International Journal of Cloud Computing and Database Management

E-ISSN: 2707-5915
P-ISSN: 2707-5907
IJCCDM 2024; 5(2): 97-108
www.computersciencejournals.com/ijccdm
Received: 23-07-2024
Accepted: 30-08-2024

Ifeanyi Amuche Ilochonwu
Department of Campbellsville University School of Business, Economics and Technology Campbellsville University Louisville City, Kentucky, U.S.A

Corresponding Author:
Ifeanyi Amuche Ilochonwu
Department of Campbellsville University School of Business, Economics and Technology Campbellsville University Louisville City, Kentucky, U.S.A

Cloud security paradigms: A systematic review of threat mitigation strategies in cloud-based applications

Ifeanyi Amuche Ilochonwu

DOI: https://doi.org/10.33545/27075907.2024.v5.i2b.75

Abstract
Cloud computing has become a cornerstone of modern digital technology, enabling organizations to scale operations, enhance accessibility, and reduce costs. However, as cloud-based applications proliferate, they are increasingly exposed to sophisticated security threats that jeopardize data integrity, privacy, and service availability. This paper presents a systematic review of cloud security paradigms with a focus on threat mitigation strategies. The study analyzes literatures on security threats in cloud environments, such as data breaches, distributed denial-of-service (DDoS) attacks, account hijacking, malware attacks, and data breaches, insider attacks, and service disruptions. The review explores a range of mitigation techniques, such as encryption, multi-factor authentication, data encryption technique, cloud network security, cloud penetrating testing, physical security of the infrastructure, servers' intrusion detection systems, and secure cloud architectures. The paper assesses the efficacy of these strategies in addressing vulnerabilities specific to cloud platforms. The study findings showcase the need for a multi-layered security approach that involves both technical and organizational measures to safeguard cloud-based applications. This review provides a comprehensive understanding of the current state of cloud security and highlights emerging trends in threat mitigation, offering valuable insights for researchers, cloud service providers, and organizations deploying cloud technologies.

Keywords: Cloud security, cyber-attacks, mitigation strategies, cloud computing, applications

Introduction

Modern information technology heavily relies on cloud computing, which offers businesses a host of advantages including cost-effectiveness, scalability, and flexibility (Mikkonen & Khan, 2016) [41]. To effectively employ cloud services, however, businesses now need to guarantee the security of their data, apps, and cloud-based networks. Cloud computing is becoming a fundamental component of internet services offered to consumers in high-demand industries including manufacturing, entertainment, healthcare, and retail (Nazari *et al*., 2020) [47]. Enterprises are pursuing "cloud-first" approaches to application development and operations due to the flexibility of on-demand elasticity as well as other advantages including variety of resources, dependability, and cost-effectiveness (Zatonatska & Dluhopolskyi, 2019) [73]. Technological developments, software-centric advances in cloud resource orchestration are usually necessary to achieve these identified benefits.

A paradigm shift in technology and services for providing computer resources and services online is known as cloud computing. The primary idea behind cloud computing is to provide on-demand access to a range of IT resources, including storage, servers, networking, databases, and software, so doing away with the requirement for physical, on-premises infrastructure (Alhenaki *et al*., 2019) [4]. Among these innovations are cloud platforms built on Software Defined Everything Infrastructures (SDxI), which provide programmability to achieve capabilities such as the speed and agility of elastic capacity provisioning (Schulz, 2017) [59]. Additionally, these platforms create opportunities to set up Software-Defined Internet Exchange Points (SDXs) across different Software-Defined Network (SDN) domains, or Autonomous Systems (ASes), enabling cross-domain collaboration, application-specific peering, and the exchange of knowledge related to cyber threats (Gupta, *et al*., 2014) [27]. When effective, cyberattacks can lead to significant, lasting damage to a business's income and reputation (Perera *et al*., 2022) [49]. Interruptions caused by these attacks can negatively affect customers' quality of experience (QoE), causing them to lose trust in the service provider. In the worst cases, this can even lead to customers discontinuing the use of services from the cloud-based application provider entirely (Perera *et al*., 2022) [49].

According to Akhtar *et al*. (2022) [2], cloud computing safeguards sensitive and private data, such as data on finances, customer information from significant businesses and multinational organizations, and information pertaining to intellectual property. Thus, it is essential to guarantee sensitive data's accessibility and confidentiality, which includes limiting unauthorized parties' access to the data (Hassan *et al*., 2022) [28]. Data is protected by cloud services from potential institutional catastrophes like floods, fires, and conflicts, among other natural disasters (Vellela *et al*., 2022) [70]. Sharing operational and accessible resources further lowers costs when employing cloud computing (Vellela *et al*., 2022) [70]. Cloud security is a difficult task. It is essential to safeguard the cloud from all known dangers since an increasing number of businesses are putting their data on the cloud (Golightly *et al*., 2022) [26]. Cloud storage will hold 100 zettabytes of data by the end of 2025. According to Basu (2022) [14] that quantity is one hundred billion terabytes. However, 45% of data breaches originate via the cloud. A recent poll found that 27% of businesses had encountered a public cloud security incident, an increase of 10% from 2022, and that 80% of firms had at least one cloud security issue in 2022 (Jones, 2023) [31]. Data breaches and other security-related problems can harm an organization's brand and erode consumer trust. The cloud must adjust to innovations and create appropriate defenses against advanced vulnerabilities like ransomware, zero-day vulnerabilities, and advanced persistent threats (APTs) in light of the growth of security attacks and the introduction of new threats that jeopardize data security (Saratchandra & Shrestha, 2022) [56]. It seems that concerns about security are growing in frequency, which may put data and cloud resources at risk. The malicious activity like phishing, the danger connected with it has increased by 33% between 2020 and 2022 (Saratchandra & Shrestha, 2022) [56].

Common threats include account hijacking, data breaches distributed denial-of-service (DDoS) attacks and malware infections (Ahmadi, 2024; Khalifa & Elmedany, 2023) [1, 32]. Organizations can use a variety of tactics, including intrusion detection systems, vulnerability management, security awareness training, and encryption, to reduce these risks (Ahmadi, 2024; Khalifa & Elmedany, 2023) [1, 32]. To improve cloud security, specialized methods have been suggested, such as the iADTree mechanism for threat and risk assessment (Kar & Mishra, 2016). Mitigation solutions based on signal processing techniques, including discrete cosine transform, have been proposed for cloud-internal denial-of-service attacks (Alarifi & Wolthusen, 2014). Serverless computing, containerization, and the use of AI and machine learning are emerging trends in cloud security (Ahmadi, 2024) [1]. In order to handle changing threats and preserve a security-conscious culture in companies using cloud services, ongoing research and innovation are essential (Ahmadi, 2024; Khalifa & Elmedany, 2023) [1, 32].

The purpose of this study is examine emerging Threat in cloud computing and identify threat mitigation strategies in cloud-based applications

Literature Review: Numerous forms of service deployment are offered by cloud computing. According to Rani, *et al*. (2015) [52] there is four distinct models used to classify the cloud services. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Container as a Service (CaaS) are the four cloud service paradigms. Software as a Service (SaaS) is a cloud computing concept that uses the internet to distribute software applications. Under the SaaS model, customers don't need to install or maintain the software on their own devices; instead, they may access and utilize it through a web browser. Most SaaS apps are subscription-based, requiring users to pay a regular charge in order to use the service. The SaaS solution replaces the requirement for internal applications, data storage, and administrative support for the applications. Businesses pay for each user's use of the SaaS resources (Surya, 2019) [66].

A cloud computing concept called Platform as a Service (PaaS) gives developers a platform to create, launch, and maintain applications without having to worry about the supporting infrastructure. PaaS provides a comprehensive cloud-based development and deployment environment, replete with resources that enable developers to give their consumers everything from basic cloud-based applications to complex corporate applications (Yasrab, 2018) [72]. The primary illustrations of the PaaS concept include Google App Engine, Google's Azure services platform, and Amazon's relational database services (RDS). A cloud computing architecture known as Infrastructure as a Service (IaaS) offers virtualized computer resources online. Businesses may rent servers, storage, networking, and virtualization as well as other IT infrastructure on a pay-as-you-go basis from cloud providers under the Infrastructure as a Service (IaaS) model. By doing this, businesses may avoid the expenses and hassles associated with owning and maintaining physical servers and data center equipment (Suliman & Madinah, 2021). It is not necessary for clients to buy servers, data centers, network hardware, or space (such as Amazon EC2).

A cloud computing paradigm called Container as a Service (CaaS) offers a framework for organizing, launching, and operating containerized applications. CaaS, which is based on container virtualization, has become a popular cloud paradigm to address problems with application development in PaaS environments (Tao *et al*., 2018) [67]. Code, libraries, dependencies, runtime, and other components required to operate an application are all included in containers, which are small, lightweight, isolated environments. By abstracting the underlying infrastructure, Container as a Service (CaaS) enables developers to automate scaling, orchestrate clusters, and deploy and manage containers. CaaS models include Google Container Engine and Amazon EC2 Container Service (ECS) (Bentaleb *et al*., 2022) [16-17]. General cloud security paradigms including SaaS, PaaS, IaaS, and CaaS have been highlighted in studies (Hussein *et al*., 2019) [29]. According to empirical research, these models are essential for cloud security from the standpoints of customers and cloud security providers (Raja & Hanifa, 2017; Elsayed, 2018; Awaysheh *et al*., 2021) [51, 23, 11]. To safeguard consumers' online activities, a growing set of cloud security models is even more crucial. Users are more likely to feel comfortable using client computing services if a security model is more secure.

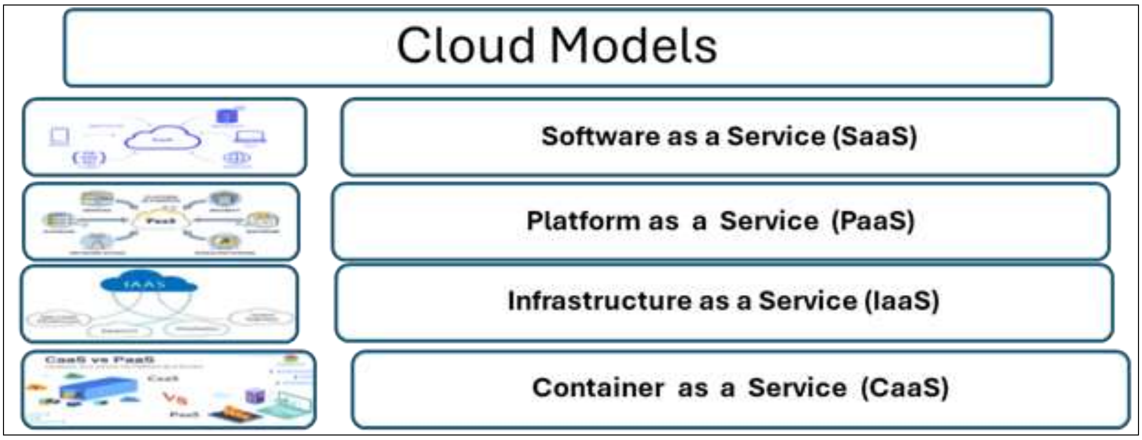

Fig 1: Cloud Models

Emerging Threat in cloud computing

Numerous typical threats can affect cloud computing. This is because it is solely a technological platform, meaning that potential cyberattacks might occur at any time. According to Mozumder *et al*. (2017) [43], data breaches are common. They lead to either data theft or illegal access to data. Data breaches disclose a firm's private information, which leads in severe brand and financial effects (Martin *et al*., 2017) [39]. The complex and constantly changing nature of cyberattacks is a significant obstacle to cloud system security and cloud applications (Mallick & Nath, 2024) [38]. The attackers focus on developing novel methods and strategies to obtain data within an organization, which might be harmful to the company. Therefore, in order to handle the growing threats in the industry, a comprehensive security system is essential. When a new threat emerges, a standard security solution can have trouble protecting an organization's data, making the cloud environment open to sophisticated attacks. Therefore, having a flexible security plan that can deal with cyberthreats is crucial. The study of Walling and Lodh (2022) [71], claims that organizations are compelled by data breaches to put stringent security measures in place to safeguard data. In this sense, malware assaults are also very common. Software that breaches the cloud server and takes all the needed data is one of these assaults.

The study of Nayak *et al*. (2022) [46] charts the development of cyber dangers from their beginnings in artificial intelligence to their current level of sophistication, highlighting their growing intricacy and capacity to interfere with vital activities and compromise private information. Threats such as malware, phishing schemes, man-in-the-middle assaults, denial-of-service (DoS) attacks, and SQL injections are categorized and examined. The goal is to clarify how they may steal, disrupt, trick, and penetrate systems. Organizations and users are at serious danger from the threats that have been described. Razi and Batan (2023) [53], conducted a study on security risks associated with cloud computing. The study emphasizes the concerns people have about privacy and data security when using cloud services. It recognizes the objections about keeping data on servers located abroad, emphasizing worries about possible data breaches, cyberattacks, illegal access, and the possibility of data loss or corruption.

Data breaches

A data breach in cloud computing refers to unauthorized access or exposure of sensitive data stored on cloud platforms (Barona & Anita, 2017; Mozumder *et al*., 2017) [13, 43]. These breaches can lead to significant financial, legal, and reputational damage for businesses and individuals alike (La Torre *et al*., 2018) [35].

Account hijacking

Account hijacking is a significant security threat in cloud computing where attackers gain unauthorized access to cloud accounts, leading to a wide range of malicious activities (Christina, 2015) [19]. This type of cyberattack allows hackers to manipulate data, steal sensitive information, disrupt services, or launch attacks against other cloud users (Arunkumar, 2023) [10].

Insider Threat

An insider threat in cloud computing refers to risks posed by individuals within an organization, such as employees, contractors, or business partners, who have access to sensitive cloud systems and data (Claycomb & Nicoll, 2012) [20]. Unlike external attacks, insider threats come from trusted individuals with legitimate access but who intentionally or unintentionally misuse their privileges, leading to data breaches, financial loss, or operational disruptions (Saxena *et al*., 2020) [57].

Data loss

Data loss in cloud computing refers to the accidental or deliberate destruction, corruption, or deletion of data stored in the cloud. This can result in the permanent unavailability of critical business information, leading to financial, legal, and operational consequences for organizations. Cyberattacks such as ransomware, malware, and hacking can lead to the destruction or unauthorized modification of cloud-stored data. Attackers may encrypt or delete critical data, causing significant disruption to cloud operations.

Identity Theft

Identity theft in cloud computing occurs when malicious actors gain unauthorized access to a user's credentials or personal information stored in the cloud. This type of cybercrime can lead to significant financial, reputational, and operational damage, as attackers may use stolen identities to commit fraud, steal sensitive data, or engage in other illegal activities.

Misconfiguration

Misconfiguration in cloud computing refers to errors or gaps in setting up cloud services, resources, or applications, which can lead to vulnerabilities and security risks. These mistakes often arise from improper management of cloud settings, permissions, or access controls, leaving cloud environments exposed to cyberattacks, data breaches, and other incidents.

DDoS Attacks (Distributed Denial of Service)

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. In a DDoS attack, multiple compromised systems (often part of a botnet) are used to send vast amounts of traffic to the target, overwhelming its resources and making it unavailable to legitimate users. DDoS attacks exploit the capacity limits of a server or network. Websites, applications, and other services are designed to handle a certain amount of traffic, but when the traffic surpasses their capacity, they become slow or completely inaccessible.

Man-in-the-Middle Attacks

A Man-in-the-Middle (MitM) attack is a cyberattack where an attacker intercepts and potentially alters communication between two parties without their knowledge. In this type of attack, the attacker positions themselves between the sender and receiver, often posing as a legitimate participant to gain access to sensitive data, such as login credentials, personal information, or financial details.

Malware injection: Malware injection is the process where an attacker inserts malicious code into a cloud service, application, or system with the intent to compromise the security and integrity of data and services (Medaram & Maglaras, 2023). In cloud environments, malware injection attacks pose significant risks, as they can exploit vulnerabilities in shared infrastructure or applications, potentially affecting multiple users.

SQL Injection (SQLi)

SQL Injection (SQLi) is a common and severe web security vulnerability that allows attackers to interfere with the queries that an application makes to its database (Jemal *et al*., 2020) [23]. In an SQL injection attack, the attacker manipulates the SQL queries sent to the database by injecting malicious code into input fields or URLs, tricking the database into executing unintended commands. This can lead to unauthorized access, data leakage, or even the complete compromise of the system (Shahriar & Zulkernine, 2012) [64].

Phishing attacks

Phishing attacks in cloud computing involve deceptive practices designed to trick users into divulging sensitive information or credentials that can compromise cloud-based services and resources (Nadeem *et al*., 2021) [45]. These attacks exploit the growing reliance on cloud services and often target both individuals and organizations to gain unauthorized access to cloud accounts, data, or infrastructure.

Materials and Methods

This systematic review aims to enhance the analysis of empirical findings whilst expanding on the authors' previous research findings. This study analyzed and synthesized previous research on cloud computing security, including research papers and academic articles, using a qualitative research approach. The aim was to ascertain many noteworthy threats and assess ways for mitigation. In order to fulfill the study's aims, the researcher performed an organized literature search on prominent digital libraries, including IEEE Xplore, Springer, Elicit, Google Scholars, and Science Direct. The main sources of articles on computer science-related subject are in these prominent digital libraries. The search terms and phrases, such "Cloud security threats", "cloud security models", "cloud security mitigation strategies", "cloud security models" are developed from specific study objectives. Selected papers were the most pertinent research articles that contained all or most of the keywords, such as security, mitigation measures, and threats to cloud computing. Even though attempts were made to methodically find and choose pertinent research articles, it's possible that some studies were unintentionally left out of the search criteria and selection procedure. The search turned in 400 scholarly publications. Through a rigorous selection process grounded on study objectives, this research endeavors to concentrate on the threats and mitigation measures that have garnered attention over the 2017–2024 timeframe. The time frame was constrained by the constantly shifting trends in the cloud computing industry. Due diligence was necessary to ensure that the research only took into account the most current developments in cloud computing security. To get the desired findings, reviews, studies done in other countries, and duplicates were discarded. Quality evaluation criteria were also implemented, and only the studies that met the inclusion criterion were selected. The procedures that resulted in the identification of 20 appropriate papers are displayed in the PRISMA flowchart that follows as fig 4.

Many papers, though related to cloud computing, did not specifically address threat mitigation strategies in cloud-based applications. Some focused on general cybersecurity or cloud architecture, which did not contribute to the review's central research question. To maintain focus, these papers were excluded. Additionally, as the search was conducted across multiple databases like IEEE Xplore and Google Scholar, duplicate studies were identified and removed to avoid skewing the synthesis of findings. Ensuring a unique set of studies is essential for a systematic review. Some papers were excluded due to poor methodological quality which could introduce bias. Only high-quality studies were included to strengthen the reliability of the review. In some cases, papers were excluded because full-text versions were unavailable, preventing a proper evaluation of their relevance. The fast-evolving nature of cloud computing and cybersecurity led to the exclusion of outdated studies that did not reflect current threats or mitigation strategies. Including only recent and relevant studies ensured that the review provided accurate and up-to-date conclusions about cloud-based threat mitigation. This current review adopted a qualitative analysis of content summation for the research investigation. Employing content summation was done in order to draw conclusions and important patterns from the chosen research papers. In order to detect new trends in cloud computing security as well as threats and mitigation measures, the material was first arranged into pertinent sections based on the subjects found in the qualitative analysis. The results of all the research investigations were then compiled and combined in order to obtain pertinent and current data that may offer insights into cloud security.

Figure 3: A PRISSMA flowchart demonstrating the procedure for identification, screening, exclusion and inclusion of the articles in this review.

The cloud is considered one of the most important technologies in storing, protecting, and processing data, but the cloud is still vulnerable to many security risks that may threaten the stored data. Previous studies have identified various threat to cloud security such as data breaches, insider threat, Distributed Denial of Service (DDoS) Attacks, Insecure interfaces and APIs, Data Breache, Abuse and Nefarious Use of Cloud Computing, Data loss, Account traffic hijacking, Poorly Access Control, Compliance Violations, Man-in-the-Middle (MitM), Denial of Service (DoS), Malware, Compliance Violations, SQL injection, Third-Party Service Risks (Mohamad *et al*.,2022; Razi & Batan, 2023; Mozumder *et al*., 2017; Nayak *et al*., 2022) [42, 53, 43, 46].

The study's findings revealed several key mitigating strategies that are essential for addressing cyber-attacks in cloud computing. These strategies encompass both technical and organizational measures, focusing on enhancing security protocols, adopting advanced technologies, and fostering a culture of cybersecurity awareness among users and administrators.

A major finding from the study is that identity and access management (IAM) plays a crucial role in mitigating cyberattacks in cloud computing by ensuring that only authorized users have access to cloud resources (AL-Qtiemat & AL-Odat, 2024; Sai Shreya & Kavitha, 2024; Liubchenko & Volkov 2024; Reece *et al*., 2024; Amara *et al*., 2017; Kunduru, 2023; Pranjal, 2024) [5, 55, 37, 54, 7, 34, 50].

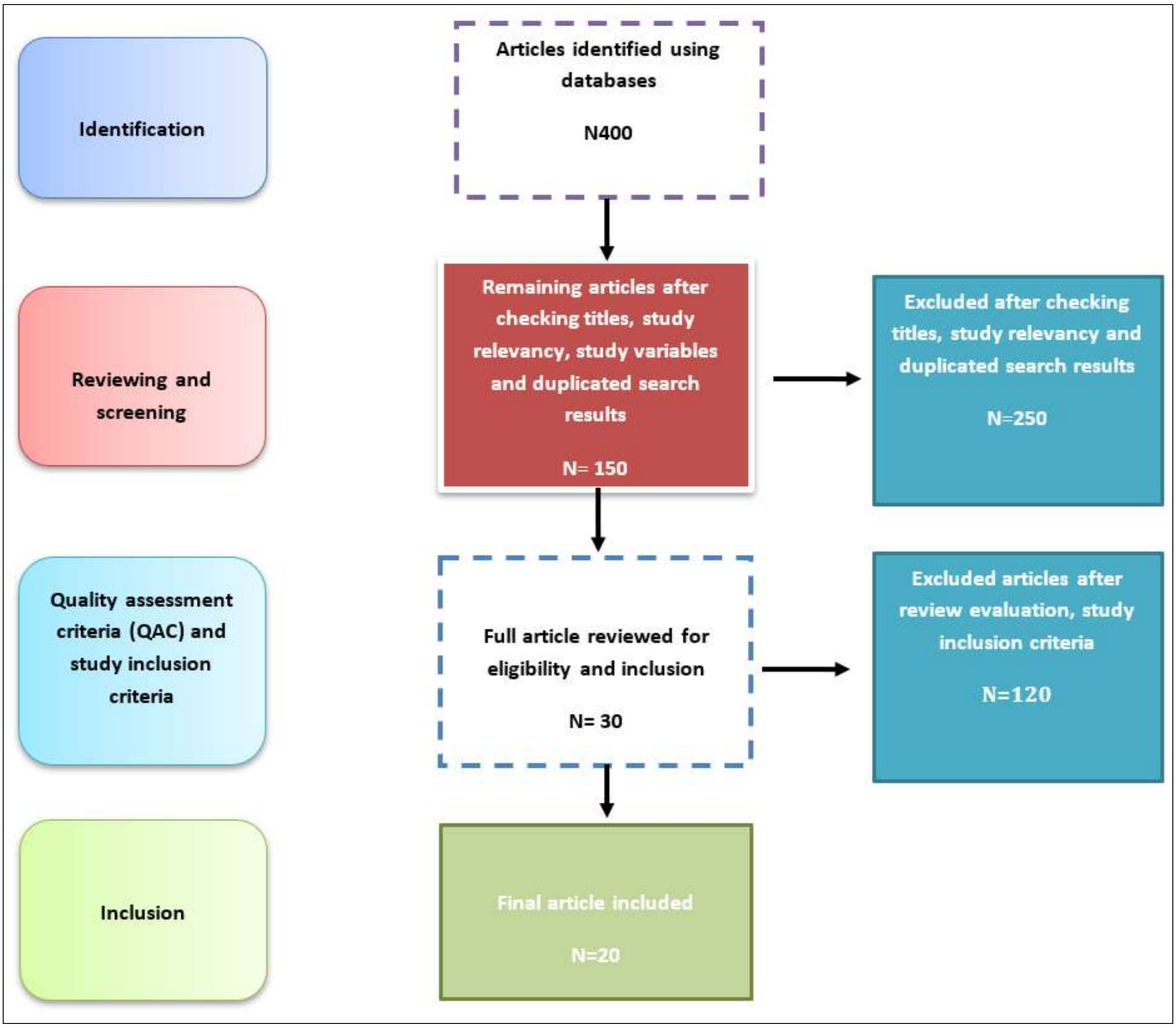

Table 1: Quality Assessment Criteria (QAC)

S/N	Quality Assessment Criteria	Rating Scale
1.	Is the study focusing on the research field of study	Yes=1, NO=0, Fairly=1
2.	Is the study succinctly focusing on cloud computing	Yes=1, NO=0, Fairly=1
3.	Is the study explicitly focusing on emerging cloud security issues	Yes=1, NO=0, Fairly=1
4.	Is the study focusing on threat mitigating strategies in cloud applications	Yes=1, NO=0, Fairly=1

Table 2: Selected papers for the review

S/ N	Author	Year	Publication
1	AL-Qtiemat and AL-Odat	2024	Examining cloud security: identifying risks and the implemented mitigation strategies
2	Sai Shreya and Kavitha	2024	Securing SaaS: Key Challenges and Effective Mitigation Strategies
3	Nwaocha and Oloyede	2023	Averting DDOS Attacks in Web-Based Applications
4	Liubchenko and Volkov	2024	Cyber-aware threats and management strategies in cloud environments.
5	Amara, N., Zhiqui, H., & Ali, A.	2017	Cloud computing security threats and attacks with their mitigation techniques.
6	Mukherjee	2019	Cloud-based Security Solutions
7	George and Sagayarajan,	2023	Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS, and SaaS environments.
8	Alenezi	2021	Safeguarding Cloud Computing Infrastructure: A Security Analysis.
9	Kunduru	2023	Security concerns and solutions for enterprise cloud computing applications.
10	Pranjal	2024	Data Security on Cloud Services: Threats and Mitigation
11	Bautista-Villalpando and Abran	2021	A Data Security Framework for Cloud Computing Services.
12	Shabbir *et al*.	2024	Analyzing enterprise data protection and safety risks in cloud computing using ensemble learning.
13	Amjad *et al*.	2019	Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm.
14	Bouchama and Kamal	2021	Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns.
15	Khodayer *et al*.	2024	Cloud Computing and Its Security in Real applications.
16	Shilpa	2024	Navigating Privacy and Security in Cloud Computing. Recent Trends in Parallel Computing.
17	Sharma	2024	The evolution of cybersecurity challenges and mitigation strategies in cloud computing systems.
18	Arogundade	2024	Strategic Security Risk Management in Cloud Computing
19	Upadhyay	2024	Mitigating Risks in the Cloud-Based Metaverse Access Control Strategies and Techniques.
20	Saxena and Gayathri	2021	A study on vulnerable risks in security of cloud computing and proposal of its remedies.

Results and Discussion of Findings

Table 3: Study review on mitigating strategies in cloud based applications

S/N	Mitigating Strategies	Supporting Authors
1	Identity and Access Management (IAM).	Bautista-Villalpando and Abran (2021) [15], AL-Qtiemat & AL-Odat, (2024) [5], Sai Shreya and Kavitha (2024) [55], Liubchenko & Volkov (2024) [37], Reece *et al*. (2024) [54], Amara *et al*. (2017) [6-7], Kunduru (2023) [34]. Pranjal (2024) [50], Bouchama and Kamal (2021) [18], Shilpa (2024) [64], Sharma (2024) [63] Upadhyay (2024) [69]
2	Data Encryption	Amara *et al*. (2017) [6-7], Bautista-Villalpando and Abran (2021) [15], Shabbir *et al*. (2024) [61], Bouchama and Kamal (2021) [18] Khodayer *et al*. (2024) [33], Shilpa (2024) [64], Arogundade (2024) [9] Saxena and Gayathri (2021) [58] Mukherjee (2019) [44], George and Sagayarajan, (2023) [25], AL-Qtiemat & AL-Odat, (2024) [5], Sai Shreya, R., & Kavitha, R. (2024) [55]. Reece *et al*. (2024) [54],Kunduru (2023) [34] and Pranjal (2024) [50]
3	Cloud network security	AL-Qtiemat & AL-Odat, (2024) [5], Alenezi (2021) [3], Kunduru (2023) [34], Bautista-Villalpando and Abran (2021) [15], Shabbir *et al*. (2024) [61], Shilpa (2024) [64] Sharma (2024) [63] Pranjal (2024) [50], Amara *et al*. (2017) [6-7], George and Sagayarajan, S. (2023) [25].
4	Regular Auditing and Monitoring	Alenezi (2021) [3], Kunduru (2023) [34], AL-Qtiemat & AL-Odat, (2024) [5], Shabbir *et al*. (2024) [61], Bouchama and Kamal (2021) [18] Saxena and Gayathri (2021) [58] Arogundade (2024) [9] Amara *et al*. (2017) [6-7], Mukherjee (2019) [44], George, A. S., & Sagayarajan, S. (2023) [25].
5	Physical security of the infrastructure and servers	AL-Qtiemat & AL-Odat, (2024) [5], Bautista-Villalpando and Abran (2021) [15] Alenezi (2021) [3]
6	Multifactor Authentication	Sai Shreya, R., & Kavitha, R. (2024) [55]. Bautista-Villalpando and Abran (2021) [15] George, A. S., & Sagayarajan, S. (2023) [25]. Alenezi (2021) [3], Reece *et al*. (2024) [54]. Amara *et al*. (2017) [6-7], Shabbir *et al*. (2024) [61] Khodayer *et al*. (2024) [33] Shilpa (2024) [64] Sharma (2024) [63] Saxena and Gayathri (2021) [58]
7	Use Of A Web Application Firewall (WAF)	Nwaocha & Oloyede (2023) [48], Amjad *et al*. (2019) [8] Sharma (2024) [63] Alenezi (2021) [3]. Alenezi (2021) [3] and Pranjal (2024) [50]
8	Content Delivery Network (CDN)	Nwaocha, V.O. & Oloyede, A. (2023) [48].
9	Security Information and Event Management (SIEM	Sharma (2024) [63], Upadhyay (2024) [69] Reece *et al*. (2024) [54]. Amara *et al*. (2017) [6-7], Shilpa (2024) [64]
10	Implementing strong Application Programming Interfaces (API)	Saxena and Gayathri (2021) [58] Reece *et al*. (2024) [54]. Amara *et al*. (2017) [6-7], Mukherjee (2019) [44]
11	Cloud penetrating Testing	George and Sagayarajan, (2023) [25]. Kunduru (2023) [34]

It provides a framework for managing digital identities and controlling access to sensitive data and systems. Through IAM, organizations can enforce security policies such as multi-factor authentication (MFA), role-based access control (RBAC), and least privilege principles. These measures minimize unauthorized access, reduce the risk of insider threats, and protect against data breaches (Bouchama & Kamal 2021; Shilpa 2024; Sharma, 2024) [18, 64, 63]. IAM also allows for continuous monitoring and auditing, helping to detect suspicious activities and respond to potential security incidents in real time (AL-Qtiemat & AL-Odat, 2024; Sai Shreya & Kavitha, 2024; Liubchenko & Volkov 2024; Upadhyay 2024; Bautista-Villalpando & Abran, 2021) [5, 55, 37, 69, 15]. A survey by CyberArk in 2021 revealed that 70% of organizations faced security breaches due to mismanagement of privileged access. Implementing IAM effectively can reduce unauthorized access risks by over 50%, particularly when the principle of least privilege (PoLP) is enforced across user roles (Orca security, 2022) [48]. The study analysis highlights that data encryption is major mitigating strategy against cyber-attack. Studies by Amara *et al*. (2017) [7], Bautista-Villalpando and Abran (2021) [15], Shabbir *et al*. (2024) [61], Bouchama and Kamal (2021) [18] Khodayer *et al*. (2024) [33], Shilpa (2024) [64], Mukherjee (2019) [44], George and Sagayarajan, (2023) [25], AL-Qtiemat and AL-Odat, (2024) [5], Sai Shreya, and Kavitha, (2024) [55], Reece *et al*. (2024) [54], Kunduru (2023) [34] and Pranjal (2024) [50] shows that data encryption is a critical strategy in mitigating cyberattacks in cloud computing by converting sensitive information into a secure format, making it unreadable to unauthorized users. Encryption ensures that data, both at rest (stored) and in transit (during transmission), is protected from interception, tampering, or theft. By using strong encryption algorithms, organizations can safeguard their data, even if attackers gain access to cloud systems (Arogundade 2024; Saxena & Gayathri 2021; Reece *et al*., 2024; Kunduru, 2023; Pranjal, 2024) [9, 58, 34, 50, 58, 54, 34, 50]. Encryption also helps maintain compliance with regulatory standards and provides an additional layer of security, ensuring that sensitive information remains confidential and secure from cyber threats like hacking, data breaches, and insider threats (Sai Shreya & Kavitha, 2024; Reece *et al*., 2024; Kunduru, 2023; Pranjal, 2024) [5, 54, 34, 50]. Encryption remains a key defense mechanism. A 2023 report by Thales highlights that encryption of data at rest and in transit reduces data breaches by up to 60% (Thales 2023) [68]. Cloud providers such as AWS and Azure offer advanced encryption tools like AWS Key Management Service and Azure Key Vault, further boosting security.

Regular auditing and monitoring are essential strategies for mitigating cyberattacks in cloud computing according to the study review. (Alenezi 2021; Kunduru 2023; AL-Qtiemat & AL-Odat, 2024; Amara *et al*., 2017; Mukherjee, 2019; Shabbir *et al*., 2024; Bouchama & Kamal 2021; Saxena & Gayathri 2021; George & Sagayarajan, 2023) [3, 34, 5, 7, 44, 61, 18, 58, 25]. It provides continuous oversight of cloud environments. Auditing involves reviewing access logs, system configurations, and security protocols to identify vulnerabilities or suspicious activities (Kunduru 2023) [34]. Monitoring, on the other hand, tracks real-time network traffic, user behaviors, and system performance to detect any anomalies that could indicate a cyberattack. Together, these practices enable early detection of potential threats, ensure compliance with security policies, and help organizations respond quickly to security incidents. Regular auditing and monitoring also provide valuable insights for improving security measures and mitigating future risks (Mukherjee, 2019; Shabbir *et al*., 2024; Bouchama & Kamal 2021; Saxena & Gayathri 2021; Arogundade 2024; Alenezi 2021; Amara *et al*., 2017) [44, 61, 18, 58, 9, 34, 7].

Cloud network security is a key strategy highlighted by study as a mitigating strategy against cyberattacks in cloud computing, focusing on protecting the cloud infrastructure from unauthorized access, attacks, and data breaches (Kunduru, 2023; Pranjal 2024; Bautista-Villalpando & Abran 2021; Shabbir *et al*., 2024; AL-Qtiemat & AL-Odat, 2024; Amara *et al*., 2017; Alenezi, 2021) [34, 50, 15, 61, 5, 6, 3]. It involves implementing security measures such as firewalls, intrusion detection and prevention systems (IDPS), and secure virtual private networks (VPNs) to safeguard network traffic. Cloud network security also includes segmentation, where the network is divided into secure zones to limit the spread of threats, and the use of encryption to protect data in transit. By enhancing visibility into network activities and restricting access, cloud network security helps prevent common cyberattacks like DDoS, man-in-the-middle, and unauthorized intrusions (Kunduru 2023; George & Sagayarajan, 2023; Bautista-Villalpando and Abran 2021; Shabbir *et al*., 2024; AL-Qtiemat & AL-Odat, 2024; Alenezi, 2021) [34, 25, 15, 61, 3]. Implementing robust network security practices, including monitoring and intrusion detection systems, has been shown to reduce unauthorized access incidents by 30% (Exabeam 2023) [24].

Physical security of infrastructure is another mitigating strategy revealed in the study review (AL-Qtiemat & AL-Odat, 2024; Bautista-Villalpando & Abran 2021; Alenezi, 2021) [5, 15, 3]. Physical security of infrastructure and servers is a critical strategy in mitigating cyberattacks in cloud computing by ensuring that the hardware hosting cloud data and services is protected from unauthorized physical access, damage, or theft. This includes securing data centers with multiple layers of defense, such as biometric access controls, surveillance systems, and security personnel. Additionally, backup power supplies, fire suppression systems, and climate controls are essential to maintaining the integrity of the servers. By preventing physical tampering or damage, physical security measures help safeguard the infrastructure, ensuring the availability and confidentiality of cloud services and data (Bautista-Villalpando & Abran 2021; AL-Qtiemat & AL-Odat, 2024; Alenezi, 2021) [15, 5, 3].

The use of a Web Application Firewall (WAF) is an effective strategy for mitigating cyberattacks in cloud computing (Nwaocha & Oloyede, 2023; Amjad *et al*., 2019; Sharma 2024; Alenezi 2021; Pranjal 2024) [48, 8, 63, 3, 50]. A WAF monitors and filters incoming and outgoing traffic to cloud-based web applications, protecting them from threats such as cross-site scripting (XSS), SQL injection, and distributed denial-of-service (DDoS) attacks. By inspecting HTTP/HTTPS requests, a WAF can detect and block malicious traffic in real time, ensuring that only legitimate users gain access to the cloud applications. This adds an extra layer of defense, preventing vulnerabilities from being exploited and enhancing the overall security of cloud environments (Amjad *et al*., 2019; Sharma 2024; Nwaocha & Oloyede, 2023; Alenezi 2021; Pranjal 2024) [8, 63, 48, 63, 3, 50]. WAFs are highly effective for protecting against common web application attacks, such as SQL injections and cross-site scripting (XSS). When used with proper patching and updates, WAFs can block over 70% of known web-based attacks (El Kafhali *et al*., 2022) [22].

A Content Delivery Network (CDN) is a valuable strategy for mitigating cyberattacks in cloud computing by distributing content across multiple servers located globally. This decentralization enhances security by reducing the risk of DDoS attacks, as traffic is spread across several points, preventing any single server from being overwhelmed.

CDNs also provide faster content delivery, improving website performance and reducing latency. Additionally, CDNs can include built-in security features such as encryption, bot protection, and traffic filtering, which further help mitigate cyber threats like malware and unauthorized access to cloud resources.

Implementing strong Application Programming Interfaces (API) is a crucial strategy for mitigating cyberattacks in cloud computing, as APIs are often gateways to cloud services and data (Saxena & Gayathri 2021; Reece *et al*., 2024; Amara *et al*., 2017; Nwaocha & Oloyede, 2023) [58, 54, 6, 48]. Securing APIs involves enforcing strict authentication and authorization protocols, such as OAuth, and using encryption to protect data in transit. Rate limiting and input validation are also important to prevent abuse and attacks like denial-of-service (DoS) and injection attacks. By ensuring APIs are properly designed, monitored, and patched for vulnerabilities, organizations can reduce the risk of unauthorized access, data breaches, and other cyber threats targeting cloud-based applications (Reece *et al*., 2024; Amara *et al*., 2017; Mukherjee 2019; Nwaocha & Oloyede, 2023) [54, 6, 44, 48].

Cloud penetration testing is a proactive strategy for mitigating cyberattacks in cloud computing by simulating real-world attacks to identify vulnerabilities in cloud infrastructure, applications, and services (George & Sagayarajan, 2023; Kunduru, 2023) [25, 34]. This testing involves assessing security controls, access points, and configurations to uncover weaknesses that could be exploited by malicious actors. By conducting regular penetration tests, organizations can detect security gaps, evaluate the effectiveness of existing defenses, and implement necessary fixes before attackers can exploit them. This approach enhances cloud security by enabling continuous improvement and preparedness against potential cyber threats (George & Sagayarajan, 2023; Kunduru, 2023) [25, 34]. Regular cloud penetration testing helps identify and address vulnerabilities before they can be exploited. It has been shown that organizations that conduct frequent penetration tests experience 27% fewer successful attacks (SecurDI, 2023) [60].

Conclusion

The findings of this study revealed the critical importance of adopting a multi-layered approach to mitigate cyber-attacks in cloud computing environments. Through a systematic review of empirical evidence, it is clear that no single solution is sufficient to address the complex and evolving nature of cloud security threats. Strategies such as advanced data encryption, Web Application Firewall (WAF), content delivery network (CDN), and the use of cloud network security have demonstrated significant effectiveness in protecting cloud systems. Moreover, the integration of multi-factor authentication (MFA), robust Identity and Access Management (IAM) systems, and adherence to regulatory standards are essential in reducing the risks of data breaches and unauthorized access. Regular security audits, penetration testing, and ongoing employee training also emerged as vital components of a resilient cloud security framework. The review emphasizes that a comprehensive approach, combining technical defenses with procedural policies and human awareness, offers the best protection against the wide array of cyber-attacks targeting cloud infrastructure. By implementing these mitigation strategies, organizations can not only improve their cloud security but also strengthen their ability to detect, prevent, and respond to cyber threats in real time. This study concludes that cloud service providers and users must remain vigilant, continuously evolving their security practices in response to emerging cyber threats to safeguard data, maintain trust, and ensure the integrity of their cloud systems.

Study Limitations

This study has several limitations that should be considered when interpreting the findings. First, the systematic review was based on a relatively small sample of studies, with only twenty papers selected for analysis. This limited number of studies may not capture the full range of available research on mitigating strategies against cyber-attacks in cloud computing. As a result, some relevant strategies or emerging trends could have been overlooked. Second, the review exclusively focused on papers written in English, which may have introduced a language bias. Research published in other languages might have provided valuable insights or alternative perspectives on the topic that were not captured in this review. Consequently, the study may not represent the full global landscape of cloud security strategies.

The timeframe for selecting the studies was restricted to those published between 2017 and 2024. While this period includes recent advancements in cloud computing security, it may exclude foundational studies or earlier empirical research that could still be relevant to understanding long-term trends and strategies. The study employed content summation as the primary method for analyzing the selected papers. While this approach provides an overview of common themes and strategies, it may lack the depth of more rigorous qualitative or quantitative analysis techniques, potentially limiting the comprehensiveness of the findings. These limitations suggest that future research should consider expanding the sample size, including non-English papers, and employing diverse analytical methods to provide a more holistic view of mitigating strategies against cyber-attacks in cloud computing.

References

1. Ahmadi S. Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security. 2024 Mar 27;15:148-67. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4775074
2. Akhtar N, Kerim B, Perwej Y, Tiwari A, Praveen S. A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science, Engineering and Technology. 2021. https://hal.science/hal-03350900/
3. Alenezi M. Safeguarding Cloud Computing Infrastructure: A Security Analysis. Computer Systems Science & Engineering. 2021, 37(2). https://malenezi.github.io/malenezi/pdfs/Safeguarding%20Cloud%20Computing%20Infrastructure%20%20A%20Security%20Analysis.pdf
4. Alhenaki L, Alwatban A, Alahmri B, Alarifi N. Security in cloud computing: a survey. International Journal of Computer Science and Information Security. 2019;17(4):67-90. https://www.academia.edu/download/59222973/05_Pap

er_31031920_IJCSIS_Camera_Ready_pp67-9020190512-80804-19u1ak0.pdf
5. AL-Qtiemat EMA, AL-Odat ZEY. Examining cloud security: identifying risks and the implemented mitigation strategies. Journal of Theoretical and Applied Information Technology. 2024, 102(7). http://www.jatit.org/volumes/Vol102No7/26Vol102No7.pdf
6. Amara N, Zhiqui H, Ali A. Cloud computing security threats and attacks with their mitigation techniques. In: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE; c2017. p. 244-251. https://ieeexplore.ieee.org/abstract/document/8250365/
7. Amara N, Zhiqui H, Ali A. Cloud computing security threats and attacks with their mitigation techniques. In: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC); c2017 Oct 12 p. 244-251. IEEE. https://ieeexplore.ieee.org/abstract/document/8250365/
8. Amjad A, Alyas T, Farooq U, Tariq MA. Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems. 2019 Aug 12;6(23):e7-. https://publications.eai.eu/index.php/sis/article/view/2157
9. Arogundade OR. Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework. International Advanced Research Journal in Science, Engineering and Technology. IARJSET. 2024 Jan 1;11(1):2394-1588
10. Arunkumar JR. Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies. Journal of Scientific Computing and Engineering Research. 2023;6(8):6-10. https://jscer.org/wp-content/uploads/2023-Volume%206-Issue%208/Study%20Analysis%20of%20Cloud%20Security%20Challenges%20and%20Issues%20in%20Cloud%20Computing%20Technologies%20five.pdf
11. Awaysheh FM, Aladwan MN, Alazab M, Alawadi S, Cabaleiro JC, Pena TF. Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management. 2021;69(6):3676-3693. https://ieeexplore.ieee.org/abstract/document/9349765/
12. Baciu IE. Advantages and disadvantages of cloud computing services, from the employee's point of view. National Strategic Observations. 2015, 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2787612
13. Barona R, Anita EM. A survey on data breach challenges in cloud computing security: Issues and threats. In: 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE; c2017. p. 1-8. https://ieeexplore.ieee.org/abstract/document/8074287/
14. Basu S. 68 Cloud Security Statistics to Be Aware of in 2023. 2022 [cited 2024 Sep 28]. Available from: https://securitysenses.com/archive/organisation/2179/created/202304
15. Bautista-Villalpando LE, Abran A. A Data Security Framework for Cloud Computing Services. Computer Systems Science & Engineering. 2021 May 1;37(2). https://pdfs.semanticscholar.org/8965/a915ebc6ab187e70b392cb183d287dd981f3.pdf
16. Bentaleb O, Belloum AS, Sebaa A, El-Maouhab A. Containerization technologies: Taxonomies, applications and challenges. Journal of Supercomputing. 2022;78(1):1144-1181. https://link.springer.com/article/10.1007/s11227-021-03914-1
17. Bentaleb O, Belloum AS, Sebaa A, El-Maouhab A. Containerization technologies: Taxonomies, applications and challenges. The Journal of Supercomputing. 2022 Jan;78(1):1144-1181. https://link.springer.com/article/10.1007/s11227-021-03914-1
18. Bouchama F, Kamal M. Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. International Journal of Business Intelligence and Big Data Analytics. 2021 Sep 3;4(9):1-9. https://research.tensorgate.org/index.php/IJBIBDA/article/view/76
19. Christina AA. Proactive measures on account hijacking in cloud computing network. Asian Journal of Computer Science and Technology. 2015;4(2):31-34. https://ajcst.co/index.php/ajcst/article/view/1753
20. Claycomb WR, Nicoll A. Insider threats to cloud computing: Directions for new research challenges. In: 2012 IEEE 36th Annual Computer Software and Applications Conference. IEEE; c2012. p. 387-94. https://ieeexplore.ieee.org/abstract/document/6340188/
21. Deepak MD, Kumar S, Lal D. Major hurdles of cyber security in the 21st Century. International Journal of Engineering and Advanced Technology. 2020;9(3):1470-1476. DOI: https://doi.org/10.35940/ijeat.C5135.029320.
22. El Kafhali S, El Mir I, Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering. 2022 Jan;29(1):223-246. https://link.springer.com/article/10.1007/s11831-021-09573-y
23. Elsayed MAMA. Advancing Security Services for Cloud Applications [Doctoral dissertation]. Queen's University (Canada); c2018. https://search.proquest.com/openview/44ce14c578e5fb08355550002fe52510/1?pq-origsite=gscholar&cbl=18750
24. Exabeam. Cloud Security Threats: Top Threats and 3 Mitigation Strategies. 2023. Available at: https://www.exabeam.com/explainers/cloud-security/cloud-security-threats-top-threats-and-3-mitigation-strategies/
25. George AS, Sagayarajan S. Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS, and SaaS environments. Partners University International Research Journal. 2023;2(1):24-34. https://www.puirj.com/index.php/research/article/view/84
26. Golightly L, Chang V, Xu QA, Gao X, Liu BS. Adoption of cloud computing as innovation in the organization. International Journal of Engineering and Business Management. 2022;14:18479790221093992.

https://journals.sagepub.com/doi/abs/10.1177/18479790221093992
27. Gupta A, Vanbever L, Shahbaz M, Donovan SP, Schlinker B, Feamster N, *et al*. SDX: A software defined internet exchange. ACM SIGCOMM Computer Communication Review. 2014;44(4):551-562. https://dl.acm.org/doi/abs/10.1145/2740070.2626300
28. Hassan J, Shehzad D, Habib U, Aftab MU, Ahmad M, Kuleev R, *et al*. [Retracted] The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR). Computational Intelligence and Neuroscience. 2022;2022:8303504. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/8303504
29. Hussein MK, Mousa MH, Alqarni MA. A placement architecture for a container as a service (CaaS) in a cloud environment. Journal of Cloud Computing. 2019;8:1-15. https://link.springer.com/article/10.1186/s13677-019-0131-1
30. Jemal I, Cheikhrouhou O, Hamam H, Mahfoudhi A. SQL injection attack detection and prevention techniques using machine learning. International Journal of Applied Engineering Research. 2020;15(6):569-580.
31. Jones C. Phishing stats you should know in 2022. ExpertInsights.com. 2022 [cited 2024 Sep 28]. Available from: https://expertinsights.com/insights/50-cloud
32. Khalifa N, Elmedany W. Security in cloud computing: threats, mitigation strategies, and future directions. The Institution of Engineering and Technology. 2023 Nov 5;499-505. https://digital-library.theiet.org/content/conferences/10.1049/icp.2024.0974
33. Khodayer A, Khodayer O, Alexandra M. Cloud computing and its security in real applications. Al-Rafidain Journal of Engineering Sciences. 2024 Jun 4:310-21. https://rjes.iq/index.php/rjes/article/view/63
34. Kunduru AR. Security concerns and solutions for enterprise cloud computing applications. Asian Journal of Research in Computer Science. 2023;15(4):24-33. http://article.researchpromo.com/id/eprint/667/
35. La Torre M, Dumay J, Rea MA. Breaching intellectual capital: critical reflections on big data security. Mediterrari Accountancy Research. 2018;26(3):463-482. https://www.emerald.com/insight/content/doi/10.1108/MEDAR-06-2017-0154/full/html
36. Li Q, Wang ZY, Li WH, Li J, Wang C, Du RY. Applications integration in a hybrid cloud computing environment: Modelling and platform. Enterprise Information Systems. 2013;7(3):237-271. https://www.tandfonline.com/doi/abs/10.1080/17517575.2012.677479
37. Liubchenko VV, Volkov DV. Cyber-aware threats and management strategies in cloud environments. Herald of Advanced Information Technology. 2024;2(7):158-70. https://hait.od.ua/index.php/journal/article/view/215
38. Mallick MAI, Nath R. Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News. 2024;190(1):1-69. https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf
39. Martin KD, Borah A, Palmatier RW. Data privacy: Effects on customer and firm performance. Journal of Marketing. 2017;81(1):36-58. https://journals.sagepub.com/doi/abs/10.1509/jm.15.0497
40. Medaram SK, Maglaras L. Malware mitigation in cloud computing architecture. In: Cyber Malware: Offensive and Defensive Systems. Cham: Springer International Publishing; c2023. p. 235-78. https://link.springer.com/chapter/10.1007/978-3-031-34969-0_9
41. Mikkonen I, Khan I. Cloud computing: SME company point of view. In: Management Challenges in the 21st Century: Digitalization of Society, Economy and Market; c2016. https://www.theseus.fi/handle/10024/114309
42. Mohamad Fadli Z, Yong SS, Kee LK, Ching GH. Cyber attack awareness and prevention in network security. International Journal of Informatics and Communication Technology. 2022;11(2):105-115. DOI: https://doi.org/10.11591/ijict.v11i2.pp105-115. https://hait.od.ua/index.php/journal/article/view/215
43. Mozumder DP, Mahi JN, Whaiduzzaman M, Mahi MJN. Cloud computing security breaches and threats analysis. International Journal of Scientific & Engineering Research. 2017;8(1):1287-1297. https://www.researchgate.net/profile/Mdjulkar-Nayeen-Mahi/publication/320124329_Cloud_Computing_Security_Breaches_and_Threats_Analysis/links/59cef3c8aca2721f434f0493/Cloud-Computing-Security-Breaches-and-Threats-Analysis.pdf
44. Mukherjee S. Cloud-based security solutions. IUP Journal of Computer Science. 2019;13(4):72-78. https://pdfs.semanticscholar.org/078c/1f5d23b147b17d74caa5038a452c9e96222e.pdf
45. Nadeem M, Zahra SW, Abbasi MN, Nazir MM, Shahid M. Phishing attacks and online security practices in cloud computing. In: 2021 2nd International Conference on Computing and Information Technology (ICCIT-1442). IEEE; c2021. p. 129-33.
46. Nayak J, Meher SK, Souri A, Naik B, Vimal S. Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. The Journal of Supercomputing. 2022 Sep;78(13):14866-14891. https://link.springer.com/article/10.1007/s11227-022-04453-z
47. Nazari Jahantigh M, Masoud Rahmani A, Jafari Navimirour N, Rezaee A. Integration of internet of things and cloud computing: a systematic survey. IET Communications. 2020 Jan;14(2):165-176. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2019.0537
48. Nwaocha VO, Oloyede A. Averting DDOS attacks in web-based applications. Available at: Orca security. 2022 State of Public Cloud Security Report Reveals Critical Cloud Security Gaps. 2022 Available at: https://orca.security/resources/blog/state-public-cloud-top-critical-cloud-security-gaps/
49. Perera S, Jin X, Maurushat A, Opoku DG. Factors affecting reputational damage to organisations due to

cyberattacks. Informatics. 2022 Mar 18;9(1):28. https://www.mdpi.com/2227-9709/9/1/28
50. Pranjal, M. R. Data security on cloud services: threats and mitigation. International Journal of Scientific Research in Engineering and Management. 2024, April 21;2582-3930. https://ijsrem.com/download/data-security-on-cloud-services-threats-and-mitigation/
51. Raja K, Hanifa SM. Big data driven cloud security: A survey. In: IOP Conference Series: Materials Science and Engineering. 2017 Aug;225(1):012184. https://iopscience.iop.org/article/10.1088/1757-899X/225/1/012184/meta
52. Rani BK, Rani BP, Babu AV. Cloud computing and inter-clouds – types, topologies, and research issues. Procedia Computer Science. 2015 Jan 1;50:24-29. https://www.sciencedirect.com/science/article/pii/S1877050915005074
53. Razi M, Batan A. Opportunities and challenges of cloud computing in developing countries. Artificial Intelligence in Society. 2023 Jan 11;3(1):1-8. https://www.researchberg.com/index.php/ai/article/view/93
54. Reece M, Rastogi N, Lander T, Dykstra J, Mittal S, Sampson A. Defending multi-cloud applications against man-in-the-middle attacks. In: Proceedings of the 29th ACM Symposium on Access Control Models and Technologies. 2024 Jun 24:47-52. https://dl.acm.org/doi/abs/10.1145/3649158.3657051
55. Sai Shreya R, Kavitha R. Securing SaaS: key challenges and effective mitigation strategies. 2024. http://www.ijmrset.com/upload/96_Securing.pdf
56. Saratchandra M, Shrestha A. The role of cloud computing in knowledge management for small and medium enterprises: A systematic literature review. Journal of Knowledge Management. 2022 Nov 2;26(10):2668-2698. https://www.emerald.com/insight/content/doi/10.1108/JKM-06-2021-0421/full/html
57. Saxena N, Hayes E, Bertino E, Ojo P, Choo KK, Burnap P. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020 Sep 7;9(9):1460. Available from: https://www.mdpi.com/2079-9292/9/9/1460
58. Saxena R, Gayathri E. A study on vulnerable risks in security of cloud computing and proposal of its remedies. Journal of Physics: Conference Series. 2021 Oct 1;2040(1):012008. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/2040/1/012008/meta
59. Schulz-Zander J, Mayer C, Ciobotaru B, Lisicki R, Schmid S, Feldmann A. Unified programmability of virtualized network functions and software-defined wireless networks. IEEE Transactions on Network and Service Management. 2017 Aug 25;14(4):1046-1060. Available from: https://ieeexplore.ieee.org/abstract/document/8016637/
60. SecurDI. Data Security in the Cloud: Risks and Mitigation Strategies. 2023. Available from: https://securdi.com/cloud-security/data-security-in-the-cloud-risks-and-mitigation-strategies/
61. Shabbir A, Anwar AS, Taslima N, Sayem MA, Sikder AR, Sidhu GS. Analyzing enterprise data protection and safety risks in cloud computing using ensemble learning. International Journal on Recent and Innovation Trends in Computing and Communication. 2024;12(2):499-507.
62. Shahriar H, Zulkernine M. Information-theoretic detection of SQL injection attacks. In: 2012 IEEE 14th international symposium on high-assurance systems engineering; 2012 Oct 25; pp. 40-47. IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/6375635/
63. Sharma H. The evolution of cybersecurity challenges and mitigation strategies in cloud computing systems. International Journal of Computer Engineering and Technology. 2024 Jul 31;15(4):118-27. Available from: https://iaeme-library.com/index.php/IJCET/article/view/IJCET_15_04_010
64. Shilpa M. Navigating Privacy and Security in Cloud Computing. Recent Trends in Parallel Computing. 2024 Aug 22;11(02):1-0. Available from: https://research-reels.com/publication/navigating-privacy-and-security-in-cloud-computing/
65. Suliman ME, Madinah KS. A brief analysis of cloud computing Infrastructure as a Service (IaaS). International Journal of Innovative Science and Research Technology. 2021 Jan;6(1):1409-12.
66. Surya L. Software as a service in cloud computing. International Journal of Creative Research Thoughts. 2019 Dec 4;2320-882. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3674386
67. Tao Y, Wang X, Xu X, Liu G. Container-as-a-service architecture for business workflow. International Journal of Simulation and Process Modelling. 2018;13(2):102-15. Available from: https://www.inderscienceonline.com/doi/abs/10.1504/IJSPM.2018.091692
68. Thales. Cloud assets the biggest targets for cyberattacks, as data breaches increase. 2023. Available from: https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release
69. Upadhyay U, Kumar A, Sharma G, Saini AK, Arya V, Gaurav A, *et al*. Mitigating risks in the cloud-based metaverse access control strategies and techniques. International Journal of Cloud Applications and Computing. 2024 Jan 1;14(1):1-30. Available from: https://www.igi-global.com/article/mitigating-risks-in-the-cloud-based-metaverse-access-control-strategies-and-techniques/334364
70. Vellela SS, Balamanigandan R, Praveen SP. Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology. 2022 May;2(1). Available from: https://jnxtgentech.com/mail/documents/Strategic%20Survey%20on%20Security%20and%20Privacy%20Methods%20of%20Cloud%20Computing%20Environment.pdf
71. Walling S, Lodh S. A Comprehensive Review on Security Attacks and Countermeasures in IoT Environment. In: International Conference on Information and Communication Technology for Competitive Strategies; 2022 Oct 9; p. 613-623. Singapore: Springer Nature Singapore. Available from:

https://link.springer.com/chapter/10.1007/978-981-19-9638-2_53
72. Yasrab R. Platform-as-a-service (PaaS): The next hype of cloud computing. arXiv preprint arXiv:1804.10811. 2018 Apr 28. Available from: https://arxiv.org/abs/1804.10811
73. Zatonatska T, Dluhopolskyi O. Modelling the efficiency of the cloud computing implementation at enterprises. Available from: https://essuir.sumdu.edu.ua/handle/123456789/74690