A Descriptive Analysis of Security Threats and Attacks in Public Cloud Computing: Safeguarding Data from Cyber Attacks.

Daniel Okari Orucho[1], Charles Katila[2], Ngaira Mandela[3]
[1, 2]Department of Computer Science and Information Technology, School of Computing and Mathematics, The Co-operative University of Kenya, Karen, Kenya
[3]Department of Computing and Informatics, School of Science and Technology, Open University of Kenya
[1]danielokari@yahoo.com
[2]ckatila@cuk.ac.ke
[3]pngaira@ouk.ac.ke

***Abstract*— Cloud computing has revolutionized how organizations and individuals store, access, and interact with data, software, and computing resources. Public cloud platforms offer scalable, cost-efficient, and globally accessible services, often characterized by managed infrastructure and multi-tenancy. However, this technological advancement faces escalating cyber threats and sophisticated attack vectors such as Denial-of-Service (DoS), Man-in-the-Middle (MITM) attacks, data breaches, and insecure APIs. These threats compromise data integrity, availability, and confidentiality. This study employs a descriptive research methodology, supplemented by desktop analysis, to examine the evolving landscape of security threats in public cloud computing. It further evaluates mitigation strategies including encryption, access control, secure API management, and continuous monitoring, while highlighting persistent research gaps that demand attention for robust cloud security frameworks.**

I. INTRODUCTION

Cloud computing offers numerous advantages, including cost efficiency, resource sharing, configurable computing power, on-demand accessibility, and exceptional scalability and flexibility [1,2]. Public cloud computing refers to a system where third-party providers deliver computing resources over the internet, accessible to individuals and organizations. As a widely adopted technology, it delivers internet-based services tailored to diverse organizational needs. The cloud model has evolved from virtualization, distributed computing, and utility computing, enabling enhanced availability and scalability for enterprise applications. It supports virtual machines provisioned from extensive physical resource pools.

In public cloud computing, services may be free or offered via subscription or pay-as-you-go models. Public clouds empower users to leverage advanced technologies, ranging from artificial intelligence and developer tools to storage and compute power, while achieving global scalability without incurring direct infrastructure costs [3]. Prominent public cloud providers include Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), Oracle Cloud, Alibaba Cloud, and IBM Cloud. Key characteristics of public clouds include on-demand scalability, multi-tenancy, cost efficiency, accessibility, and managed security [4].

These advantages have driven large organizations to migrate their IT infrastructure to cloud environments. However, ensuring data security remains a critical concern. Public cloud systems face a wide range of threats and attacks, including legal and compliance issues, malicious insiders, data breaches, mobile malware, social engineering, Denial-of-Service (DoS) attacks, Man-in-the-Middle (MITM) attacks, Cross-Site Scripting (XSS), and Structured Query Language (SQL) injection attacks [5].

The diversity and complexity of these threats pose significant challenges for cloud providers and administrators tasked with implementing effective security solutions [6]. The severity of risks varies depending on the unique security requirements of cloud users. Consequently, service providers must continuously assess and deploy protective measures to meet evolving security demands. Despite these efforts, achieving a fully secure system remains elusive [7]. Therefore, identifying and mitigating security threats in public cloud computing is essential for maintaining a secure cloud environment [6, 8,9].

This study seeks to address the following research questions:

RQ1: What are the major security threats and attacks in public cloud computing?

RQ2: What strategies are employed to mitigate these threats and attacks?

The remainder of this paper is organized as follows: Section 2 defines the problem; Section 3 outlines the methodology; Section 4 analyses security threats, Section 5 analyses Security attacks; Section 6 presents discussion; and Section 7 concludes the study.

II. PROBLEM DEFINITION

Public cloud computing delivers scalable and cost-effective solutions for individuals and organizations. However, it introduces critical security challenges, including malicious insiders, legal and compliance complexities, data breaches, data corruption, and insecure Application Programming Interfaces (APIs). Additional threats such as malware infections, social engineering, cloud misconfigurations, and multi-cloud vulnerabilities further increase the risk of unauthorized data access and exposure.

Cloud environments are also susceptible to direct attacks such as DoS, MITM, SQL injection, and XSS). These malicious activities can disrupt services, compromise sensitive data, and inflict financial and reputational damage on organizations.

To counter these risks, robust security frameworks are essential. These include encryption, granular access controls, secure API management, and continuous monitoring. This paper examines the spectrum of security threats and cyberattacks in public cloud computing, alongside mitigation strategies. It emphasizes the importance of comprehensive security policies and proactive defence mechanisms. By evaluating emerging protection techniques, organizations can enhance data security, achieve regulatory compliance, and improve system resilience, ultimately fostering a more secure cloud infrastructure.

Existing literature has addressed individual threats such as DoS and SQL injection [7,8], but few studies have examined their compounded impact in multi-cloud environments. Our research addresses this gap by analysing how overlapping vulnerabilities interact across platforms, increasing systemic risk.

III. METHODOLOGY

This study employed a descriptive research design, which is particularly effective for accurately characterizing existing phenomena. Through this approach, the researcher examined the spectrum of security threats and attacks affecting public cloud computing, while also identifying unresolved research challenges within the domain. The descriptive design allowed for a comprehensive exploration of current trends and vulnerabilities without manipulating variables, making it suitable for a study grounded in secondary data.

Data collection was conducted through desktop research, leveraging academic databases such as IEEE Xplore, SpringerLink, and ScienceDirect, alongside reputable search engines. The researcher gathered secondary information from peer-reviewed journals, technical reports, and industry publications. To ensure the quality and relevance of the sources, selection criteria included topical relevance to public cloud security, publication recency (with a focus on works from 2018 to 2024), credibility of the source, and scope of coverage. Keywords used during the search included “cloud computing threats,” “cybersecurity in public cloud,” “multi-cloud vulnerabilities,” and “cloud attack mitigation.”

For data analysis, two qualitative techniques were applied. The first was content analysis, which was used to evaluate the nature, frequency, and impact of security threats, as well as the effectiveness of various mitigation strategies. This method enabled the researcher to extract meaningful patterns and insights from the literature. The second technique was gap analysis, which helped identify limitations in current security frameworks and highlight areas requiring further research. This dual approach ensured a balanced assessment of both existing knowledge and its shortcomings.

Findings from the analysis were critically reviewed and organized into thematic categories. Initially, threats and attacks were grouped based on their origin, such as human-centric, network-based, or application-level vulnerabilities. As patterns emerged, these categories were refined to reflect commonalities in attack vectors, impact severity, and mitigation approaches. Each theme was validated through cross-referencing multiple sources to ensure consistency and relevance. This thematic organization facilitated a structured understanding of the threat landscape and corresponding defence mechanisms in public cloud environments, providing a clear foundation for future research and practical application.

IV. LITERATURE REVIEW

The literature review highlights a broad spectrum of security threats in public cloud computing, including data breaches, account hijacking, insecure APIs, and denial-of-service attacks among others, often intensified by cloud-specific challenges like multi-tenancy and limited visibility. It examines commonly proposed mitigation strategies such as encryption, identity and access management, and compliance frameworks, while identifying persistent gaps in adaptive security models, threat intelligence sharing, and standardized resilience metrics. The review draws on recent peer-reviewed and industry sources published between 2018 and 2024 to ensure relevance and depth.

V. SECURITY THREATS IN PUBLIC CLOUD COMPUTING

Cloud computing environments are increasingly targeted by a wide range of security threats and attacks due to their open, scalable, and multi-tenant nature. These vulnerabilities can compromise data confidentiality, disrupt service availability, and erode stakeholder trust. This section categorizes and analyses the most prevalent threats and attacks, along with corresponding mitigation strategies.

A. Malicious Insiders

Malicious insiders such as disgruntled employees, contractors, or administrators—pose a significant risk to cloud security. These actors may exploit privileged access to exfiltrate data, escalate permissions, or sabotage systems [10]. For instance, an insider breach at Sage led to a 4.3% drop in stock value, highlighting the financial and reputational impact of such threats. Mitigation strategies against malicious insiders include: strict access controls and least privilege policies, background checks and continuous monitoring, encryption and secure authentication, incident response protocols among others.

B. Legal and Compliance Issues

Cross-border data flows introduce complex legal and regulatory challenges. Variations in privacy laws and compliance standards across jurisdictions can lead to non-compliance and legal exposure [11]. These threats can be mitigated by instituting regulatory awareness and adherence, utilization of automated compliance frameworks such as knowledge graphs, and sector-specific compliance such as financial services.

C. Data Corruption

Data corruption refers to loss or corruption of cloud-stored information due to hardware failure, encryption key loss, or accidental deletion [12]. Without robust backup strategies, such incidents can result in irreversible damage.

Mitigation strategies include regular backups and disaster recovery planning, and secure storage, utilization of strong authentication and continuous monitoring, and immutable backups and soft delete features.

D. Data Breaches

Data breaches involve unauthorized access to sensitive information, often resulting from cyberattacks, misconfigurations, or poor security practices [13,14]. These incidents can lead to financial loss, reputational damage, and regulatory penalties. Additionally, such breaches compromise an organization's confidential information, resulting in significant reputational damage and financial losses. For instance, the 2019 Capital One data breach, which exposed over 100 million customer records, was traced to a misconfigured firewall in AWS. This incident underscores how even well-resourced organizations remain vulnerable to basic cloud misconfigurations, reinforcing the prevalence and severity of such threats [15]. Mitigation strategies against data breaches are: enforcing least privilege access and encryption, data backup and retention policies, and malware detection and incident response

E. Insecure APIs

Cloud APIs facilitate service integration but can become attack vectors if poorly designed or inadequately secured [16, 17]. They are vulnerable to bot attacks and unauthorized access. Most common mitigation strategies are: utilization of robust authentication and encryption, secure API design and input validation, and monitoring and rate limiting.

F. Malware

Malware is harmful software that is designed to undermine cloud computing security. It brings about data breaches and identifies theft and can spread through executable files or software platforms [18]. Most common propagation techniques include drive-by-downloads, backdoors, phishing, removable drives, and using other tools such as exploit kits [19,20]. Malware threats can be mitigated by using behaviour-based detection and heuristic analysis, deep learning models for zero-day threats, and endpoint protection and sandboxing.

G. Social Engineering

Social engineering exploits human vulnerabilities through deception, manipulation, and influence. Techniques include phishing, impersonation, and pretexting [21,22]. They exploit human vulnerabilities, including inadequate awareness, insufficient training, and use of unauthenticated communication channels [23]. Social engineering threats can be alleviated using employee training and awareness programs, utilization of multi-factor authentication and strict access controls and reporting culture.

H. Cloud Misconfigurations

Cloud misconfigurations in components like storage, networking, and access controls can expose systems to cyber threats. In June 2023, Japanese automaker Toyota reported that a misconfigured cloud environment led to the online exposure of approximately 260,000 customers' data. Some of the potential mitigation strategies include: implementation of robust access controls, secure storage in cloud, ensuring the functioning of logging mechanisms, periodic configurations audits, and hardening of servers and closing of the open ports [24].

I. Multi-cloud Vulnerabilities

In the year 2024, 89% of organizations were utilizing multi-cloud environments, increasing the risk of shared technology vulnerabilities. Weaknesses in common software design, web browsers, and widely used database systems can expose businesses to phishing attacks, malware infections, data breaches, and other security concerns. Mitigation strategies against multi-cloud vulnerabilities include network segmentation and proper de-militarized zone management, patch management schedule per vendor recommendations, hardening of servers and firewalls per best practices and standards, and secure architecture implementation, following security by design methodology [25].

Table I: Security Threats and Mitigation Strategies in Public Cloud Computing

Threat Type	Mitigation Strategies
Malicious insiders	Strict access controls, Encryption and secure authentication, Background checks, Continuous monitoring, Incident response plans
Legal and compliance issues	Organizations must: stay informed about applicable laws, adhere to regulations, using knowledge graph frameworks to simplify compliance processes.
Data corruption	Regular data backups, encryption of data, utilization of strong authentication mechanisms, and conducting regular security audits
Data breaches	Organization should: enforce least privilege access, enable encryption, enable 'soft delete' features, and establish data backups
Insecure APIs	Implementation of robust API authentication model, and utilization of encryption algorithms
Malware	Utilization of behaviour-based malware detection, heuristic analysis, and deep learning
Social engineering	Employee training programs, multi-factor authentication, and implementation of strict access control measures
Cloud misconfigurations	Implementation of robust access controls, secure data storage in cloud, periodic configuration audits, and closing of open ports
Multi-cloud vulnerabilities	Network segmentation, patch management, and hardening of servers and firewalls

Table I illustrates various threats in public cloud computing and provides mitigation strategies for each of the threats. Threats in public cloud computing pose several disadvantages such as downtime and service disruptions in business operations that reduce service availability, data breaches where sensitive cloud-stored data is at risk of unauthorized access, compliance with regulations can be complex due to shared responsibility in cloud computing, and limited control

in which organizations depend on cloud providers to manage security and infrastructure.

However, mitigation strategies against threats in public cloud computing offer several remedies such as enhanced security, reduced risk of data breaches [24], regulatory compliance, cost efficiency [25], improved system reliability, and better incidence response [26].

VI. SECURITY ATTACKS IN PUBLIC CLOUD COMPUTING

Security attacks are malicious activities in public cloud computing that target cloud-based systems, services, and data, and thereby posing security risks.

A. Denial of Service Attacks

This kind of cyberattack floods a network or service with an overwhelming number of data requests, causing the server to struggle with too many simultaneous connections. As a result, the host's buffer memory gets overloaded with repetitive and unnecessary data. If that buffer space runs out, the server loses its ability to establish new connections [28]. This disruption leads to users being cut off from accessing key services or resources, and in severe cases, can take down entire websites, applications, or systems.

The frequency of DoS attacks is rising due to key characteristics of cloud computing, such as on-demand services, self-service, and broad network access. These attacks specifically target the availability of cloud services by overwhelming networks, leading to reduced bandwidth, service disruptions, and restricted access for users [29]. A notable variation is Distributed DoS (DDoS) attacks, which escalate the impact by leveraging multiple compromised network hosts to intensify the assault on the target system.

B. Man-in-the-Middle Attacks

Man-in-the-Middle (MITM) attacks pose a serious risk in public cloud computing which comes in two categories: Passive and active MITM attacks. A passive MITM attack occurs when an attacker stealthily intercepts communication without altering its content. The attacker listens in, gaining access to sensitive details such as usernames, passwords, and other confidential data. Eavesdropping is a common form of passive MITM attack. On the other hand, active MITM attach occurs when an attacker deliberately intercepts and alters communication between two parties. After gaining access to the communication channel, the attacker can modify, redirect, or inject new messages. Common forms of active MITM include impersonation, spoofing attacks, and data tampering [30]. MITM attacks compromise data security and privacy, impacting services across Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) by intercepting sensitive communications and unauthorized data access.

C. SQL Injection

SQL injection is a cyberattack that takes advantage of vulnerabilities commonly found in the design of web applications. In this method, attackers embed harmful commands within standard SQL inputs, often through user entry fields. When executed, these commands manipulate the backend database in unintended ways, giving unauthorized users access to confidential data. Once the attack is successful, hackers can retrieve sensitive records, compromise database integrity, and in some cases, even rewrite or delete data altogether [31].

D. Cross-Site Scripting

These assaults occur when threat actor manages to deliver malware to unsuspecting participants via software platforms, typically through scripts that run in their browsers [31,32]. One major trigger for XSS attacks is poor validation of user-provided input. This can lead to two critical issues: the input is not correctly neutralized, or the site applies flawed validation logic. Such oversights open up security loopholes that attackers can readily exploit.

Table II: Security Attacks and Mitigation Strategies in Public Cloud Computing

Type of Attack	Mitigation Strategies
DoS	Implementation of multi-factor authentication, Utilization of stringent access controls, Deployment of DDoS protection services, Utilization of web application firewalls
MITM	Utilization of virtual private networks, Implementation of multi-factor authentication, Utilization of machine learning techniques
SQL Injection	Applying filtering techniques to sanitize user input, Usage of proxy-based architecture, Avoiding dynamically generated SQL statements in the code
XSS	Utilization of active content filtering techniques, Implementation of content-based data leakage prevention, Using web application vulnerability detection mechanisms

Table II illustrates the various types of attacks and their corresponding mitigation strategies in public cloud computing. Security attacks in public cloud computing can disrupt business operations and limit customer access due to downtime. This can cause organizations to face expenses related to incident response, recovery, and potential regulatory fines. Notably, security breaches can lead to regulatory non-compliance, potentially resulting in legal repercussions. Additionally, increased attack surface in multi-cloud setups and remote access increase exposure to cyber threats. These lead to loss of trust in cloud computing in which data security breaches erode customer and stakeholder trust in an organization's ability to safeguard information.

Mitigation strategies against security attacks in public cloud computing require a multi-layered approach with strategies such as utilization of secure encryption schemes, regular patch management, secure API management, implementation of strong identity and access management, network segmentation and firewalls, and cloud security posture management [33].

VII. DISCUSSION

Differentiating legitimate users from malicious insiders remains one of the most persistent challenges in public cloud computing [34]. These threats are particularly difficult to detect due to the insider's authorized access and

familiarity with system operations. Mitigation strategies include thorough vetting of employees, contractors, and third-party vendors before granting access, enforcing the principle of least privilege, and deploying AI-driven security tools to detect anomalous behaviour. Strong encryption, multi-factor authentication (MFA), and well-defined protocols for identifying, responding to, and recovering from insider threats are also essential [35].

Legal and compliance challenges further complicate cloud security, especially in multi-jurisdictional environments. Organizations must familiarize themselves with applicable laws and standards to ensure regulatory adherence [36]. Financial institutions, in particular, are required to uphold stringent data protection regulations to maintain consumer trust [37]. To streamline compliance, researchers have proposed frameworks leveraging automated knowledge representation systems such as knowledge graphs, which enhance regulatory processes in domains like mobile wallet transactions.

Data corruption, defined as the loss of cloud-stored data, can severely impact availability and integrity. Mitigation requires regular backups, secure storage, encryption, and disaster recovery planning to ensure resilience and compliance with security protocols [38,39]. Continuous monitoring, strong authentication, and periodic security audits further reinforce data protection [40]. Organizations should also strengthen their cloud security posture by selecting secure storage options, limiting exposure to public IPs, enforcing least privilege access, enabling object versioning and immutable backups, and understanding cloud service provider (CSP) data retention policies. Features like soft delete can protect against accidental or malicious deletions [41].

Insecure APIs, another major vulnerability, require robust authentication models and encryption to prevent unauthorized access. Cryptographic techniques such as public and private key encryption ensure that only authorized users can decrypt sensitive data [42]. Malware threats continue to evolve, rendering traditional signature-based detection insufficient against zero-day attacks. Researchers are advancing behaviour-based detection, heuristic analysis, and deep learning models to enhance malware identification and response capabilities [46,47,48].

Social engineering attacks exploit human vulnerabilities through deception and manipulation. Prevention strategies include comprehensive employee training, strict access controls, and MFA to reduce credential theft. Cultivating a security-conscious culture encourages employees to report suspicious activity without fear of repercussions [48].

Cloud misconfigurations also pose significant risks. Organizations must implement strong access controls, secure cloud storage, proper logging, configuration audits, server hardening, and port management to minimize exposure. In multi-cloud environments, vulnerabilities are amplified due to the complexity of managing diverse platforms. Mitigation strategies include network segmentation, DMZ management, scheduled patching per vendor guidelines, and secure architecture based on security-by-design principles [24].

A notable example is the 2021 Microsoft Exchange vulnerabilities, where attackers exploited shared infrastructure to access data across multiple tenants. This incident demonstrates how cloud-specific architecture can amplify the impact of security flaws, especially when visibility and isolation are limited [49].

DoS attacks disrupt service availability by overwhelming cloud resources. MFA and access controls help prevent unauthorized access, while DoS protection services detect and mitigate attacks in real time. Techniques such as Domain Name System (DNS) and Border Gateway Protocol (BGP) redirection are employed to divert malicious traffic [50,51]. Web Application Firewalls (WAFs) offer additional protection by analysing HyperText Transfer Protocol (HTTP) requests and blocking threats like SQL injection, XSS, and Cross-site Request Forgery (CSRF). These tools operate at the application layer, providing granular control and adaptive security [52].

MITM attacks compromise communication channels, allowing attackers to intercept or alter data. Mitigation involves using MFA, VPNs, secure communication tools, and properly configured Secure Socket Layer/ Transport Layer Security (SSL/TLS) certificates. Machine learning enhances detection by identifying anomalies through supervised and unsupervised learning [53]. Secure communication protocols and end-to-end encryption ensure data confidentiality during transmission.

SQL injection and XSS attacks exploit input validation flaws in web applications. Preventive measures include sanitizing user inputs, avoiding dynamic SQL statements, and employing proxy-based architectures to detect suspicious sequences [54]. Active content filtering, data leakage prevention, and vulnerability detection mechanisms help identify and neutralize threats [55]. Blueprint-based approaches reduce browser reliance and detect untrusted content, further enhancing application security [56].

Looking ahead, future research must address emerging threats posed by Generative AI. While this technology offers transformative potential, it also introduces risks such as data poisoning, prompt injection attacks, sensitive data leakage, adversarial misuse, and shadow AI deployments. These threats challenge traditional security paradigms and require innovative mitigation strategies. Research should focus on developing robust detection frameworks, ethical guidelines, and adaptive security models that can safeguard cloud environments against AI-driven threats. As public cloud computing continues to evolve, proactive and interdisciplinary research will be essential to ensure secure, resilient, and trustworthy infrastructures.

These threats challenge traditional security paradigms and require innovative mitigation strategies. Research should focus on developing robust detection frameworks, ethical guidelines, and adaptive security models that can safeguard cloud environments against AI-driven threats. As public cloud computing continues to evolve,

proactive and interdisciplinary research will be essential to ensure secure, resilient, and trustworthy infrastructures.

This research contributes to the academic discourse by offering a structured and comprehensive analysis of security threats and attacks in public cloud computing, supported by a descriptive methodology and thematic categorization. It bridges existing gaps in literature by integrating emerging threats such as multi-cloud vulnerabilities and AI-driven risks.

For industry stakeholders, the study provides actionable insights into mitigation strategies that enhance cloud resilience, regulatory compliance, and operational continuity. The findings serve as a practical guide for cloud service providers, IT administrators, and cybersecurity professionals seeking to strengthen their security posture in increasingly complex cloud environments.

VIII. CONCLUSION

The security landscape of public cloud computing continues to evolve in response to technological advancements and increasingly sophisticated cyber threats. As cloud adoption grows, so does the complexity of the threat environment, with adversaries exploiting vulnerabilities across multiple layers of cloud infrastructure and services.

This study set out to examine the evolving threat landscape, identify predominant security threats, and evaluate mitigation strategies in public cloud environments. It has identified and analysed a wide spectrum of attacks, including malware, data breaches, data corruption, legal and compliance challenges, social engineering, insecure APIs, MITM attacks, SQL injection, cloud misconfigurations, multi-cloud vulnerabilities, DoS attacks, XSS, and insider threats. Each poses distinct risks to data confidentiality, system integrity, and service availability.

Mitigation strategies typically include encryption, identity and access management (IAM), intrusion detection systems, and zero-trust models. IAM frameworks are essential for controlling user privileges and minimizing unauthorized access, while zero-trust approaches enhance security by eliminating implicit trust and requiring continuous verification of user identity and device integrity. A practical example of mitigation success is Google Cloud's implementation of the BeyondCorp zero-trust architecture [57]. By shifting access controls from the network perimeter to user identity and device posture, Google significantly reduced insider threat incidents, demonstrating the real-world effectiveness of adaptive IAM frameworks. This case illustrates how strategic deployment of identity-based controls can materially improve cloud security outcomes, especially in environments with high user mobility and distributed access points.

A multi-layered security approach, combining technical, procedural, and organizational measures, is essential for safeguarding public cloud environments. As emerging technologies such as Generative AI introduce new dimensions of risk, future research should focus on adaptive security frameworks capable of anticipating and responding to novel attack vectors. Specific areas for exploration include AI-driven anomaly detection, cross-cloud security orchestration, and regulatory models for data sovereignty. Ultimately, enhancing cloud security requires continuous collaboration between cloud service providers, regulatory bodies, and end users to ensure resilient, trustworthy, and compliant cloud infrastructures.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Dr. Charles Katila and Dr. Ngaira Mandela, for their invaluable guidance, support, and encouragement throughout the development of this manuscript. Their expert insights and thoughtful feedback were instrumental in shaping the quality and direction of this work. I am truly grateful for their mentorship and dedication.

REFERENCES

[1] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, and C. C. Chang, "Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack," IEEE Access, vol. 6, pp. 74993–75001, 2018.
[2] H. Qiu, H. Noura, M. Qiu, Z. Ming, and G. Memmi, "A user-centric data protection method for cloud storage based on invertible DWT," IEEE Trans. Cloud Comput., vol. 9, pp. 1293–1304, 2019.
[3] Google Cloud, "What is a Public Cloud?" 2025. [Online]. Available: https://cloud.google.com/learn/what-is-public-cloud
[4] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things," IEEE Trans. Ind. Inform., vol. 15, pp. 3661–3669, 2019.
[5] X. Fan, J. Yao, and N. Cao, "Research on Cloud Computing Security Problems and Protection Countermeasures," in Proc. Int. Symp. Cyberspace Safety and Security, Guangzhou, China, Dec. 1–3, 2019, pp. 542–551.
[6] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Comput. Sci. Rev., vol. 33, pp. 1–48, 2019.
[7] M. Huss, M. Waqas, A. Y. Ding, Y. Li, and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," IEEE Commun. Surv. Tutor., vol. 19, pp. 1054–1079, 2017.
[8] H. Fazal, I. Memon, T. K. Khatri, G. Muhammad, and Q. Ali, "A survey on cloud computing, security challenges, architecture, applications & solutions," Univ. Sindh J. Inf. Commun. Technol., vol. 4, pp. 24–30, 2020.
[9] S. Tu et al., "Reinforcement Learning Assisted Impersonation Attack Detection in Device-to-Device Communications," IEEE Trans. Veh. Technol., vol. 70, pp. 1474–1479, 2021.
[10] Comparethecloud, "8 Public Cloud Security Threats," 2018. [Online]. Available: https://www.comparethecloud.net/articles/8-public-cloud-security-threats-to-enterprises-in-2017/
[11] T. Islam, D. Manivannan, and S. Zeadally, "A classification and characterization of security threats in cloud computing," Int. J. Next Gener. Comput., vol. 7, no. 1, pp. 1071–1081, 2016.
[12] S. Gupta, G. Shankar, and A. Gupta, "Cloud Computing: Services, Deployment Models and Security Challenges," in Proc. 2nd Int. Conf. Smart Electronics and Communication (ICOSEC), 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9591794
[13] CSOonline, "Top Cloud Security Threats," 2018. [Online]. Available: https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html
[14] B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," Procedia Comput. Sci., vol. 92, pp. 128–135, 2016.
[15] Cloud Security Alliance, "A technical analysis of the Capital One cloud misconfiguration breach," *CSA Blog*, Aug. 2019. [Online]. Available: https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach/
[16] M. Bettendorf, "API growth continues to skyrocket in 2020 and into 2021," 2021. [Online]. Available: https://blog.postman.com/api-growth-rate/
[17] Salt Labs, "Salt State of API Security Report Q1 2023," 2023. [Online]. Available: https://content.salt.security/state-api-report.html
[18] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," ACM Comput. Surv., vol. 50, no. 3, pp. 1–40, 2018.

[19] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, "A comprehensive survey for IoT security datasets taxonomy, classification and machine learning mechanisms," Comput. Secur., vol. 132, 2023. doi: 10.1016/j.cose.2023.103283.
[20] L. Caviglione et al., "Tight arms race: Overview of current malware threats and trends in their detection," IEEE Access, vol. 9, pp. 5371–5396, 2021.
[21] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples," Springer Open, pp. 1–21, 2021.
[22] A. Samad, "Social Engineering in Cybersecurity. Prevention and Mitigation Strategies," EasyChair Preprint, 2024. [Online]. Available: https://easychair.org/publication/preprint/wL93
[23] R. Alavi, S. Islam, and H. Mouratidis, "A conceptual framework to analyse human factors of information security management system (ISMS)," in Human Aspects of Information Security, Privacy, and Trust, vol. 8533, Lecture Notes in Computer Science, Springer, pp. 297–305, 2014.
[24] R. Ramachandran, "Evolving Threats to Cloud Computing Infrastructure and Suggested Countermeasures," ISACA, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/evolving-threats-to-cloud-computing-infrastructure-and-suggested-countermeasures
[25] Cyber Security News, "10 Cloud Security Mitigation Strategies," 2025. [Online]. Available: https://cybersecuritynews.com/cloud-security-mitigation-strategies
[26] Educative, "Top 11 Strategies to Mitigate Cloud Security Threats," 2024. [Online]. Available: https://www.educative.io/blog/mitigate-cloud-security-threats
[27] exabeam, "Cloud Security Threats: Top Threats and 3 Mitigation Strategies," 2025. [Online]. Available: https://www.exabeam.com/explainer/cloud-security/cloud-security-threats-top-threats-and-3-mitigation-strategies/
[28] M. Kaur and A. B. Kaimal, "Analysis of Cloud Computing Security Challenges and Threats for Resolving Data Breach Issues," in Proc. Int. Conf. Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1–6, 2023. doi: 10.1109/ICCCI56745.2023.10128329.
[29] V. D. Soni, "IoT connected with e-learning," Int. J. Integr. Educ., vol. 2, no. 5, pp. 273–277, 2019.
[30] R. Petrović et al., "Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform," in Proc. 15th Int. Conf. Advanced Technologies, Systems and Services in Telecommunications, Nis, Serbia, pp. 307–310, 2021. doi: 10.1109/TELSIKS52058.2021.9606392.
[31] R. Bhadauria and S. Sanyal, "Survey on security issues in cloud computing and associated mitigation techniques," Int. J. Comput. Appl., vol. 47, no. 18, pp. 47–66, 2012.
[32] I. Hydara et al., "Current state of research on cross-site scripting (XSS): A systematic literature review," Inf. Softw. Technol., vol. 58, pp. 170–186, 2015.
[33] Cybersecurity Insiders, "Top 10 Cloud Security Mitigation Tactics," 2025. [Online]. Available: https://www.cybersecurity-insiders.com/top-10-cloud-security-mitigation-tactics/
[34] M. Dawood et al., "Cyberattacks and Security of Cloud Computing: A Complete Guideline," Symmetry, vol. 15, p. 1981, 2023. doi: 10.3390/sym15111981
[35] Aristium, "Insider Threat Management in Public Cloud: Strategies and Best Practices," 2024. [Online]
[36] D. Y. Kim and K. P. Joshi, "A Semantically Rich Knowledge Graph to Automate HIPAA Regulations for Cloud Health Services," in Proc. 7th IEEE Int. Conf. High Performance and Smart Computing and IEEE Int. Conf. Intelligent Data Security, May 2021, pp. 7–12.
[37] I. Nagar, E. Elluri, and K. P. Joshi, "Automated Compliance of Mobile Wallet Payment for Cloud Services," in Proc. 7th Int. Conf. Big Data Security on Cloud, IEEE Int. Conf. High Performance and Smart Computing and IEEE Int. Conf. Intelligent Data Security, 2021, pp. 38–45.
[38] S. H. Alrasheed, M. Aied alhariri, S. A. Adubaykhi, and S. El Khediri, "Cloud Computing Security and Challenges: Issues, Threats, and Solutions," in Proc. 5th Conf. Cloud and Internet of Things (CIoT), Marrakech, Morocco, 2022, pp. 166–172. doi: 10.1109/CIoT53061.2022.9766571.
[39] Eshare.ai, "5 Essential Steps for Mitigating Security Threats in Cloud Computing," 2025. [Online]. Available: https://blog.eshare.ai/5-essential-steps-for-mitigating-security-threats-in-cloud-computing
[40] SecurDi, "Data Security in the Cloud: Risks and Mitigation Strategies," 2025. [Online]. Available: https://securdi.com/cloud-security/data-security-in-the-cloud-risks-and-mitigation-strategies/
[41] National Security Agency, "NSA's Top Ten Cloud Security Mitigation Strategies," 2024. [Online]. Available: https://media.defense.gov/2024/mar/07/2003407860/-1/-1/0/csi-CloudTop10-Mitigation-Strategies.PDF
[42] L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," in Proc. 3rd Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Palladam, India, 2019, pp. 376–380. doi: 10.1109/I-SMAC47947.2019.9032545.
[43] P. Mishra, I. Verma, S. Gupta, V. S. Rana, and K. Kadarla, "vProVal: Introspection based process validation for detecting malware in KVM-based cloud environment," in Proc. 4th Int. Conf. Fog and Mobile Edge Computing (FMEC), Rome, Italy, 2019, pp. 271–277. doi: 10.1109/FMEC.2019.8795365.
[44] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical propagation model of malware for cloud computing security," IEEE Access, vo. 8, pp. 20325–20333, 2020. doi: 10.1109/ACCESS.2020.2968916.
[45] H. M. Al-Khafaji, E. S. Alomari, and H. S. Majdi, "Review of analytics tools on traffic for IoT and cloud-based network environment," in Proc. 3rd Int. Conf. Engineering Technology and its Applications (IICETA), Najaf, Iraq, 2020, pp. 73–77. doi: 10.1109/IICETA50496.2020.9318914.
[46] P. Mishra et al., "VMShield: Memory introspection-based malware detection to secure cloud-based services against stealthy attacks," IEEE Trans. Ind. Inform., vol. 17, no. 10, pp. 6754–6764, 2021.
[47] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," ACM Comput. Surv., vol. 50, no. 3, pp. 1–40, 2018.
[48] T. Ergen, S. O. Sahin, and S. S. Kozat, "Recurrent neural networks based online learning algorithms for distributed systems," in Proc. 26th Signal Processing and Communications Applications Conf., Izmir, Turkey, 2018, pp. 1–4. doi: 10.1109/SIU.2018.8404806.
[49] Pitney, A. M., Penrod, S. W., Foraker, M., & Bhunia, S. (2022). *A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities*. Miami University, Department of Computer Science and Software Engineering. Retrieved from sbhunia.me/publications/manuscripts/split22microsoft.pdf
[50] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor authentication framework for cloud computing," in Proc. 5th Int. Conf. Computational Intelligence, Modelling and Simulation, 2013, pp. 105–110.
[51] M. Jonker and A. Pras, "DDoS Mitigation: A Measurement-based Approach," in Proc. Network Operations and Management Symposium, IEEE, 2020. [Online]. Available: https://ris.utwente.nl/ws/portal/237704486/jonker2020ddos.pdf
[52] D. R. Chittibala, "Web Application Firewalls. Integration in DevOps Practices," J. Artif. Intell. Cloud Comput., vol. 1, p. 210, 2022. doi: 10.47363/JAICC/2022
[53] R. Zagrouba and R. Alhajri, "Machine Learning based Attacks Detection and Countermeasures in IoT," Int. J. Commun. Netw. Inf. Secur., vol. 13, pp. 158–167, 2021. doi: 10.17762/ijcnis.v13i2.4943.
[54] A. Liu, Y. Yuan, and A. Stavrou, "SQLProb: A Proxy-based Architecture towards Preventing SQL Injection Attacks," in Proc. ACM Symp. Appl. Comput. (SAC), Honolulu, HI, USA, Mar. 2009.
[55] D. Gollmann, "Securing Web Applications," Inf. Secur. Tech. Rep., vol. 13, no. 1, pp. 1–8, 2008. doi: 10.1016/j.istr.2008.02.002.
[56] T. M. Lou and V. N. Venkatakrishnan, "BluePrint: Robust Prevention of Cross-Site Scripting Attacks for Existing Browsers," in Proc. 30th IEEE Symp. Security and Privacy, May 2009, pp. 331–346. doi: 10.1109/SP.2009.33.
[57] [50] S. Barker, "Implementing Zero Trust Security in the Cloud Era with BeyondCorp Enterprise," *ExpertBeacon*, Sep. 2024. [Online]. Available: https://expertbeacon.com/implementing-zero-trust-security-in-the-cloud-era-with-beyondcorp-enterprise/

Call for Papers: International Journal of Computer Science and Information Security (IJCSIS)

Scope and Topics: The International Journal of Computer Science and Information Security (IJCSIS) invites researchers, practitioners, and academicians to submit original, unpublished contributions covering a wide range of topics in the field of computer science and information security. We welcome submissions that include but are not limited to:

- Computer and Network Security
- Cryptography and Data Security
- Information Assurance
- Artificial Intelligence and Machine Learning in Security
- Cybersecurity Policies and Standards
- Security in Cloud Computing
- Internet of Things (IoT) Security
- Blockchain and Distributed Ledger Technologies
- Secure Software Development
- Privacy-Enhancing Technologies

Submission Guidelines:

- Manuscripts must be original and not currently under consideration for publication elsewhere. All papers should be submitted in English.
- The manuscript should follow the IJCSIS formatting guidelines, available on our website: https://sites.google.com/site/ijcsis/ijcsis
- Submissions must include the title of the paper, abstract, keywords, and full contact information for all authors.
- Papers should be submitted via our submission system here: https://sites.google.com/site/ijcsis/submit-paper

Important Dates:

- **Paper Submission Deadline:** Monthly, 2025
- **Notification of Acceptance:** Within TWO weeks, 2025
- **Final Manuscript Due:** Monthly, 2025
- **Publication Date:** Monthly Issue

Review Process: All submitted papers will undergo a rigorous peer-review process by the IJCSIS editorial board and selected external reviewers. Authors will be notified of the review results by the notification of acceptance date.a

Contact Information: For further inquiries, please contact the editorial office at:

Email: ijcsiseditor@gmail.com

We look forward to receiving your submissions!

Website: https://sites.google.com/site/ijcsis/ijcsis

Call for Papers – May-June/July-August/September-October 2025 Issue
International Journal of Computer Science and Information Security (IJCSIS)

ISSN: 1947-5500 | Impact Factor: 1.38

The **International Journal of Computer Science and Information Security (IJCSIS)** has received a total of **27,959 citations** as of March 2025. [Google Scholar]
Website: **https://sites.google.com/site/ijcsis/**

The **International Journal of Computer Science and Information Security (IJCSIS)** invites high-quality research papers for its **Monthly 2025** issue. IJCSIS is a **peer-reviewed, open-access journal** that publishes original research articles, review papers, and technical studies in the fields of **computer science, cybersecurity, artificial intelligence, information security, data science, and emerging technologies**.

Topics of Interest:

We welcome submissions in (but not limited to) the following areas:

- **Cybersecurity & Information Security**
- **Artificial Intelligence & Machine Learning**
- **Data Science & Big Data Analytics**
- **Computer Networks & Cloud Computing**
- **Blockchain & Cryptography**
- **Internet of Things (IoT) & Edge Computing**
- **Software Engineering & Software Security**
- **Digital Forensics & Cyber Threat Intelligence**
- **Human-Computer Interaction & Usability**
- **Computational Intelligence & Algorithms**

Important Dates:

- **Manuscript Submission Deadline:** Monthly, 2025
- **Acceptance Notification:** Within 2 weeks, 2025
- **Publication Date:** End of Month, 2025

Submission Guidelines:

Authors are requested to submit their manuscripts via the **IJCSIS online submission system** or email at **ijcsiseditor@gmail.com**. The paper should be formatted according to **IJCSIS template guidelines** and must not have been previously published or under consideration elsewhere.

Review Process:

All submitted manuscripts undergo a **double-blind peer-review process** to ensure high academic quality. Authors will receive constructive feedback from **expert reviewers**.

Why Publish with IJCSIS?

- **Indexed in major databases** such as Google Scholar, ResearchGate, and more.
- **High visibility** with open-access publication.
- **Fast peer-review and publication process.**
- **DOI and indexing services** for all published papers.

Contact Information:

For any inquiries, please contact the editorial team at **[ijcsiseditor@gmail.com]** or visit our website at **[** **https://independent.academia.edu/JournalofComputerScienceIJCSIS** **]**.

We look forward to your submissions!
IJCSIS Editorial Board

https://sites.google.com/site/ijcsis/ijcsis/editorial-board