Mitigation Strategies for Security Challenges and Attacks in Cloud Computing

Author* | Email | Orcid

Asmatullah Nashir
Assistant Professor, Information Technology Computer Science Faculty, Badakhshan University, Badakhshan, Afghanistan
asmatullah@badakhshan.edu.af
https://orcid.org/0009-0004-9976-4461

Author | Email | Orcid

Mohammadullah shirpoor
Assistant Professor, Information Technology Computer Science Faculty, Badakhshan University, Badakhshan, Afghanistan
m.shirpoor@badakhshan.edu.af
https://orcid.org/0009-0001-2115-1217

Abstract

Cloud computing, as one of the emerging technologies, has rapidly become a significant part of information systems and plays an important role in daily life and businesses. While this technology is recognized as an effective tool for delivering services, it faces various types of attacks and challenges. The purpose of this study to investigate the security challenges and types of attacks that cloud computing faces and propose mitigation strategies to address these issues. The research employed a qualitative method, focusing on analyzing previous studies and reports to identify the primary security vulnerabilities and attacks targeting cloud services. The paper identifies security challenges and attacks in cloud computing, proposing mitigation strategies such as encryption, multi-factor authentication, and regular audits to improve security and reliability in cloud environments.

Keywords: Cloud Computing, Deployment Models, Service Models, Security Challenges, Attacks, Mitigation Strategies

[*] asmatullah@badakhshan.edu.af

راه‌کارهای کاهش چالش‌های امنیتی و حملات در محاسبات ابری

پوهنمل عصمت الله ناشر
نویسنده دیپارتمنت تکنالوژی معلوماتی، پوهنځی کمپیوترساینس، پوهنتون بدخشان
نشانی برقی Asmatullah@badakhshan.edu.af
نشانی ارکاید https://orcid.org/0009-0004-9976-4461

پوهنمل محمدالله شیرپور
نویسنده تکنالوژی معلوماتی پوهنځی کمپیوترساینس، پوهنتون بدخشان،
نشانی برقی m.shirpoor@badakhshan.edu.af
نشانی ارکاید https://orcid.org/0009-0001-2115-1217 4461

چکیده

محاسبات ابری، به عنوان یکی از تکنالوژی‌های نوظهور، به سرعت به بخشی مهم از سیستم‌های اطلاعاتی تبدیل شده و نقش قابل توجهی در زندگی روزمره و کسب‌وکارها ایفا می‌کند. در حالی‌که این فناوری به عنوان ابزاری مؤثر برای ارایه‌ی خدمات شناخته می‌شود، با انواع مختلفی از حملات و چالش‌های امنیتی مواجه است. این مقاله به بررسی چالش‌ها و حملات امنیتی موجود در محاسبات ابری پرداخته و راه‌کارهای موثر برای رسیدگی به این موضوع را ارایه می‌دهد. این تحقیق از روش کیفی استفاده کرده و بر تحلیل و بررسی‌های تحقیقات قبلی تمرکز دارد تا آسیب‌پذیری‌های اصلی امنیتی و حملات هدف‌گذاری شده به خدمات ابری را شناسایی کند. در نتیجه، استفاده این راه‌کارهای می‌تواند امنیت و قابلیت اعتماد خدمات ابری را بهبود بخشد و محیط‌های ایمن‌تری برای کاربران و سازمان‌ها فراهم کند.

کلیدواژه‌ها: محاسبات ابری، مدل‌های استقرار، مدل‌های خدمات، چالش‌های امنیتی، حملات، راه‌کارها

Pamir Academic & Research Journal - دپامیر علمی څېړنیزه مجله - مجله‌ی علمی-تحقیقی پامیر /

Mitigation Strategies for Security Challenges and Attacks in Cloud Computing

Introduction

The term "Cloud" refers to a network or the Internet, symbolizing a paradigm shift in how data and applications are stored, accessed, and managed. It implies that the resources, whether they be computing power, storage, or applications, are available remotely rather than on local machines. This remote availability allows users to access their data and services from anywhere with an Internet connection, providing unprecedented flexibility and convenience (Malik et al.,2018). Cloud computing refers to the delivery of computing resources, such as hardware and software, as services over a network. It represents a modern approach to computing where resources are dynamically scalable and often virtualized, available via the Internet. With cloud technology, users can access applications, storage, and development platforms using various devices, including PCs, laptops, smartphones, and PDAs, through services provided by cloud computing providers(Mujahid et al., 2016). Cloud services can be implemented through five primary models: (i) public cloud, (ii) private cloud, (iii) hybrid cloud, (iv) community cloud, and (v) multi-cloud deployment (Surianarayanan & Chelliah, 2019).

While previous research has addressed security issues in cloud computing, the rapid evolution of the technology, coupled with a lack of understanding of the underlying problems, means that it remains in its early stages. As researchers struggle to offer effective solutions to the quickly emerging challenges, existing literature has outlined various challenges and attacks along with some proposed solutions. This paper aims to compile and explain the fundamental security threats and attacks present in the cloud environment, detailing mitigation strategies for each. Additionally, it categorizes these threats based on the cloud services they impact, and the network layers involved. This classification aids security engineers in addressing specific issues and enhances newcomers' understanding of cloud computing challenges, attacks, and mitigation strategies (T.K & B, 2016).

Problem statement

Cloud computing has become an important part of our everyday lives and modern technology, but it faces many security problems, including data breaches and unauthorized access to sensitive information. Despite its effectiveness in delivering essential services such as data storage and remote access, the rise of sophisticated cyber-attacks poses significant risks to the confidentiality and integrity of cloud-stored data. The lack of comprehensive understanding and effective mitigation strategies to address these security challenges hampers the reliability of cloud services and undermines user trust. This paper aims to identify the specific security challenges and attack vectors present in cloud computing environments and propose targeted mitigation strategies to improve safety and trust in cloud services.

Research Questions

The main and sub-research questions for this study are outlined as follows:

Main research questions:

1. What are the most effective mitigation strategies to protect cloud computing environments from security challenges and attacks?

Sub question:

1. What are the most common security challenges faced by cloud computing services?

2. What are the common types of security attacks and threats in cloud computing environments? What best practices can organizations adopt to protect against data breaches and unauthorized access in cloud environments?

Research Objectives

Main Objective

1. To identify and evaluate effective mitigation strategies for enhancing security in cloud computing environments against various challenges and attacks.

Sub-Objectives

1. To analyze the common security challenges and attacks faced by cloud computing services.
2. To investigate the different types of security attacks.
3. To develop recommendations for organizations to adopt best practices that enhance security cloud services.
4. Research Significance
5. The significance of this research lies in addressing the growing security concerns in cloud computing, which has become a critical component of modern information technology infrastructures. As cloud services continue to evolve and become integral to daily operations for individuals and organizations alike, they face increasing threats in the form of various cyber-attacks. This research provides valuable insights into the types of security challenges and attacks that target cloud environments. By identifying these threats and proposing effective mitigation strategies, the study contributes to enhancing the overall security and reliability of cloud services, protecting sensitive data, and improving user trust. Additionally, the findings of this research have the potential to guide cloud service

providers and users in adopting better security measures, which are essential for safeguarding information in a rapidly digitizing world.

Literature review

This paper highlights various security issues in the cloud computing environment and identifies future directions to address these challenges. However, this paper does not provide any solutions to mitigate the security challenges and attacks (Sabeena & Antelin Vijila, 2021).

In this paper, the researchers explore key challenges such as XML Signature Wrapping attacks, browser vulnerabilities, and vendor lock-in, and provide potential solutions to address these issues. The findings aim to contribute to improving the security and reliability of cloud environments. While this paper focuses on three specific types of attacks, my paper covers a broader range of attacks in the cloud environment (Alshammari et al., 2017).

This research compares three cloud service models, examines associated security risks and threats, highlights real-world cloud attacks, and proposes countermeasures to address cloud security breaches. While this paper focuses on service models, my paper also explores the security issues related to deployment models (Chou, 2013).

This study highlights well-known authentication attacks and reviews various studies that have explored each attack. However, it does not provide any strategies to improve security in the cloud computing (Abusaimeh, 2020).

This paper explores the architectural principles of cloud computing, key security requirements, security threats and attacks, and their mitigation techniques, while also identifying future research challenges. However, it does not explore the security challenges specific to cloud computing (Amara et al., 2017).

The researchers conduct a survey to identify the most critical threats to cloud computing, their impacts, causes, and suggest solutions. It also highlights the affected security attributes of cloud computing and ranks these threats according to their severity. While this research identifies the threats, my paper also covers the attacks in addition to the threats (A. Kofahi, 2018).

This paper provides an overview of cloud computing architecture, security issues, and frameworks, reviews literature on security solutions, categorizes cloud attacks and privacy challenges, and discusses defense mechanisms. While this paper focuses on identifying and categorizing security threats, my paper not only highlights these issues but also provides detailed mitigating techniques and solutions to address the identified security risks in cloud computing environments (El Kafhali et al., 2022) .

Research Methodology

The research method employed in this study is primarily based on library research. This approach involves an extensive review of existing literature related to cloud computing security challenges and attacks. By analyzing scholarly articles, reports, and case studies, the research aims to identify prevalent security issues, categorize various types of attacks, and explore mitigation strategies. This method allows for a comprehensive understanding of the current state of research in the field, providing a solid foundation for proposing recommendations to enhance the security and reliability of cloud services.

Results and Findings

Cloud computing architecture has five main deployment models which are defined below:

Private Cloud: A private cloud is set up by an organization or a chosen service provider, offering a dedicated, single-tenant environment. It provides the advantages of cloud computing, such as scalability and flexibility, along with the accountability and utility features of the cloud model (Pakash et al, 2016). A private cloud limits access to a specific group of users, typically within a particular organization. It functions similarly to an intranet, where services are delivered internally through the organization's own network (Sehgal et al., 2023).

Public cloud: A public cloud is a cloud computing model where services, such as storage and applications, are provided by third-party providers over the internet. These resources are shared among multiple users or organizations, offering cost-effective and scalable solutions. In a public cloud deployment, cloud service providers deliver their infrastructure and services remotely over the internet to any public users who subscribe, offering a pay-per-use pricing model based on demand (Surianarayanan & Chelliah, 2019).

Hybrid cloud: This model of cloud computing is a composition of two cloud (public or private) (Zatakiya & Tank, 2013). A hybrid cloud combines both public and private cloud environments, allowing data and applications to be shared between them. This model offers greater flexibility, enabling organizations to take advantage of both public cloud scalability and the security of a private cloud. It is ideal for businesses that need to manage sensitive data while also leveraging the cost-efficiency of public cloud resources.

Community cloud: Cloud infrastructure can be shared by multiple organizations to support a specific community, like shared resources in a housing complex. Residents use and share the costs of cloud-based services provided exclusively for them, much like they would with communal utilities (Sehgal et al., 2023).

Multi-cloud deployment: multi-cloud refers to the use of services from multiple public cloud providers by an organization or individual to achieve specific business goals. It allows users to integrate different services, such as IaaS from one provider and PaaS from another, to optimize cost, performance, and functionality according to their needs (Surianarayanan & Chelliah, 2019).

Service delivery model of the cloud

Software as a Service (SaaS): In the SaaS model, the cloud provider is responsible for deploying the applications on the cloud (A. Kofahi, 2018). (SaaS) delivers applications over the internet, allowing users to access software without installing it locally. It provides a convenient, subscription-based model where the service provider manages infrastructure, maintenance, and updates.

Platform as a Service (PaaS): In this model, users can utilize the programming languages and tools provided by the service provider to deploy their own developed or acquired applications on the cloud infrastructure. While the client can manage the deployment of applications and, in some cases, adjust the hosting environment settings, they do not have control over the underlying cloud infrastructure. Examples of PaaS services include Google App Engine and Force.com (El Kafhali et al., 2022).

Infrastructure as a Service (IaaS): In this model, the Cloud Service Provider (CSP) offers users virtualized hardware infrastructure to host their data. Users install their own operating systems and applications, managing tasks such as processing, networking, and storage on their deployed systems(Parikli et al., 2019). provides virtualized computing resources over the internet, such as servers, storage, and networking. Users have control over the operating systems and deployed applications but not the underlying cloud infrastructure.

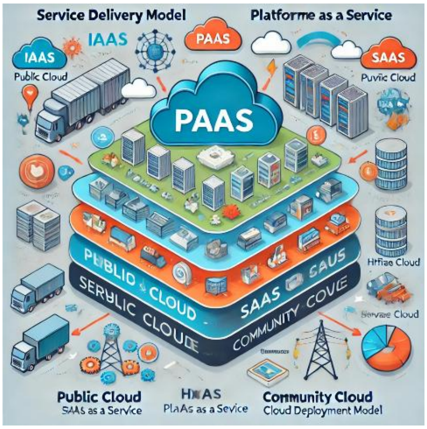

Fig 1: Deployment cloud Model

Fig2: Service delivery model

I. Security challenges in cloud computing

Cloud computing faces various data security risks, including hacker attacks, network failures, and inadequate encryption key management. Specific to cloud environments are challenges like resource separation failures and privilege abuse. In multi-tenant systems, if a cloud provider fails to properly isolate resources, a customer’s deleted data might still be accessible to others, increasing security vulnerabilities. Effective encryption and key management are crucial for protecting data; however, poor practices can lead to key loss or unauthorized access. (Kuo, 2011). Additionally, as cloud adoption grows, employees, especially system administrators, may become targets for cybercriminals who could exploit their privileges to steal sensitive information. The security of cloud computing differs depending on the models implemented, with the public cloud model presenting the most significant security challenges (Sehgal et al., 2023). Security and privacy are the primary concerns in cloud computing. In the cloud environment, users can access computing resources beyond those available in their physical systems. However, to interact with this virtual space, users must transmit their data across the cloud, which leads to various security concerns (Sajid, 2013). Cloud computing, while offering essential services like data storage and remote access, faces significant security challenges. Key concerns include data theft and unauthorized access by hackers, leading to potential attacks on users' sensitive and confidential information (Sasubilli & Venkateswarlu, 2021). Cloud computing presents numerous challenges each of these challenges has impacted the reliability and efficiency of cloud-based environments in relation to their core concept.

A: Privacy and security: One of the most significant challenges that reduce reliability and efficiency in cloud computing environments is ensuring the security and privacy of stored data. Cloud computing security has become a crucial subject in both industry and academic research and is a key factor hindering its advancement. Generally, security concerns in cloud-based environments are classified into three primary areas: susceptibility to attacks, adherence to standard security practices, and compliance with state or national data storage laws related to privacy and record-keeping. These challenges have raised concerns across various levels, including service providers, infrastructure, and end-users (Moghaddam et al., 2015).

B. Resource Allocation: Resource allocation is a key concept in cloud computing data centers due to the large volume of resources in cloud environments. It must ensure quality network service, avoid performance issues without increasing costs, and manage energy use efficiently. The challenges are categorized into three areas: network resources, processing resources, and energy-efficient resource allocation in data centers (Moghaddam et al., 2015).

C. Availability and Scalability: Adapting cloud capacity to meet on-demand services during varying workloads—such as static, periodic, unique, unpredictable, and continuously changing workloads—poses a significant challenge for cloud-based services. Without this adaptability, performance may suffer during peak workloads, or resources may become oversized during low-demand periods. Elastic resource scaling is the most effective solution for managing these workloads in a cloud computing environment, as it allows for more flexible resource provisioning compared to static scaling and reduces reliance on workload predictions.

D. Clouds Migration and Compatibility: The swift expansion and widespread adoption of cloud computing among users and businesses have prompted traditional IT providers to transition and modify their products such as conventional applications, operating systems, and middleware for cloud-based environments (Surianarayanan & Chelliah, 2019).

II. Possible Security attacks in cloud computing

The next section outlines various attacks on cloud computing security along with the corresponding mitigation techniques that can be implemented to address these threats. Table 2 below organizes these attacks according to Basic Security Level, VM Level, Network Security Level, and Application Security Level, along with their respective mitigation strategies.

(SQL) Injection Attacks: In standard SQL code, the attacker injects harmful code to access an unauthorized database in order to obtain sensitive user information. in this scenario, the website mistakenly recognizes the hacker's data as legitimate user data, allowing the attacker to understand the website's operations and subsequently make alterations to it (Ramasamy & V, 2016), (Egerton Taylor et al., 2019).

(XSS) Cross Site Scripting Attacks: The attacker embeds harmful code into the user's webpage, redirecting them to the attacker's site to retrieve sensitive information. This can occur through two methods: Stored XSS, which permanently saves the malicious code in a resource managed by the web application, or Reflected XSS, which immediately sends back the malicious code to the user without permanent storage. To mitigate XSS attacks, web applications should implement input validation and output encoding to prevent the insertion of malicious code. Additionally, employing security mechanisms like Content Security Policy (CSP) can help restrict the execution of unauthorized scripts (Gupta & Gupta, 2017).

Phishing Attacks: Attackers exploit cloud services in phishing attacks by manipulating web links to redirect users to fraudulent sites, allowing them to hijack accounts and access sensitive information. To combat phishing attacks, identifying spam emails and pop-ups using anti-spam tools is essential (Abusaimeh, 2020)**.**

Domain Name Server (DNS) Attacks: In DNS attacks, users inadvertently access malicious code instead of the intended domain name due to the attacker manipulating DNS to translate the domain into an IP address, compromising confidential data. To combat these attacks, security measures such as Domain Name System Security Extensions (DNSSEC) can be employed, providing authentication, data integrity, and verified denial of existence through digitally signed results to confirm data authenticity from the authoritative DNS server (Aishwarya et al., 2014)**.**

Man in the Middle Attacks (MITM): when an attacker intercepts communication between two parties, allowing unauthorized access to sensitive data. Common scenarios include session hijacking, data interception, and credential theft, where attackers can manipulate or eavesdrop on the exchange between users and cloud service providers. To mitigate these risks, organizations should implement several strategies: encrypt data in transit using Transport Layer Security (TLS) and end-to-end encryption to protect against eavesdropping; enforce strong authentication methods, such as Multi-Factor Authentication (MFA) and secure token systems; and establish a Public Key Infrastructure (PKI) to manage digital certificates for identity verification.

(DOS) Attacks: this kind of attacks are aimed at rendering services unavailable to authorized users by overwhelming the server with excessive data packets through methods such as SYN flooding, UDP flooding, and ICMP flooding. In this type of attack, the attacker continuously sends data packets to the target server without altering the nodes, consuming network bandwidth and depleting server resources, which ultimately disrupts legitimate access to the services. To mitigate these attacks, organizations can implement various strategies, including using firewalls to filter out malicious traffic, deploying Intrusion Prevention Systems (IPS) to detect and block attack patterns, and employing rate limiting to control the volume of traffic directed at the server (Kumar et al., 2016)**.**

Distributed Denial of Service (DDOS) Attacks: Distributed Denial-of-Service (DDoS) attacks are a more sophisticated form of Denial-of-Service (DoS) attacks, where the target server is flooded with an overwhelming volume of packets originating from multiple compromised networks. This coordinated influx of traffic exceeds the server's capacity to handle requests, effectively disabling the services it provides. The key distinction between DDoS and traditional DoS attacks lies in the scale and complexity, as DDoS attacks generate significantly more traffic, making them more difficult for the target server to manage (Lua & Yow, 2011). A Distributed Denial-of-Service (DDoS) attack involves multiple compromised computers, often referred to as bots or zombies, that target a single system to overwhelm it and disrupt its services (Sattar et al., 2015), (Dong et al., 2019).

Reused IP Address Attacks: When a user leaves a network, their allocated IP address is reassigned to a new user. This creates a risk of the new user accessing the previous user's data, as the IP address may still be stored in the DNS cache, potentially allowing unauthorized access to sensitive information. To combat denial of service attacks on cloud-based virtual networks, utilizing unpredictable IP addresses can increase the difficulty for attackers trying to find a target host. However, an analysis of IP address allocation by major cloud providers like Amazon Web Services and Google Cloud Platform reveals that the unpredictability of allocated IP addresses is limited. This predictability allows simple models to effectively reduce the search space for IP addresses, undermining the effectiveness of randomization defenses (Almohri et al., 2020).

Zombie Attacks: Zombie attacks involve the use of compromised computers, often referred to as "bots" or "zombies," that are controlled by an attacker to carry out malicious activities, such as Distributed Denial of Service (DDoS) attacks, against a target system. To mitigate these attacks, organizations can implement robust intrusion detection systems to identify and isolate infected machines, as well as utilize rate limiting and traffic filtering to block suspicious requests.

Sniffer Attacks: Sniffing refers to the practice of intercepting and analyzing data packets transmitted over a network, such as TCP/IP, using specialized software known as a sniffer or network protocol analyzer. This process can lead to unauthorized access to sensitive information, including passwords and personal data. To mitigate sniffing attacks, organizations should implement strong encryption protocols, such as SSL/TLS, to secure data in transit, use Virtual Private Networks (VPNs) for secure connections, and apply network segmentation to limit access to sensitive data (Prabadevi & Jeyanthi, 2018).

Wrapping Attacks: In a wrapping attack, an attacker replicates a SOAP message during its transmission and sends it to the server, posing as an authorized user. This allows the attacker to exploit cloud services by executing malicious code (Gajek et al., 2009).

CAPTCHA Breaking Attacks: which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, is a security measure designed to determine if a user is a human or a malicious program. It serves as a standard mechanism to identify and prevent automated threats, such as Trojans, worms, and botnets (Zhang et al., 2019)**.**

Table 1. Security attacks in cloud computing with their mitigation techniques

Kind of security Attacks	**Mitigation techniques and solution**
SQL Injection Attacks	- Avoid dynamic SQL to prevent injection risks. - Sanitize user input to block malicious data. - Use a proxy-based system to detect and secure user input.
Cross Site Scripting (XSS)	- Implementing Active Content Filtering. - Adopting Web Application Vulnerability Detection technologies (Gupta & Gupta, 2017) - Implementing a blueprint approach to reduce reliance on web browsers. - Configuring Secure Socket Layer (SSL) properly.
Phishing Attacks	- Detecting spam emails.
DNS Attacks	- Implementing DNS security measures, such as Domain Name System Security Extensions (DNSSEC) (Aishwarya et al., 2014)
MITM Attacks	- Correctly configuring Secure Socket Layer (SSL). - Utilizing encryption tools such as Dsniff, Ettercap, Wsniff, and Airjack.
DOS Attacks	- Implementing improved authentication and authorization methods. - Employing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (Kumar et al., 2016)
DDOS Attacks	- Adopting enhanced authentication and authorization mechanisms. - Utilizing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)(Dong et al., 2019)
Reused IP Address	Using better authentication and authorization.
Zombie Attacks	- Implementing improved authentication and authorization processes.

	- Employing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (Kumar et al., 2016)
Sniffer Attacks	- Implementing sniffer detection methods using Address Resolution Protocol (ARP). - Utilizing sniffer detection techniques based on Round-Trip Time (RTT).(Prabadevi & Jeyanthi, 2018)
Wrapping Attacks	- Implementing an effective signature mechanism. - Ensuring proper configuration of Secure Socket Layer (SSL).
Cookie Poisoning	- Adopting enhanced encryption methods. - Regularly clearing cookie data. - Leveraging the browser's security policy. - Establishing sessions and employing additional authentication methods.
CAPTCHA Breaking	- Increasing string length. - Utilizing a perturbative background. - Employing letter overlap to prevent vertical segmentation attacks. - Using different font sizes.
Hypervisor Attacks	- Implementing a secure hypervisor and effective hypervisor monitoring. - Ensuring virtual machine (VM) isolation (Dildar et al., 2017)

Source: (Altulaihan & Almaiah, 2022), (https://doi.org/10.3390/electronics11203330)

Conclusion

In conclusion, this study identifies the most effective mitigation strategies to protect cloud computing environments from security challenges and attacks. The research highlights several common security challenges, including data breaches, unauthorized access, and vulnerabilities in cloud infrastructure. These issues arise due to factors such as improper configuration, insufficient authentication mechanisms, and weak access controls. The study also outlines the most common types of security attacks, including XML Signature Wrapping, DoS attacks, and data theft, which target cloud environments. To protect against these threats, organizations can adopt best practices such as implementing robust encryption techniques, using multi-factor authentication, ensuring proper cloud configurations, and continuously monitoring cloud activities. By adopting these mitigation strategies, organizations can enhance the security and reliability of their cloud services, safeguard sensitive data, and reduce the risks associated with cloud computing.

References

A. Kofahi, N. (2018). Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey. *Advances in Networks*, *6*(1), 1. https://doi.org/10.11648/j.net.20180601.11

Abusaimeh, H. (2020). Security Attacks in Cloud Computing and Corresponding Defending Mechanisms. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 4141–4148. https://doi.org/10.30534/ijatcse/2020/243932020

Aishwarya, C., Sannidhan, M. S., & Rajendran, B. (2014). DNS Security: Need and Role in the Context of Cloud Computing. *Proceedings - 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, ICECCS 2014*, 229–232. https://doi.org/10.1109/Eco-friendly.2014.53

Almohri, H. M. J., Watson, L. T., & Evans, D. (2020). Predictability of IP Address Allocations for Cloud Computing Platforms. *IEEE Transactions on Information Forensics and Security*, *15*(c), 500–511. https://doi.org/10.1109/TIFS.2019.2924555

Alshammari, A., Alhaidari, S., Alharbi, A., & Zohdy, M. (2017). Security Threats and Challenges in Cloud Computing. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 46–51. https://doi.org/10.1109/CSCloud.2017.59

Amara, N., Zhiqui, H., & Ali, A. (2017). Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. *Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017*, *2018-Janua*, 244–251. https://doi.org/10.1109/CyberC.2017.37

Chou, T.-S. (2013). Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science and Information Technology*, *5*(3), 79–88. https://doi.org/10.5121/ijcsit.2013.5306

C.Prakash, S. Dasgupta.(2016) Cloud computing security analysis: Challenges and possible solutions. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. (2016). IEEE.

Dildar, M. S., Khan, N., Abdullah, J. Bin, & Khan, A. S. (2017). Effective way to defend the hypervisor attacks in cloud computing. *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 154–159. https://doi.org/10.1109/Anti-Cybercrime.2017.7905282

Dong, S., Abbas, K., & Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing

Environments. *IEEE Access*, *7*(c), 80813–80828. https://doi.org/10.1109/ACCESS.2019.2922196

Egerton Taylor, O., Promise Sochima, E., Emmah, V., Egerton, O., Sochima, P., & Thomas, V. (2019). Preventing Structured Query Language (SQL) Injection Attacks using PHP Data Object and Prepared Statement. *International Journal of Computer Science and Mathematical Theory E*, *5*(2), 1–9. www.iiardpub.org

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*, 223–246. https://doi.org/10.1007/s11831-021-09573-y

Gajek, S., Jensen, M., Liao, L., & Schwenk, J. (2009). Analysis of signature wrapping attacks and countermeasures. *2009 IEEE International Conference on Web Services, ICWS 2009*, 575–582. https://doi.org/10.1109/ICWS.2009.12

Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, *8*, 512–530. https://doi.org/10.1007/s13198-015-0376-0

Kumar, R., Lal, S. P., & Sharma, A. (2016). Detecting Denial of Service Attacks in the Cloud. *Proceedings - 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, DASC 2016, 2016 IEEE 14th International Conference on Pervasive Intelligence and Computing, PICom 2016, 2016 IEEE 2nd International Conference on Big Data*, 309–316. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.70

Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of Medical Internet Research*, *13*(3). https://doi.org/10.2196/jmir.1867

Lua, R., & Yow, K. C. (2011). Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network. *IEEE Network*, *25*(4), 28–33. https://doi.org/10.1109/MNET.2011.5958005

Moghaddam, F. F., Ahmadi, M., Sarvari, S., Eslami, M., & Golkar, A. (2015). Cloud computing challenges and opportunities: A survey. *2015 International Conference on Telematics and Future Generation Networks, TAFGEN 2015*, 34–38. https://doi.org/10.1109/TAFGEN.2015.7289571

Parikli, S., Dave, D., Patel, R., & Doshi, N. (2019). Security and privacy issues in cloud, fog and edge computing. *Procedia*

Computer Science, *160*, 734–739. https://doi.org/10.1016/j.procs.2019.11.018

Prabadevi, B., & Jeyanthi, N. (2018). A review on various sniffing attacks and its mitigation techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, *12*(3), 1117–1125. https://doi.org/10.11591/ijeecs.v12.i3.pp1117-1125

Ramasamy, S., & V, V. (2016). Preventing Structured Query Language (SQL) Injection Attacks in Mobile Applications. *International Journal of Control Theory and Applications*, *9(2016)*(September), 993–999.

Sabeena, S. J., & Antelin Vijila, S. (2021). A Scrutiny on Cloud Computing Security Issues. In *International Research Journal on Advanced Science Hub (IRJASH) Special Issue of First International Conference on Social Work* (Vol. 03). www.rspsciencehub.com

Sajid, M. (2013). *Cloud Computing: Issues & Challenges*.

Sasubilli, M. K., & Venkateswarlu, R. (2021). Cloud Computing Security Challenges, Threats and Vulnerabilities. *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, 476–480. https://doi.org/10.1109/ICICT50816.2021.9358709

Sattar, I., Shahid, M., & Abbas, Y. (2015). A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment. *International Journal of Computer Applications*, *115*(8), 23–27. https://doi.org/10.5120/20173-2370

Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2023). Cloud Computing with Security and Scalability. In *Cloud Computing with Security and Scalability*. https://doi.org/10.1007/978-3-031-07242-0

Surianarayanan, C., & Chelliah, P. R. (2019). *Essentials of Cloud Computing*. Springer.

T.K, S., & B, D. (2016). Security Attack Issues and Mitigation Techniques in Cloud Computing Environments. *International Journal of UbiComp*, *7*(1), 1–11. https://doi.org/10.5121/iju.2016.7101

Zatakiya, S., & Tank, P. (2013). A Review of Data Security Issues in Cloud Environment. In *International Journal of Computer Applications* (Vol. 82, Issue 17).

Zhang, Y., Gao, H., Pei, G., Luo, S., Chang, G., & Cheng, N. (2019). A survey of research on CAPTCHA designing and breaking techniques.