γενικότερα. Η διατήρηση της ακεραιότητας των δεδομένων είναι σημαντική για να αποφευχθούν οι ανεξουσιοδοτημένες τροποποιήσεις και οι καταχρήσεις. Αυτό ισχύει τόσο σε αυτόνομα συστήματα όσο και στο πλαίσιο του cloud computing. Στον τομέα του cloud computing, η ακεραιότητα των δεδομένων είναι σημαντική, καθώς τα δεδομένα αποθηκεύονται και διαχειρίζονται σε απομακρυσμένες υπηρεσίες και υποδομές. Η χρήση τεχνικών όπως ο έλεγχος πρόσβασης και η κρυπτογράφηση βοηθά στην εξασφάλιση της ακεραιότητας των δεδομένων.

Ο έλεγχος πρόσβασης διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα και μπορούν να πραγματοποιήσουν αλλαγές. Αυτό περιορίζει τον κίνδυνο μη εξουσιοδοτημένης τροποποίησης των δεδομένων. Η κρυπτογράφηση είναι επίσης σημαντική για την ασφάλεια των δεδομένων στο cloud computing. Οι δεδομένοι κρυπτογραφούνται κατά τη μεταφορά και κατά την αποθήκευσή τους, καθιστώντας δύσκολη την πρόσβαση από μη εξουσιοδοτημένους. Αυτό προστατεύει την ακεραιότητα των δεδομένων από πιθανές παρεμβάσεις. Συνολικά, οι προσεγγίσεις αυτές συμβάλλουν στη διασφάλιση της ακεραιότητας των δεδομένων στο cloud computing, βοηθώντας τους χρήστες να εμπιστευθούν περισσότερο τις υπηρεσίες cloud και να αποφύγουν ανεπιθύμητες παρεμβάσεις στα δεδομένα τους.

Η ακεραιότητα των δεδομένων είναι πραγματικά κρίσιμη για την προστασία της ακρίβειας και της αξιοπιστίας των πληροφοριών σε περιβάλλοντα cloud computing. Η εξουσιοδότηση, όπως αναφέρατε, παίζει σημαντικό ρόλο στη διαχείριση της πρόσβασης σε αυτά τα δεδομένα. Μερικοί τρόποι που μπορούν να διασφαλίσουν την ακεραιότητα των δεδομένων στο πλαίσιο του cloud computing περιλαμβάνουν:

Έλεγχος πρόσβασης: Αυτός ο μηχανισμός καθορίζει ποιοι χρήστες έχουν πρόσβαση στα δεδομένα και με ποιες άδειες. Η αυστηρή διαχείριση των δικαιωμάτων πρόσβασης μειώνει τον κίνδυνο ανεξουσιοδοτημένης πρόσβασης.

Κρυπτογράφηση: Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί κατά τη μεταφορά και την αποθήκευση δεδομένων. Αυτό καθιστά τα δεδομένα ανεπίληπτα σε περίπτωση ανεξουσιοδοτημένης πρόσβασης.

Παρακολούθηση και ελέγχους: Οι προηγμένες λύσεις παρακολούθησης και ανίχνευσης επιτρέπουν την παρακολούθηση της αλληλεπίδρασης με τα δεδομένα και την ανίχνευση ακανθών. Αυτό μπορεί να βοηθήσει στον προσδιορισμό ανεξουσιοδοτημένων ενεργειών.

Συστήματα ψηφιακής υπογραφής: Οι ζψηφιακές υπογραφές είναι ένας τρόπος επαλήθευσης της ακεραιότητας των δεδομένων. Υπογράφουν τα δεδομένα και επιτρέπουν στους άλλους να επαληθεύσουν ότι δεν έχουν τροποποιηθεί.

Αντίγραφα ασφαλείας: Οι αντίγραφα ασφαλείας δεδομένων είναι σημαντικά για την αποφυγή απώλειας δεδομένων λόγω ατυχημάτων ή κακόβουλων επιθέσεων. Τα τακτικά αντίγραφα ασφαλείας επιτρέπουν την ανακτησιμότητα των δεδομένων ακόμη και αν προκύψουν προβλήματα.

Η χρήση αυτών των μηχανισμών σε συνδυασμό μπορεί να διασφαλίσει ότι τα δεδομένα στο cloud computing παραμένουν ακέραια και αξιόπιστα, διατηρώντας την εμπιστοσύνη των χρηστών και των επιχειρήσεων στην ασφάλεια των υπηρεσιών cloud. Η διατήρηση του απορρήτου των δεδομένων στο cloud computing είναι πραγματικά σημαντική για τους χρήστες, ειδικά όταν πρόκειται για προσωπικά ή εμπιστευτικά δεδομένα. Όπως αναφέραμε, η κρυπτογράφηση είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για τη διατήρηση του απορρήτου των δεδομένων στο cloud, αλλά υπάρχουν και άλλες στρατηγικές που μπορούν να ενισχύσουν την ασφάλεια και την εμπιστοσύνη των χρηστών στο cloud computing:

Ελέγχος Ταυτότητας: Η χρήση ισχυρών μεθόδων ελέγχου ταυτότητας, όπως πολυπαράγοντες ελέγχου και πολυεπίπεδες ταυτότητες, μπορεί να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα. Οι τεχνικές, όπως η πολυπαράγοντη ταυτοποίηση, προσφέρουν επιπλέον επίπεδο ασφάλειας.

Ελέγχος Πρόσβασης: Οι πολιτικές ελέγχου πρόσβασης είναι κρίσιμες για τον περιορισμό της πρόσβασης σε δεδομένα μόνο στους αποδεκτούς χρήστες. Οι πολιτικές

αυτές πρέπει να είναι αυστηρές και να προσδιορίζουν ποιος έχει πρόσβαση σε ποια δεδομένα και για ποιο χρονικό διάστημα.

Επιθεώρηση και παρακολούθηση: Οι προχωρημένες λύσεις παρακολούθησης και ανίχνευσης επιτρέπουν την παρακολούθηση των αλληλεπιδράσεων με τα δεδομένα και την ανίχνευση ανωμαλιών. Αυτές οι λύσεις μπορούν να προειδοποιήσουν για πιθανές απειλές.

Εξουσιοδότηση τρίτων: Οι ανεξάρτητοι ελεγκτές μπορούν να επιβεβαιώσουν τη συμμόρφωση του παρόχου cloud με τις απαιτήσεις ασφάλειας. Οι ανεξάρτητες αξιολογήσεις μπορούν να ενισχύσουν την εμπιστοσύνη των χρηστών.

Ενημερωμένη κρυπτογράφηση: Η χρήση προηγμένων τεχνικών κρυπτογράφησης, όπως η κρυπτογράφηση με πλειόμετρα ή η κρυπτογράφηση των δεδομένων κατά την αποθήκευση, μπορεί να προστατέψει τα δεδομένα από ανεξουσιοδοτημένη πρόσβαση.

Συνδυάζοντας αυτές τις στρατηγικές, μπορούν να επιτευχθούν υψηλά επίπεδα ασφάλειας και εμπιστοσύνης στο cloud computing, καθιστώντας τον πιο αξιόπιστο για την αποθήκευση τόσο προσωπικών όσο και επαγγελματικών δεδομένων.

5.2 Απόρρητο & προστασία προσωπικών δεδομένων

Το απόρρητο των δεδομένων είναι ένα ζωτικό στοιχείο στον ψηφιακό κόσμο, καθώς αφορά τη διατήρηση της ιδιωτικότητας και του έλεγχου των προσωπικών και εμπιστευτικών πληροφοριών. Η τεχνολογία Oblivious RAM (ORAM) αναδεικνύεται ως ισχυρό εργαλείο για τη διατήρηση του απορρήτου των δεδομένων στο cloud computing. Οι αλγόριθμοι ORAM επιτρέπουν στους χρήστες να αποθηκεύουν και να ανακτούν δεδομένα στο cloud χωρίς να αποκαλύπτουν τις προτιμήσεις ή τις προσβάσεις τους. Τα στοιχεία που περιγράφονται σχετικά με το απόρρητο είναι σημαντικά, καθώς καθορίζουν το πώς οι χρήστες επιθυμούν να προστατεύσουν τις πληροφορίες τους. Οι αλγόριθμοι ORAM παρέχουν έναν τρόπο να διατηρηθεί το απόρρητο των δεδομένων, δηλαδή, πότε, πώς και με ποιον τρόπο τα δεδομένα προσπελάζονται, χωρίς να αποκαλύπτεται η πραγματική πληροφορία.

Οι αλγόριθμοι ORAM έχουν ευρεία χρήση, κυρίως στην προστασία του απορρήτου στο cloud computing. Παρέχουν τη δυνατότητα στους χρήστες να αποθηκεύουν και να ανακτούν δεδομένα αποτελεσματικά, διατηρώντας την εμπιστευτικότητα και τον

έλεγχο πάνω στα δεδομένα τους. Αυτό είναι κρίσιμο στον ψηφιακό κόσμο, όπου η απορρήτου των δεδομένων είναι υψίστης σημασίας. Τα ζητήματα απορρήτου στον τομέα του cloud computing μπορούν πράγματι να διακριθούν σε διάφορες υποκατηγορίες, όπως αναφέραμε, λαμβάνοντας υπόψη τον τρόπο που τα δεδομένα αντιμετωπίζονται σε διάφορες καταστάσεις. Αυτές οι υποκατηγορίες μπορούν να συνοψιστούν ως εξής:

Αποθηκευμένα Δεδομένα (Data at Rest): Αφορούν τα δεδομένα που αποθηκεύονται στο cloud, δηλαδή όταν αυτά βρίσκονται σε κατάσταση αδράνειας. Σε αυτήν την περίπτωση, τα μέτρα ασφάλειας περιλαμβάνουν την κρυπτογράφηση των δεδομένων κατά την αποθήκευση.

Δεδομένα κατά τη Μεταφορά (Data in Transit): Πρόκειται για τα δεδομένα που μεταδίδονται ανάμεσα στον χρήστη και τον cloud υπάροντα ή ανάμεσα σε διάφορες υπηρεσίες του cloud. Εδώ, κρίνεται σημαντικό να χρησιμοποιείται ασφαλής μεταφορά, συνήθως μέσω πρωτοκόλλων όπως το HTTPS.

Δεδομένα σε Χρήση (Data in Use): Σε αυτήν την περίπτωση, τα δεδομένα βρίσκονται σε ενεργή χρήση κατά την επεξεργασία από τις υπηρεσίες του cloud. Είναι σημαντικό να ελεγχθεί ποιος έχει πρόσβαση σε αυτά τα δεδομένα και πώς χρησιμοποιούνται.

Νομικές Απαιτήσεις: Σε ορισμένες περιπτώσεις, η αποθήκευση και η επεξεργασία δεδομένων στο cloud υπάγονται σε νομικές απαιτήσεις όπως οι νομοθεσίες περί προστασίας δεδομένων. Σε αυτές τις περιπτώσεις, οι χρήστες πρέπει να εξασφαλίσουν ότι οι παρόχοι cloud συμμορφώνονται με τις απαιτήσεις αυτές.

Καθένα από αυτά τα σενάρια απαιτεί διαφορετικά μέτρα ασφαλείας και προσεγγίσεις για τη διατήρηση του απορρήτου των δεδομένων στο cloud. Η κρυπτογράφηση, ο έλεγχος πρόσβασης, οι νομικές συμμορφώσεις και η χρήση ασφαλών πρωτοκόλλων μεταφοράς είναι ορισμένες από τις βασικές αρχές που εφαρμόζονται για τη διασφάλιση του απορρήτου στον ψηφιακό χώρο του cloud computing.

Data-at-rest: Η αποθήκευση δεδομένων στο cloud προσφέρει πολλά πλεονεκτήματα, όπως τη δυνατότητα πρόσβασης από οπουδήποτε και τη μείωση του κόστους, όπως αναφέρατε. Ωστόσο, είναι σημαντικό να αντιμετωπίζονται και να αναγνωρίζονται οι κίνδυνοι που ενδέχεται να συνοδεύουν την αποθήκευση δεδομένων στο cloud. Οι βασικοί κίνδυνοι σχετίζονται με την ασφάλεια, τον έλεγχο και την απορρήτου των δεδομένων. Ας εξετάσουμε πιο αναλυτικά τους κινδύνους που αναφέρνται:

- ✓ **Κίνδυνοι Σχετιζόμενοι με την Κοινή Χρήση Μέσων Αποθήκευσης**: Οι κίνδυνοι αυτοί σχετίζονται με την πιθανότητα της εσφαλμένης χρήσης ή της κακής χρήσης των δεδομένων από ανθρώπους που έχουν πρόσβαση σε αυτά. Είναι σημαντικό να γίνεται έλεγχος ποιος έχει πρόσβαση στα δεδομένα μας, να εφαρμόζουμε συνθήκες χρήσης, και να παρακολουθούμε την δραστηριότητα πρόσβασης.
- ✓ **Κίνδυνοι Σχετιζόμενοι με την Τοποθεσία Δεδομένων**: Η τοποθεσία όπου αποθηκεύονται τα δεδομένα είναι σημαντική για την νομική συμμόρφωση και την απορρήτου. Κάποιες χώρες έχουν αυστηρές προδιαγραφές σχετικά με την αποθήκευση και την επεξεργασία προσωπικών δεδομένων. Είναι σημαντικό να γνωρίζουμε πού αποθηκεύονται τα δεδομένα μας και αν τηρούνται οι απαιτήσεις αυτών των νόμων.
- ✓ **Κίνδυνοι Σχετιζόμενοι με την Αξιοπιστία των Μέσων Αποθήκευσης**: Επιπλέον, υπάρχει ο κίνδυνος της απώλειας δεδομένων λόγω βλάβης των μέσων αποθήκευσης, αποτυχίας του παρόχου cloud, ή αποδυνάμωσης της αξιοπιστίας. Σε αυτήν την περίπτωση, η τακτική δημιουργία αντιγράφων ασφαλείας είναι σημαντική για την προστασία των δεδομένων μας.

Για την ασφάλεια των δεδομένων μας, πρέπει να εφαρμόζουμε τα κατάλληλα μέτρα, όπως κρυπτογράφηση, διαχείριση της πρόσβασης και συμμόρφωση με τους νόμους περί προστασίας δεδομένων. Επίσης, η τακτική παρακολούθηση και ενημέρωση για τις απειλές στην ασφάλεια των δεδομένων στο cloud είναι σημαντική για τη διασφάλιση της ασφάλειας των προσωπικών μας πληροφοριών.

Data-in-transit: Η ασφάλεια κατά τη μεταφορά δεδομένων είναι απαραίτητη για την προστασία των ευαίσθητων πληροφοριών κατά τη μετάδοσή τους από τον χρήστη στον cloud ή μεταξύ διαφόρων υπηρεσιών cloud. Καθώς τα δεδομένα ταξιδεύουν μέσω δικτύων, υπάρχει πολύ μεγαλύτερη πιθανότητα να αντιμετωπιστούν κίνδυνοι όπως η υποκλοπή, η τροποποίηση ή η αντικατάσταση των δεδομένων. Ορισμένα από τα σημαντικά μέτρα για την ασφάλεια κατά τη μεταφορά δεδομένων στο cloud περιλαμβάνουν:

- ✓ **Κρυπτογράφηση:** Η κρυπτογράφηση είναι ένα σημαντικό μέτρο ασφαλείας κατά τη μεταφορά δεδομένων. Τα δεδομένα πρέπει να κρυπτογραφούν πριν αποσταλούν και να αποκρυπτογραφούν μόνο στον προορισμό. Η χρήση

ασφαλών πρωτοκόλλων μεταφοράς, όπως το HTTPS, είναι σημαντική για την προστασία των επικοινωνιών.

- ✓ **Πιστοποιητικά:** Βεβαιωθείτε ότι συνδέεστε με αξιόπιστες υπηρεσίες cloud που χρησιμοποιούν πιστοποιητικά ασφαλείας. Αυτά τα πιστοποιητικά επιβεβαιώνουν την αυθεντικότητα των υπηρεσιών και προστατεύουν από επιθέσεις MITM (Man-in-the-Middle).
- ✓ **Ενημέρωση λογισμικού:** Επιβεβαιώστε ότι το λογισμικό και τα λειτουργικά συστήματά μας είναι ενημερωμένα, καθώς οι ενημερώσεις συχνά περιλαμβάνουν διορθώσεις για γνωστές ασφαλείας.
- ✓ **Ελέγχος της πρόσβασης:** Εφαρμόστε κανόνες για τον έλεγχο της πρόσβασης στα δεδομένα μας κατά τη μεταφορά. Μόνο εξουσιοδοτημένοι χρήστες πρέπει να έχουν πρόσβαση σε ευαίσθητα δεδομένα.
- ✓ **Διαχείριση του έλεγχου ταυτότητας:** Η πολιτική διαχείρισης του ελέγχου ταυτότητας (Identity and Access Management, IAM) πρέπει να εφαρμόζεται για να περιορίζεται η πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες.

Παρά τους κινδύνους, το cloud παρέχει επίσης πολλά εργαλεία για την ασφαλή μεταφορά δεδομένων. Ακολουθώντας τις παραπάνω βέλτιστες πρακτικές, μπορούμε να προστατεύσουμε τα δεδομένα μας κατά τη μεταφορά στο cloud.

Data-in-use: Η ασφάλεια δεδομένων σε χρήση είναι ένα κρίσιμο θέμα, ιδιαίτερα στον τομέα του cloud computing, όπου τα δεδομένα μπορεί να υποβάλλονται σε επεξεργασία από τρίτα μέρη. Οι κίνδυνοι που πρέπει να ληφθούν υπόψη περιλαμβάνουν:

- ✓ **Δικαιώματα πρόσβασης:** Ο ιδιοκτήτης των δεδομένων πρέπει να διατηρεί πλήρη έλεγχο όσον αφορά το ποιος έχει πρόσβαση στα δεδομένα του και σε ποιες επεξεργασίες υπόκεινται αυτά τα δεδομένα. Αυτό μπορεί να επιτευχθεί μέσω της διαχείρισης του ελέγχου ταυτότητας, όπως αναφέρατε, καθώς και μέσω της χρήσης πολιτικών πρόσβασης και ρυθμίσεων απορρήτου.
- ✓ **Επαλήθευση του Cloud Provider:** Επιλέγοντας έναν αξιόπιστο πάροχο cloud, μπορούμε να είμαστε βέβαιοι ότι οι διαδικασίες επεξεργασίας δεδομένων πληρούν τα υψηλά πρότυπα ασφαλείας. Εξετάζουμε την πολιτική ασφαλείας

και απορρήτου του παρόχου cloud προτού αποφασίσουμε να τον χρησιμοποιήσουμε.

- ✓ **Σύμβαση συμμόρφωσης:** Συμπεριλαμβάνουμε στη σύμβαση μας με τον πάροχο cloud όρους σχετικά με τη διατήρηση της ασφάλειας κατά τη διάρκεια της επεξεργασίας δεδομένων μας.

Σχετικά με το θέμα της διαγραφής δεδομένων, αποτελεί πραγματική πρόκληση. Είναι δύσκολο να διασφαλίσουμε ότι τα δεδομένα διαγράφονται οριστικά, καθώς στις φυσικές συσκευές αποθήκευσης μπορεί να υπάρχουν αντίγραφα και απομείναντα δεδομένα. Για να επιτευχθεί αυτό, μπορούμε να χρησιμοποιήσουμε κρυπτογράφηση για τα δεδομένα και να διαχειρίζονται προσεκτικά οι κλειδικοί πίνακες. Επίσης, κατά την διαγραφή δεδομένων, εκτελούνται διαδικασίες αφαίρεσης και καταστροφής των αρχείων με τρόπους που δυσκολεύουν την ανάκτησή τους. Αν είναι δυνατό, να επιλέγονται πάροχοι cloud που παρέχουν διαγραφή δεδομένων σε συμμόρφωση με τους κανονισμούς περί απορρήτου και ασφαλείας δεδομένων.

5.3 Διαχείριση ασφάλειας δεδομένων στο νέφος

Η ομομορφική κρυπτογράφηση είναι μια εντυπωσιακή τεχνική στον χώρο της κρυπτογραφίας και του cloud computing, καθώς επιτρέπει την εκτέλεση υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα χωρίς την ανάγκη αποκρυπτογράφησης αυτών. Αυτό αποτελεί έναν πολύ ισχυρό τρόπο προστασίας της απορρήτου και ασφάλειας των δεδομένων, ακόμα και κατά την επεξεργασία τους. Ομοιόμορφα κρυπτογραφημένα δεδομένα μπορούν να χρησιμοποιηθούν για αναλυτικές διαδικασίες, αναζητήσεις, υπολογισμούς, και άλλες λειτουργίες χωρίς να αποκρυπτογραφηθούν. Αυτό είναι ιδιαίτερα σημαντικό στον τομέα της ασφαλούς επεξεργασίας ευαίσθητων πληροφοριών στο cloud. Παρόλα αυτά, όπως αναφέρεται, η ομομορφική κρυπτογραφία είναι ακόμα σε ανάπτυξη, και οι υπολογιστικοί πόροι που απαιτούνται είναι υψηλοί, κάτι που την καθιστά δύσκολη στην εφαρμογή της σε μεγάλη κλίμακα.

Είναι σημαντικό να σημειωθεί ότι η αποτελεσματική ομομορφική κρυπτογραφία απαιτεί εξειδικευμένες γνώσεις και υπολογιστικούς πόρους, και η υψηλή πολυπλοκότητα των αλγορίθμων μπορεί να καθιστά δύσκολη την υλοποίησή της στην πράξη. Σχετικά με το Diffie-Hellman, αυτός είναι ένας αλγόριθμος συμφωνίας κλειδιού

που χρησιμοποιείται για την ασφαλή ανταλλαγή κλειδιών μεταξύ δύο μερών. Είναι σημαντικός για την ασφαλή επικοινωνία και δεν προορίζεται για την κρυπτογράφηση δεδομένων. Είναι σωστό να χρησιμοποιείται σε συνδυασμό με άλλους αλγορίθμους κρυπτογραφίας για τη διασφάλιση της ασφάλειας επικοινωνίας στο cloud computing. Η χρήση υβριδικών τεχνικών κρυπτογράφησης, όπως αναφέρεται, είναι συχνά αποτελεσματική για την επίτευξη ενισχυμένης ασφάλειας και ευελιξίας. Ο συνδυασμός διαφόρων αλγορίθμων κρυπτογράφησης, όπως το RSA, το 3DES και η γεννήτρια τυχαίων αριθμών, μπορεί να παρέχει ένα ισχυρό στρώμα ασφαλείας για τα δεδομένα μας. Κάθε αλγόριθμος έχει τις δικές του δυνατότητες και περιορισμούς, και ο συνδυασμός τους μπορεί να παρέχει ισχυρότερη προστασία.

Ωστόσο, είναι σημαντικό να ληφθεί υπόψη ότι ο συνδυασμός πολλών αλγορίθμων κρυπτογράφησης μπορεί να επηρεάσει την απόδοση του συστήματος και την πολυπλοκότητά του. Οι υπολογισμοί και οι υπολογιστικοί πόροι που απαιτούνται για την κρυπτογράφηση και τη αποκρυπτογράφηση δεδομένων ενδέχεται να αυξηθούν με τον συνδυασμό πολλαπλών αλγορίθμων. Όσον αφορά την κρυπτογραφία βάσης δεδομένων, αυτή είναι μια σημαντική τεχνική για την προστασία των δεδομένων που αποθηκεύονται σε περιβάλλοντα cloud. Η συγχρονισμένη ανταλλαγή κλειδιών μεταξύ του ιδιοκτήτη και του πελάτη για την αποκρυπτογράφηση των δεδομένων προσφέρει έναν τρόπο για την επιτήρηση και τον έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα. Ωστόσο, όπως αναφέρεαι, οι καθυστερήσεις ενδέχεται να αποτελέσουν ένα μειονέκτημα σε ορισμένες περιπτώσεις. Η εφαρμογή της ομαδικής κρυπτογράφησης και η βελτίωση της απόδοσης της επικοινωνίας μεταξύ των κόμβων είναι σημαντικές παράμετροι που πρέπει να ληφθούν υπόψη κατά την υλοποίηση αυτής της τεχνικής.

Συνολικά, η χρήση υβριδικών τεχνικών κρυπτογράφησης και η προσέγγιση βάσης δεδομένων στη μνήμη αποτελούν σημαντικά βήματα για την προστασία των δεδομένων στο περιβάλλον του cloud computing. Ωστόσο, απαιτείται προσεκτική σχεδίαση και εφαρμογή για να διασφαλίσουμε την ασφάλεια και την αποτελεσματικότητα του συστήματος. Οι τεχνικές κρυπτογράφησης και ασφαλείας που περιγράφουμε είναι σημαντικές για την προστασία των δεδομένων στο περιβάλλον του cloud computing. Είναι σημαντικό να ληφθούν μέτρα για τη διασφάλιση του απορρήτου και της ασφάλειας των δεδομένων που αποθηκεύονται και επεξεργάζονται σε αυτό το περιβάλλον. Οι τεχνικές που αναφέρονται, όπως η ανταλλακτική

κρυπτογράφηση και ο διακομιστής Shamir, προσφέρουν επιπλέον επίπεδα ασφάλειας για τα δεδομένα στο cloud. Η ανταλλακτική κρυπτογράφηση είναι ένας ενδιαφέρον τρόπος να ενισχύσουμε την ασφάλεια, καθώς μπορεί να προστατεύσει τα δεδομένα από διάφορες γωνίες. Ο διακομιστής Shamir μπορεί να χρησιμοποιηθεί για τη διάσπαση των δεδομένων σε πολλά κομμάτια, τα οποία είναι απαραίτητα για την αποκρυπτογράφηση. Αυτό προσφέρει μια επιπλέον στρώση ασφάλειας απέναντι σε διάφορες απειλές.

Επίσης, οι προσεγγίσεις που βασίζονται στη διανομή αποθήκευσης δεδομένων μπορούν να ενισχύσουν την ασφάλεια. Η διάσπαση των δεδομένων και η αποθήκευσή τους σε διάφορα μέρη του cloud μπορεί να δυσκολέψει την εξωτερική πρόσβαση. Επιπλέον, η προσαρμοσμένη μέτρηση των πόρων μπορεί να βοηθήσει στη βελτιστοποίηση της απόδοσης του συστήματος, λαμβάνοντας υπόψη τη μεταβαλλόμενη φύση του δικτύου και τις ανάγκες των χρηστών. Όπως και σε οποιοδήποτε περιβάλλον ασφάλειας, είναι σημαντικό να συνδυάσουμε διάφορες τεχνικές και προσεγγίσεις για να διασφαλίσουμε την ασφάλεια των δεδομένων μας στο cloud. Είναι επίσης σημαντικό να ενημερωνόμαστε συνεχώς για τις νέες απειλές και τις βέλτιστες πρακτικές στον τομέα της ασφάλειας πληροφοριών, καθώς αυτός εξελίσσεται συνεχώς.

Κεφάλαιο 6: Cloud computing στο μέλλον

6.1 Αμφιβολίες αξιοπιστίας χρήσης

Το cloud computing πράγματι αποτελεί μια σημαντική εξέλιξη στον τομέα της τεχνολογίας και έχει επηρεάσει θετικά τον τρόπο που όλοι οι τύποι οργανισμών διαχειρίζονται τις πληροφορίες και τις εφαρμογές τους. Όπως αναφέρεται, υπάρχουν σημαντικές ανησυχίες και προκλήσεις που συνοδεύουν τη μετάβαση στο cloud computing:

Ασφάλεια: Η ασφάλεια παραμένει μια από τις κύριες ανησυχίες. Οι οργανισμοί πρέπει να διασφαλίζουν ότι τα δεδομένα τους παραμένουν ασφαλή και προστατευμένα στο περιβάλλον του cloud. Η χρήση κρυπτογραφίας και προχωρημένων μέτρων ασφαλείας είναι απαραίτητη για την αντιμετώπιση αυτής της ανησυχίας.

Διαλειτουργικότητα και διαχείριση προμηθευτών: Η ευκολία μετάβασης από έναν πάροχο cloud σε έναν άλλον και η διαλειτουργικότητα των υπηρεσιών είναι σημαντικές ανησυχίες. Η έλλειψη προτύπων είναι ένα ζήτημα που πρέπει να αντιμετωπιστεί, ώστε να διασφαλιστεί ότι οι οργανισμοί μπορούν να αλλάξουν πάροχο χωρίς προβλήματα.

Διαθεσιμότητα και αξιοπιστία: Η αποτυχία υπηρεσίας από τον πάροχο cloud μπορεί να έχει σοβαρές συνέπειες. Οι οργανισμοί πρέπει να έχουν σχέδια ανάκαμψης και επικοινωνίας για να αντιμετωπίσουν αυτό το είδος των προβλημάτων.

Διασυνοριακή αποθήκευση δεδομένων: Η αποθήκευση δεδομένων σε πολυεθνικούς παρόχους cloud μπορεί να οδηγήσει σε νομικές διαφορές και ανησυχίες για την προστασία των δεδομένων από εκάστοτε νομοθεσίες. Οι χρήστες του cloud πρέπει να είναι ενήμεροι για τους νομικούς περιορισμούς που μπορεί να αντιμετωπίσουν.

Για να αντιμετωπιστούν αυτές τις ανησυχίες, είναι σημαντικό να υπάρχει μια σαφή στρατηγία cloud και να εργαζόμαστε σε συνεργασία με τους πάροχους cloud για να διασφαλίσουμε την ασφάλεια, τη διαλειτουργικότητα και τη διαθεσιμότητα των υπηρεσιών. Επιπλέον, πρέπει να εφαρμόζονται καλές πρακτικές για την ασφάλεια δεδομένων, όπως κρυπτογράφηση, επιθετική προστασία και παρακολούθηση των δικαιωμάτων πρόσβασης. Η συνεχής εκπαίδευση και ενημέρωση για τις ασφαλείς πρακτικές είναι απαραίτητη για τη διατήρηση της ασφάλειας στο περιβάλλον του cloud computing.

6.2 Η επόμενη μέρα

Είναι απόλυτα λογικό, ότι παρά τα οφέλη του cloud computing, υπάρχουν πολλά εμπόδια και προκλήσεις που πρέπει να αντιμετωπιστούν, και η ασφάλεια αποτελεί ένα από τα κύρια θέματα. Η ασφάλεια των δεδομένων και των εφαρμογών είναι ζωτικής σημασίας, και οι παροχείς cloud πρέπει να εργαστούν σκληρά για να διασφαλίσουν ότι παρέχουν αξιόπιστες υπηρεσίες ασφαλείας. Τα άλλα εμπόδια που αναφέραμε, όπως η γρήγορη εξέλιξη της τεχνολογίας και η έλλειψη τυποποίησης, επίσης αποτελούν προκλήσεις. Η ταχεία εξέλιξη της τεχνολογίας σημαίνει ότι οι επιχειρήσεις πρέπει να είναι διαρκώς ενημερωμένες και προετοιμασμένες να προσαρμοστούν σε νέες τεχνολογίες. Όσον αφορά την έλλειψη τυποποίησης, αυτό μπορεί να επιδρά στη δυσκολία μεταβατικών διαδικασιών μεταξύ παρόχων cloud. Η ανάπτυξη προτύπων και διεπαφών προγραμματισμού εφαρμογών (API) μπορεί να βοηθήσει στην επίλυση αυτού του προβλήματος.

Επιπλέον, οι κίνδυνοι που παρουσιάσατε, όπως αστοχίες διακυβέρνησης, θέματα διαλειτουργικότητας, διαρροή δεδομένων και νομικά ζητήματα, πρέπει να εξεταστούν προσεκτικά. Οι επιχειρήσεις πρέπει να αναπτύξουν συνολικές στρατηγικές ασφάλειας, να είναι επιφυλακτικές όταν πρόκειται να μεταφέρουν ευαίσθητα δεδομένα στο cloud, και να ακολουθούν τους νόμους και τους κανονισμούς περί ασφάλειας δεδομένων. Το cloud computing εξελίσσεται συνεχώς, και είναι σημαντικό να επιδιώκουμε λύσεις που θα ανταποκρίνονται στις αναγκαίες απαιτήσεις ασφάλειας και αξιοπιστίας. Η έρευνα και η ανάπτυξη νέων τεχνολογιών ασφάλειας και προτύπων μπορούν να βοηθήσουν στην αντιμετώπιση αυτών των προκλήσεων και στη βελτίωση της αποδοτικότητας και της ασφάλειας του cloud computing.

Σωστά επισημάναμε κρίσιμα ζητήματα που πρέπει να διερευνηθούν και να αντιμετωπιστούν για να βελτιωθεί η ασφάλεια και η αποτελεσματικότητα του cloud computing. Τα κυριότερα σημεία είναι:

Σχεδιασμός ολοκληρωμένης λύσης ασφαλείας: Η ανάπτυξη μιας ολοκληρωμένης λύσης ασφαλείας είναι αναγκαία για την προστασία του cloud computing. Αυτό προϋποθέτει την ανάπτυξη τυπικών προτύπων και προδιαγραφών για την ασφάλεια και τη συνεργασία μεταξύ παρόχων cloud και χρηστών.

Προστασία από απειλές: Η συνεχής προσαρμογή στις διάφορες γνωστές και άγνωστες απειλές είναι απαραίτητη. Αυτό περιλαμβάνει την ανάπτυξη συστημάτων ανίχνευσης και πρόληψης, καθώς και την αναβάθμιση των πολιτικών ασφαλείας.

Εξουσιοδότηση και διαχείριση πρόσβασης: Οι κανόνες εξουσιοδότησης και οι πολιτικές πρόσβασης είναι κρίσιμοι για τη διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα ευαίσθητα δεδομένα. Η διαχείριση των ταυτοτήτων και των δικαιωμάτων πρόσβασης πρέπει να είναι αυστηρή.

Πολλαπλή μίσθωση: Η αποτελεσματική χρήση της πολλαπλής μίσθωσης απαιτεί προσεκτική διαχείριση, ιδίως για να αποτραπούν οι DDoS επιθέσεις που μπορούν να επηρεάσουν όλους τους ενοικιαστές. Είναι σημαντικό να υιοθετηθούν αποτελεσματικά μέτρα πρόληψης και αποκατάστασης για να διασφαλιστεί η αποτελεσματική χρήση των υπολογιστικών πόρων.

Η έρευνα και η ανάπτυξη σε αυτούς τους τομείς είναι κρίσιμες για τη βελτίωση της ασφάλειας στο cloud computing. Επιπλέον, η συνεργασία μεταξύ των παρόχων cloud, των ερευνητών και των επιχειρήσεων είναι σημαντική για την αντιμετώπιση αυτών των προκλήσεων και την ανάπτυξη βέλτιστων πρακτικών ασφαλείας. Η ασφάλεια είναι πράγματι ένα από τα πιο κρίσιμα ζητήματα που πρέπει να αντιμετωπιστούν στο cloud computing. Οι προκλήσεις που συνδέονται με την ασφάλεια των δεδομένων στο cloud μπορούν να αντιμετωπιστούν με την εφαρμογή πολλών βασικών αρχών και τεχνικών:

Κρυπτογράφηση: Η κρυπτογράφηση είναι ένας σημαντικός παράγοντας για την προστασία των δεδομένων. Οι πάροχοι cloud μπορούν να χρησιμοποιήσουν την κρυπτογράφηση για να προστατεύσουν τα δεδομένα κατά τη μετάδοση και την αποθήκευσή τους. Επίσης, η εφαρμογή της κρυπτογράφησης με τη διατήρηση του κλειδιού κρυπτογράφησης από τον χρήστη βελτιώνει την ασφάλεια.

Διαχείριση Κλειδιών: Η διαχείριση κλειδιών είναι κρίσιμη για την πρόσβαση στα κρυπτογραφημένα δεδομένα. Οι παρόχοι cloud πρέπει να θεσπίσουν αξιόπιστα συστήματα διαχείρισης κλειδιών για τη διανομή και την ασφή αποθήκευση των κλειδιών που χρησιμοποιούνται στην κρυπτογράφηση.

Αυθεντικοποίηση και Εξουσιοδότηση: Οι χρήστες πρέπει να αυθεντικοποιούνται με ασφή τρόπο πριν έχουν πρόσβαση στα δεδομένα τους. Αυτό περιλαμβάνει τη χρήση πολυπαραγόντων μεθόδων ελέγχου ταυτότητας και εξουσιοδότησης.

Ελέγχος Πρόσβασης: Οι χρήστες πρέπει να έχουν ελεγχόμενη πρόσβαση στα δεδομένα τους. Οι παρόχοι cloud πρέπει να επιτρέπουν στους χρήστες να καθορίσουν ποιοι έχουν πρόσβαση στα δεδομένα τους και σε ποιες συνθήκες.

Επίβλεψη και Ανίχνευση: Οι παρόχοι cloud πρέπει να διαθέτουν μηχανισμούς επίβλεψης και ανίχνευσης για να παρακολουθούν την ασφάλεια και να ανιχνεύουν πιθανές απειλές.

Η ανάπτυξη συγκεκριμένων προτύπων και πρακτικών ασφαλείας για το cloud computing, καθώς και η συνεργασία μεταξύ των εμπλεκομένων φορέων, μπορούν να βελτιώσουν την ασφάλεια των υπηρεσιών cloud και να μειώσουν τον κίνδυνο για την απώλεια ή διαρροή των δεδομένων.

6.3 Συμπεράσματα

Το cloud computing προσφέρει πολλά πλεονεκτήματα όπως τη μείωση του κόστους, την ευελιξία, την ευκολία στη διαχείριση, και την δυνατότητα πρόσβασης από οπουδήποτε και με οποιαδήποτε συσκευή. Ωστόσο, υπάρχουν και προκλήσεις και κίνδυνοι που πρέπει να ληφθούν υπόψη. Ορισμένα από τα βασικά σημεία που αξίζει να εξεταστούν:

- ✓ **Ασφάλεια Δεδομένων:** Όπως αναφέρατε, η ασφάλεια των δεδομένων είναι κρίσιμη. Είναι σημαντικό να εξασφαλίζουμε ότι τα δεδομένα των μαθητών είναι ασφαλή και προστατεύονται από πιθανές παραβιάσεις ασφάλειας.
- ✓ **Διαφάνεια:** Είναι σημαντικό να κατανοείτε τι πραγματικά προσφέρει το cloud computing και πώς μπορεί να συμβάλει στο εκπαιδευτικό περιβάλλον. Επίσης, πρέπει να είστε προσεκτικοί με τις υποσχέσεις των προμηθευτών υπηρεσιών cloud.

- ✓ **Κόστος:** Ενώ το cloud computing μπορεί να μειώσει τα έξοδα στην αρχή, πρέπει να λαμβάνουμε υπόψη το συνολικό κόστος σε μεσοπρόθεσμο και μακροπρόθεσμο ορίζοντα.
- ✓ **Διαθεσιμότητα:** Πρέπει να εξασφαλίζουμε ότι τα συστήματα είναι διαθέσιμα και δεν υπάρχει κίνδυνος απώλειας πρόσβασης στα εκπαιδευτικά περιεχόμενα.
- ✓ **Εκπαίδευση και Ευαισθητοποίηση:** Η εκπαίδευση του προσωπικού και των μαθητών είναι ουσιώδης για την καλή χρήση του cloud computing και την ασφάλεια των δεδομένων.
- ✓ **Συμμόρφωση:** Πρέπει να τηρούνται όλοι οι κανονισμοί και οι νομικές υποχρεώσεις όσον αφορά τα εκπαιδευτικά δεδομένα.

Η ανάπτυξη μιας σαφούς στρατηγικής για το cloud computing, η συνεχής αξιολόγηση των αναγκών μας και η συνεργασία με αξιόπιστους παρόχους cloud υπηρεσιών μπορούν να μας βοηθήσουν να αξιοποιήσουμε τα οφέλη της τεχνολογίας αυτής ενώ παράλληλα διατηρείτε την ασφάλεια και την αποτελεσματικότητα του εκπαιδευτικού μας έργου.

Η ασφάλεια και το απόρρητο των δεδομένων αποτελούν κρίσιμους παράγοντες στον τομέα του cloud computing. Η εμπιστοσύνη μεταξύ παρόχων υπηρεσιών cloud και καταναλωτών είναι ουσιώδης για την ευρύτερη υιοθέτηση αυτής της τεχνολογίας. Σε αυτό το πλαίσιο, είναι σημαντικό να εξεταστούν διάφορες τεχνικές και προσεγγίσεις για την ασφάλεια των δεδομένων στο cloud. Ορισμένες τεχνικές που μπορούν να συμβάλουν στην προστασία των δεδομένων στο cloud περιλαμβάνουν:

- ✓ **Κρυπτογραφία:** Η κρυπτογράφηση των δεδομένων πριν από τη μεταφορά τους στο cloud και κατά την αποθήκευσή τους μπορεί να παρέχει προστασία από την ανεπιθύμητη πρόσβαση. Η επιλογή των κατάλληλων αλγορίθμων κρυπτογράφησης και η διαχείριση των κλειδιών είναι σημαντικά σημεία.
- ✓ **Ελέγχους πρόσβασης:** Οι παρόχοι cloud μπορούν να παρέχουν μηχανισμούς ελέγχου πρόσβασης, που επιτρέπουν να ορίζεται ποιος έχει πρόσβαση στα δεδομένα και με ποιες άδειες.
- ✓ **Ανίχνευση και αποτροπή απειλών:** Τα συστήματα ασφαλείας που εντοπίζουν και αποτρέπουν απειλές όπως ιοί, malware και ανεπιθύμητες εισβολές είναι ουσιώδη για την προστασία των δεδομένων.

- ✓ **Πολιτικές ασφαλείας:** Η θέσπιση αυστηρών πολιτικών ασφαλείας για τον χειρισμό, την αποθήκευση και την πρόσβαση στα δεδομένα είναι απαραίτητη.
- ✓ **Περιβάλλοντα εκτέλεσης ασφαλείας:** Η χρήση περιβαλλόντων εκτέλεσης με προηγμένες ασφαλιστικές δυνατότητες μπορεί να προστατεύσει τα ευαίσθητα δεδομένα.

Επίσης, είναι σημαντικό να συνεργάζεστε με αξιόπιστους παρόχους υπηρεσιών cloud που τηρούν υψηλά πρότυπα ασφαλείας και που συμμορφώνονται με τους κανονισμούς περί απορρήτου και ασφάλειας δεδομένων. Τα ζητήματα ασφαλείας στο cloud είναι αναμφίβολα σημαντικά, αλλά με τη σωστή στρατηγική και την κατάλληλη τεχνολογία, είναι εφικτό να επιτευχθεί υψηλό επίπεδο προστασίας για τα δεδομένα και τις εφαρμογές μας στο cloud.

Αναφορές

Abdalla, P. A., & Varol, A. (2019). Advantages to disadvantages of cloud computing for small-sized business. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.

Abdel-Basset, M., Mohamed, M., & Chang, V. (2018). NMCDA: A framework for evaluating cloud computing services. *Future Generation Computer Systems*, *86*, 12-29.

Albini, A., & Rajnai, Z. (2018). General architecture of cloud. *Procedia Manufacturing*, *22*, 485-490.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Al-Sayyed, R. M., Hijawi, W. A., Bashiti, A. M., AlJarah, I., Obeid, N., & Adwan, O. Y. (2019). An Investigation of Microsoft Azure and Amazon Web Services from Users' Perspectives. *International Journal of Emerging Technologies in Learning*, *14*(10).

AlZain, M. A., Soh, B., & Pardede, E. (2011). Mcdb: using multi-clouds to ensure security in cloud computing. In *2011 IEEE ninth international conference on dependable, autonomic and secure computing* (pp. 784-791). IEEE.

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, *12*, 529-534.

Baset, S. A. (2016). Cloud service level agreement. *Encyclopedia of Cloud Computing*, 433-445.

Buyya, R., Garg, S. K., & Calheiros, R. N. (2011). SLA-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions. In *2011 international conference on cloud and service computing* (pp. 1-10). IEEE.

El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, *29*(1), 223-246.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The characteristics of cloud computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275-279). IEEE.

Gupta, A., Mazumdar, B. D., Mishra, M., Shinde, P. P., Srivastava, S., & Deepak, A. (2023). Role of cloud computing in management and education. *Materials Today: Proceedings*, *80*, 3726-3729.

Humberg, T., & Jürjens, J. (2016). Compliance in Clouds. *Encyclopedia of Cloud Computing*, 267-273.

Hyseni, L. N., & Ibrahimi, A. (2017). Comparison of the cloud computing platforms provided by Amazon and Google. In *2017 Computing Conference* (pp. 236-243). IEEE.

Joshi, M., Budhani, S., Tewari, N., & Prakash, S. (2021). Analytical review of data security in cloud computing. In *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)* (pp. 362-366). IEEE.

Kacha, L., & Zitouni, A. (2018). An overview on data security in cloud computing. *Cybernetics Approaches in Intelligent Systems: Computational Methods in Systems and Software 2017, vol. 1*, 250-261.

Kamal, M. A., Raza, H. W., Alam, M. M., & Mohd, M. (2020). Highlight the features of AWS, GCP and Microsoft Azure that have an impact when choosing a cloud service provider. *Int. J. Recent Technol. Eng*, *8*(5), 4124-4232.

Kim, W. (2009). Cloud computing: Today and tomorrow. *J. Object Technol.*, *8*(1), 65-72.

Patel, P., Ranabahu, A. H., & Sheth, A. P. (2009). Service level agreement in cloud computing.

Qian, L., Luo, Z., Du, Y., & Guo, L. (2009). Cloud computing: An overview. In *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1* (pp. 626-631). Springer Berlin Heidelberg.

Rajaraman, V. (2014). Cloud computing. *Resonance*, *19*, 242-258.

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209.

Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421-426.

Sadiku, M. N., Musa, S. M., & Momoh, O. D. (2014). Cloud computing: opportunities and challenges. *IEEE potentials*, *33*(1), 34-36.

Samarati, P., & De Capitani di Vimercati, S. (2016). Cloud security: Issues and concerns. *Encyclopedia of cloud computing*, 205-219.

Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. *IEEE Access*, *7*, 147420-147452.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.

Tsochev, G. R., & Trifonov, R. I. (2022). Cloud computing security requirements: A Review. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1216, No. 1, p. 012001). IOP Publishing.