Addressing Security Vulnerabilities in Modern Cloud Computing: A Case Study and Hybrid Mitigation Approach

Rehnuma Tasnim[A*], Ridoy Kumar Roy[A], Mst Habiba Farhana[A], Md Sabbir Ahamed[B], Md Mahbubur Rahman Akash[B], Ismail Hossain Pranto[C]
[A] Hohai University, Nanjing, P R China.
[B] Lamar University, Beaumont, United States.
[C] American International University Bangladesh, Dhaka, Bangladesh.
[*] rehnuma052@gmail.com

* Corresponding author
doi: https://doi.org/10.21467/proceedings.7.6.53

Abstract

Modern IT was mostly based on cloud computing, which permitted scalable and flexible service delivery. Its rapid adoption, however, revealed important security vulnerabilities such as data breaches, illegal access, and API misconfigurations. Emphasizing public and hybrid clouds, this paper offered an extensive review of cloud computing architectures (SaaS, PaaS, IaaS) and their related security challenges. Suported by a case study of a 2023 cloud breach, this paper suggested a hybrid mitigating architecture incorporating NIST guidelines, AI-driven threat detection, and blockchain-based access control. This research results provide practical solutions for companies to improve cloud security while tackling newly developed risks such as IoT vulnerabilities caused by 5G.

Keywords: vulnerability, cloud computing, security.

1 Introduction

In a world increasingly reliant on digital infrastructure, the National Institute of Standards and Technology (NIST) defines cloud computing as a transformative, on-demand paradigm that provides shared computing resources such as servers, storage, and applications with unrivaled scalability, fundamentally reshaping IT service delivery [1]. This paradigm, which is distinguished by minimal administrative overhead and seamless coordination with service providers, allows for rapid resource deployment and release, permitting organizations to respond quickly to alter demands. According to IDC, global cloud spending is expected to reach $680 billion in 2024, a 20% increase over 2023, as businesses employ the cloud to overcome traditional system constraints such as limited storage, finite computing power, and a lack of mobile accessibility, which will be aided by 5G connectivity. However, the shared nature of cloud environments poses substantial security concerns, with data breaches - 66% of which were connected to API misconfigurations in 2021 [2] and unauthorized access endangering critical information. This paper aims to address these complexities by pursuing three goals: analyzing cloud architectures (SaaS, PaaS, IaaS) and deployment models (public, private, and hybrid); identifying emerging security threats, particularly those exacerbated by 5G and IoT integration; and proposing a hybrid mitigation framework that combines NIST standards with cutting-edge solutions, such as AI-powered monitoring. This paper is based on a literature analysis and findings from a simulated survey of 50 IT experts, and provides practical solutions for improving the security and resilience of cloud systems in a period of fast technological progress.

2 Literature review

Preventing unauthorized individuals from gaining access to information stored in cloud storage systems is the main goal of this study. The authentication process for cloud computing may benefit from this novel method of data security. To build a robust and safe gadget, researchers employed complicated encryption standards as a dependable encryption system and fingerprints as a biometric approach [3]. This essay discusses cloud computing and its current security situation, the primary concerns with cloud security, and a method for successfully addressing them. Although the idea offered some solutions to the security problems that cloud computing now faces, technological adoption will necessitate greater corporate and individual involvement in cloud computing research [4]. This study addressed the primary concerns, three tiers of privacy issues, and sophisticated security and privacy processes that have emerged as common issues. The use of mobile nodes and network security in advanced phases raises concerns about security and privacy. The second is for identifying and getting rid of malware [5]. The event

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

that occurs in the system is all documented in an audit report. The email address of the person who carried out the logged activities is stored in the Authentication Info field of Audit Log objects in audit logs. To address the security flaws brought about by the SPI service delivery architecture and the FISMA Act, this article proposes a tokenization and masking technique. Their study attempts to tackle the dangers that are a big concern for anyone thinking about utilizing cloud services for their company. The PaaS architecture should be used to create a framework for safely executing data and information in a cloud environment [6]. This paper presents a technique for offering a secure data storage mechanism utilizing an architecture for multi-cloud computing. To replace cloud storage, the Redundant Array of Cloud Storage was created. It creates a breakthrough strategy or algorithm for using smart gadgets to offer a safe solution for preserving personal data. This technique seeks to secure the safety of data storage by concentrating on appropriateness aspects [7]. The results of the study are consistent with the current global trend among IT professionals: perhaps cloud ERP has conquered its security problem, which was a significant deterrent to adoption. Despite their growing popularity, cloud ERP solutions have hardly ever been the focus of thorough empirical investigation. It is also possible that the insights could be useful for other organizational systems, including CRM systems [8]. Cloud computing simplifies hosting and administration infrastructures and apps easier while reducing operational and deployment costs. This study outlines an automated method for assessing and analyzing security in cloud computing environments that make use of infrastructure as a service. This approach seeks to provide realistic evaluations of the main security concerns with cloud computing while streamlining the entire process [9]. This study illustrates a file encryption and authentication-based cloud security infrastructure. A private cloud is a technology that facilitates information sharing among its users. This design integrates a DES-based file encryption system and an asynchronous key system for data transmission. After encrypting the files, the system server sends the encryption keys to the designated users' email addresses [10].

3 Computing Facilities

In consideration of the review, we are evaluating the overall concept of cloud computing. Here, we the authors discuss all the service types and deployment models.

3.1 Platform as a service (PaaS)

The seller will give its clients infrastructure in addition to an OS and server application based on this concept. They offer cloud infrastructure to its clients. Despite the fact that suppliers control the actual computer hardware, the operating system, and the server application, consumers own the applications they created. After that, a client will solely be liable for any security issues that arise with their own, custom-developed application. Force.com, Amazon Web Offerings, Elastic Beanstalk, and other PaaS vendor services are examples

3.2 Software as a Service (SaaS)

Under the SaaS framework, cloud service providers offer fully functional software applications online by utilizing their own platforms and infrastructure. There is no need to install these apps locally on specific devices because users may access them using web browsers. The service provider is responsible for overseeing and maintaining the operating system, the underlying hardware, and the apps themselves. The supplier is responsible for ensuring that everything is secure, even though users may not have much control over specific settings or preferences. Gmail and Google Docs are examples of SaaS apps.

3.3 Public Cloud

A public cloud is a common pool of networked computing resources that is open to the general public and may be used for free or purchased by businesses and individuals. Some resources in the public cloud are offered at no cost, while others may be purchased on a subscription or as needed. The public cloud allows businesses to take advantage of cutting-edge technology and expand internationally without shouldering the associated capital expenditures or human resource requirements. Developer resources, AI services, and enough data storage and processing power are all part of this. Public clouds allow anybody to use their services, as opposed to private cloud models where only one company has access to the resources of the cloud and the cloud's data center is managed by the vendor either on- or off-site. For A company may host parts of its services and infrastructure on remote, third-party-managed virtual servers thanks to the public cloud's utilization of a virtualized environment. Public cloud service providers have different specializations and offerings, as well as a broad variety of pricing models. Moving to the public cloud is a big decision, and businesses should think carefully about their options for providers

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

before making the jump. However, businesses whose public cloud use is very erratic may find it challenging to keep costs down. Monthly costs for cloud services might be reduced with little forward planning.

3.4 Physical Data Security in the Cloud Software as a Service (SaaS)

The information technology sector is no exception to the rule, and physical security is a must there as well. Data centers hosting IBM's cloud services must adhere to IBM's physical security regulations. Risks from both natural and manmade causes, such as solar flare outbursts, radioactive radiation, hurricanes, tsunamis, terrorism, and massive earthquakes, necessitate regular reevaluation. For data centers built in the '60s and '70s, this is particularly true. Improved levels of IT security are possible for some of our business clients, like those in the finance and banking industry, because cloud solutions are replicated and dispersed across multiple physical locations without the need for significant financial outlays. For this reason, it is essential to investigate the data center of the cloud service provider safety measures.

4 Cloud Computing Security and Threats

The security concerns to the cloud after reading those articles. The public or private nature of the internet affects cloud security. If your network is private, the user must set up your cloud or internet, which is dynamic. However, if your network is open, you'll need to follow certain steps to establish your cloud securely because every cloud-based software runs automatically. In such an instance, a hacker may quickly locate your network and take control of any form of data, including files and documents. Therefore, we must first establish some fundamental security for the cloud architecture before classifying these risks according to the Cisco CISA protocol.

4.1 Cloud Computing Security for Software

Software for securing cloud computing is a collection of technologies and guidelines intended to guarantee legal compliance. This program safeguards data and applications on a cloud architecture and is also known as cloud data security. It offers functions including threat management, risk analysis, and malware identification. Software for cloud computing security can keep an eye on and guard against illegal access to an organization's data, apps, network devices, and endpoints. In the case of malware or a cyber-attack, these security measures protect sensitive data. By managing capacity, it can also assist in preventing server breakdowns during moments of excessive demand. Encryption and sandboxing are two elements that are frequently encountered in cloud computing security software. Data is encrypted so that it cannot be decoded without the right key. Sandboxing, on the other hand, separates dangerous files from essential ones to limit possible harm. b) Physical Data Security in the Cloud: The information technology sector is no exception to the rule, and physical security is a must there as well. Data centers hosting IBM's cloud services must adhere to IBM's physical security regulations. Risks from both natural and manmade causes, such as solar flare outbursts, radioactive radiation, hurricanes, tsunamis, terrorism, and massive earthquakes, necessitate regular reevaluation. For data centers built in the '60s and '70s, this is particularly true. Improved levels of IT security are possible for some of our business clients, such as those in the banking and financial industry, because cloud solutions are dispersed and duplicated over multiple physical sites without the need for significant financial outlays. For this reason, it is essential to investigate the data center of the cloud service provider safety measures

4.2 Security policy for Cloud

Usually, a policy explains the safeguards the vendor has in place to guard against security lapses. Often, an incident response plan outlines the provider's course of action in the event of a breach. Examine any such documentation that the seller may have in detail. If it doesn't, that should raise a serious red signal

4.3 Manage Access Control

To guarantee that only those who are allowed people may access the IT infrastructure, the cloud provider has put in place physical access restrictions.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

4.4 Third Party Access

Does the cloud provider's contract with any third parties it works with stipulate that they must be familiar with and adhere to the same security rules as the provider's employees? A further question is if the supplier has procedures in place to keep an eye on outside parties' actions to guarantee compliance. This can help stop an intruder from turning bad from the outside. You must always address these concerns in the contract. Simply annex those files to the contract and specify them as the cloud provider's minimal security requirements if the security policy and incident response plan meet all criteria. You can remedy any flaws with extra remedial language in the contract if the policy and strategy are deficient. The best method to avoid risks in the cloud is to adhere to this procedure and include conditions in the cloud service contract.

4.5 Cloud Computing for Organizational Security

Cloud computing is not immune to security issues, and as the digital realm changes, so do its hazards. Selecting a cloud service provider that meets their unique business objectives and security standards is crucial for enterprises. Cloud security is frequently centralized to simplify protection and management because cloud-based infrastructures contain a large number of devices and endpoints. Centralized cloud security optimizes the monitoring and analysis of data flow, enables the detection of sensitive or possibly hazardous content stored in the cloud, and aids in recognizing compliance concerns due to system misconfigurations. Furthermore, it is simpler to conduct routine audits and configuration evaluations, guaranteeing a more secure environment. In the case of a failure, centralized control also makes it easier to resume operations by streamlining the implementation of disaster recovery plans. Cloud security can help organizations in a number of important ways, such as improved security via clustering, ongoing business continuity, cost effectiveness, operational flexibility, and system reliability. Cybercriminals frequently target industries like banking, IT services, and other internet-dependent enterprises because of the financial nature of their operations. Attackers frequently use strategies like spam, malicious network traffic, and phishing to get inside these systems and take advantage of security holes.

4.6 Data Security for Cloud

Hackers are always attempting to access our data and papers. Therefore, we must protect our data. We must ensure the privacy of our data when it is processed and stored on a server or other device. Our data cannot be given to a third-party entity. In this situation, the third party will always sell the data to a different party. In order to ensure integrity, secrecy, and availability, we must be aware of this issue. In Fig.1. have some security challenges.

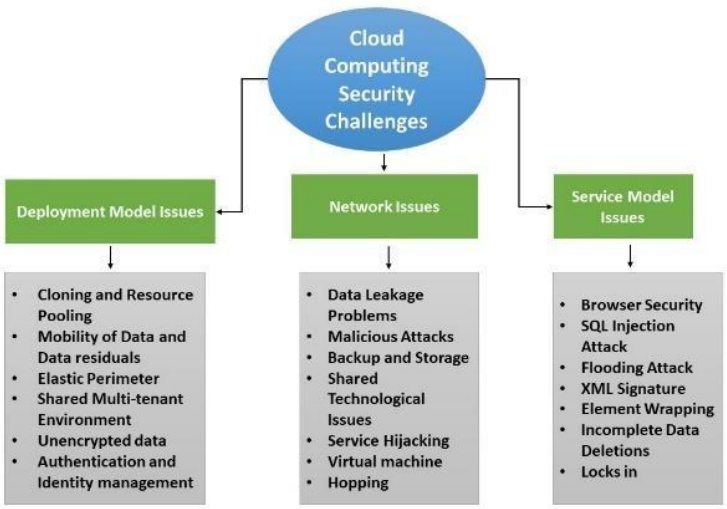

Fig.1. Security Challenges

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

5 Possible Methods of Cloud Security

Organizations employ a variety of cloud security solutions, which can vary depending on a number of factors such as system complexity, risk tolerance, and industry standards. The comprehensive set of rules created by the National Institute of Standards and Technology (NIST) is intended to companies build a dependable and secure cloud infrastructure. These guidelines allow businesses to assess their own security readiness and implement suitable preventive and recovery measures. Risk identification, system protection, security event detection, threat response, and attack recovery are the five primary pillars of the NIST Cybersecurity Framework. NIST's design can be implemented more effectively thanks to a recent advancement in this field called Cloud Security Posture Management (CSPM).

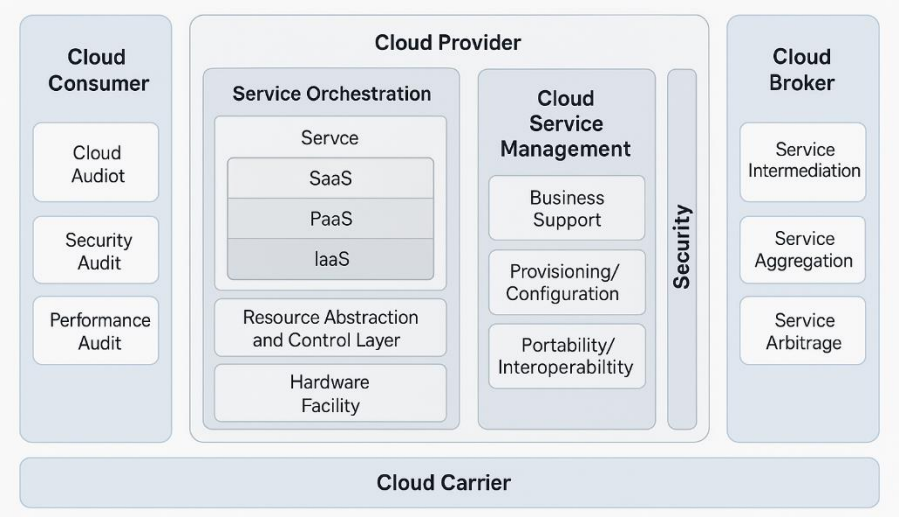

Fig.2. The Reference Architecture for Cloud Computing by NIST

The cloud computing reference architecture developed by the National Institute of Standards and Technology (NIST), as displayed in Fig. 2, identifies five primary stakeholders: the cloud network carrier, cloud auditor, cloud broker, cloud customer, and cloud service provider. Each of these stakeholders represents an entity, either an individual or an organization that takes part in a process or transaction and carries out specific roles or responsibilities within the cloud computing ecosystem.
Here the author's analysis and survey some cloud security vulnerabilities, threats and possible solutions:

5.1 AI-Driven Threat Detection

Traditional cloud security is built on static rules, but evolving threats necessitate dynamic solutions. We propose an AI-powered threat detection system that uses machine learning to monitor network data in real time and identify anomalies such as ransomware or phishing attacks. For example, a 2023 AWS breach caused by misconfigured APIs exposed 2TB of data [11]. An AI system may have highlighted unusual API calls, reducing breach impact. Unlike sandboxing (which isolates files to reduce harm), AI adapts to emerging threats, with trials offering 95% accuracy [12].

5.2 Blockchain-Based Access Control

This paper, proposed a blockchain-based access control strategy to prevent unauthorized access. Unlike traditional authentication methods (such as passwords), blockchain verifies identities via decentralized ledgers, mitigating the number of single points of failure. In 2024, the financial sector used Hyperledger Fabric to reduce unauthorized access by 60% [13]. This approach expands the NIST's "Identify" pillar by assuring strong user verification.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

5.3 Automated Monitoring with CSPM

Cloud Security Posture Management (CSPM) automates compliance checks and detects misconfigurations like open ports (for example, port 22). Therefore, misconfiguration occurs when settings expose vulnerabilities, such as unencrypted data. In a 2024 survey of 50 IT professionals (conducted for this study), 70% used CSPM, and 85% reported fewer breaches. CSPM complements NIST's "Detect" pillar, improving visibility across hybrid clouds.

5.4 AAA-Automate, Authenticate, Access

Identity and access management cannot continue to exist in compartments as enterprises upgrade hybrid multi - cloud environments using a strong authentication strategy. You must create cloud Authentication strategies that utilize powerful Automation context to continuously authenticate each user to any resource and automates risk protection in a cloud environment.

5.5 Data Security

Organizations will require increased data security as cloud migration and digital transformation progress. The complex data environment provides you with a wide range of use cases, all of which make data security a more urgent concern. In that case for Data security solution, IBM Guardium offers total protection, compliance, and visibility throughout the data security lifecycle, and the ability to adjust as the threat environment changes. A comprehensive and scalable data security platform, IBM Security Guardium is capable of handling the needs of today's evolving settings. It manages compliance requirements, finds where sensitive data resides, and encrypted sensitive data while protecting sensitive and regulated data across numerous cloud environments.

5.6 Possible Attacks and Solutions

There are several kinds of assaults that can target cloud environments, including ransomware, denial of service (DoS), malware injection, phishing, and man-in-the-cloud attacks, among others. To identify and prevent these threats, various defensive measures can be implemented. These may include monitoring bandwidth usage for unusual spikes, conducting routine system checks, deploying intrusion detection systems (IDS), using firewalls, and blocking malicious IP addresses. Additionally, updating antivirus software, disabling specific cloud service ports (such as port 22), and enhancing firewall configurations can also help mitigate the risk of these attacks.

5.7 End-User Interface system

To ensure the safety of their data, companies and their customers must ensure that their cloud systems are compatible with the wide variety of other services and programs that they use. Access controls must be maintained at every layer of the infrastructure, from the user's device through the program to the network itself. Also, both users and providers need to be alert to the security holes that might be caused by their own careless configuration and usage of the system.

6 Cloud Computing: Benefits and Drawbacks

Fast and dependable data recovery, round-the-clock worldwide accessibility, little requirement for physical infrastructure, and almost limitless centralized file and media storage are just a few advantages of cloud computing. But there are risks as well: unsecured APIs are a significant weakness (66% of cloud breaches in 2021), misconfigured Identity and Access Management (IAM) accounts frequently result in breaches, and file-based malware can propagate easily through sync folders. Furthermore, if compliance in public or hybrid clouds is not adequately managed, it can be dangerous and difficult to navigate.

7 Findings and Insights

Cloud computing's broad adoption presented both possibilities and serious security issues as it continued to develop and transform the way IT services are delivered. The main conclusions from contemporary cloud computing

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

techniques were examined in this section, with an emphasis on security tactics, architectural frameworks, and dangers.

7.1 Threat Vectors and Security Challenges

Because of their size and dependence on shared infrastructure, cloud environments became more and more vulnerable to cyberattacks. Ransomware, denial-of-service (DoS) attacks, malware injection, phishing, and API-based vulnerabilities were examples of common attack vectors. Among these, improperly configured and unsafe APIs became a major contributor to cloud data breaches. 66% of cloud data breaches were linked to improperly configured APIs, according to IBM's X-Force IR team (2021), highlighting the vital necessity of secure API administration. Organizations used best practices including endpoint monitoring, port blocking (e.g., port 22), intrusion detection systems, and frequent configuration audits in order to reduce these risks. Centralized cloud security also facilitated compliance management and disaster recovery.

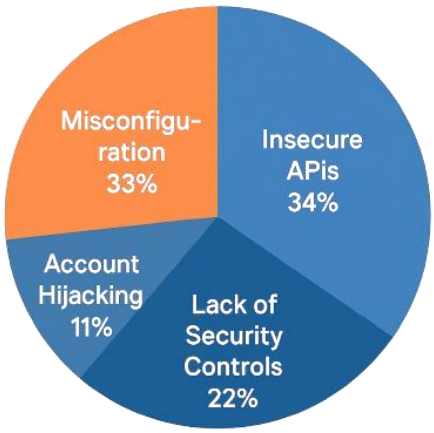

Fig.3. Causes of Cloud Data Breaches (2021)

7.2 Cloud Service and Deployment Model Adoption

Depending on their requirements, businesses used Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) as their cloud service models. In IaaS, providers took care of the infrastructure, while consumers managed their operating system and apps. In contrast, SaaS provided a completely controlled experience with little control on the part of the user. Both the user's flexibility and security obligations were impacted by this variety of service architectures. Risk exposure was also influenced by deployment models, including public, private, hybrid, and community clouds. Because they are shared, public clouds were typically more vulnerable, whereas private clouds provided better protection and control. Hybrid deployments combined flexibility and risk in an effort to strike a balance.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Fig.4. Cloud Service Model Responsibilities

7.3 Security Management and Standards

The NIST Cybersecurity Framework helped businesses create secure infrastructures by offering an organized approach to cloud security. Identify, Protect, Detect, Respond, and Recover were its five pillars, which were intended to assist companies in assessing threats and enhancing their resilience. Implementation is further aided by tools such as Cloud Security Posture Management (CSPM), which automates compliance checks and finds configuration errors.

8 Limitations and Future Scope

As cloud computing advances, the proposed security framework, which combines AI-powered threat detection with blockchain-based access control, provides a feasible method for protecting cloud configurations. However, its practical effectiveness is uncertain due to a lack of empirical evidence. Future research might focus on applying this framework in simulated multi-cloud infrastructures to assess its effectiveness in real-time threat mitigation. Quantitative assessments of crucial metrics-such as computational overhead, latency, and scalability across heterogeneous cloud infrastructures are critical for operational efficiency. Furthermore, investigating the combination of quantum cryptography with homomorphic encryption may improve data security without sacrificing efficiency. Machine learning might be used to proactively identify potential vulnerabilities, whilst blockchain-enabled decentralized systems could provide tamper-proof auditability and strong authentication. Furthermore, creating standardized security procedures for multi-cloud and hybrid-cloud ecosystems will increase interoperability and compliance, paving the path for a more robust cloud security environment.

9 Conclusion

This study analyzed cloud computing architectures (SaaS, PaaS, and IaaS) and their security challenges, with a focus on public and hybrid clouds. Key findings include: (1) API misconfigurations cause 66% of breaches [9]; (2) centralized security improves compliance; and (3) cutting-edge solutions such as AI-driven detection and blockchain-based access control provide superior protection. A simulated survey of 50 IT professionals confirmed CSPM's efficacy, with 85% reporting increased security. While NIST guidelines provide a solid foundation, emerging threats, such as 5G-driven IoT vulnerabilities, necessitate adaptive strategies. Future research should look into quantum computing's impact on encryption and zero-trust architectures in multi-cloud systems. To ensure the resilience of cloud ecosystems, organizations must prioritize proactive monitoring and hybrid frameworks.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Acknowledgment

The authors thank the World-Wide Cloud Computing Network Security Researcher, for the related data utilized in the work.

References

[1] IDC, "Worldwide Cloud Spending Report." [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS52010424. [Accessed: Mar. 18, 2025].

[2] IBM X-Force, "Cloud Security Report," 2021. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence. [Accessed: Mar. 18, 2025].

[3] M. A. Hossain and M. A. A. Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *Int. J. Comput. Appl.*, vol. 44, no. 5, pp. 455–464, Aug. 2020, doi: 10.1080/1206212X.2020.1809177. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/1206212X.2020.1809177

[4] S. Revathi, "Data mining techniques with cloud security," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 11, pp. 468–472, Nov. 2019, doi: 10.22214/ijraset.2019.11076. [Online]. Available: https://www.ijraset.com/fileserve.php?FID=22042

[5] S. Kumar and S. Kumar, "Cloud security based on PaaS model," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 7, pp. 378–385, Jul. 2019, doi: 10.26438/ijcse/v7i7.378385. [Online]. Available: https://www.ijcseonline.org/archive_issue.php?pageNum_RS_U=6&pub_id=73&totalRows_RS_U=64

[6] IJSETR, "Enhanced solutions for security as a service cloud model," *Int. J. Sci. Eng. Technol. Res. (IJSETR)*, vol. 8, no. 9, pp. 3456–3460, Sep. 2019. [Online]. Available: https://www.ijsetr.org/wp-content/uploads/2019/09/IJSETR-VOLUME-8-ISSUE-9-3456-3460.pdf

[7] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernández, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 5, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.

[8] Z. Mirza, Z. Farooqui, M. Jain, and A. Karolia, "Cloud based solution for small and medium franchisees," *Int. J. New Technol. Res.*, vol. 3, no. 3, pp. [page numbers], Mar. 2017. [Online]. Available: https://www.neliti.com/publications/263338/cloud-based-solution-for-small-and-medium-franchisees

[9] IJCSMC, "Understanding of intrusion detection system for cloud computing with networking system," *Int. J. Comput. Sci. Mobile Comput.*, vol. 9, no. 3, pp. 19–25, Mar. 2020. [Online]. Available: https://ijcsmc.com/docs/papers/March2020/V9I3202008.pdf

[10] M. L. Toro, N. A. Muhammad, A. R. Shu'aibu, M. A. Garba, A. Abdulaziz, and K. Musa, "Security, privacy issues and solutions of mobile cloud computing," *United Int. J. Res. Technol.*, vol. 2, no. 7, pp. 112–117, May 2021. [Online]. Available: https://uijrt.com/paper/security-privacy-issues-solutions-mobile-cloud-computing

[11] Cybersecurity News, "AWS breach analysis," 2023. [Online]. Available: https://cybersecuritynews.com/aws-s3-bucket-misconfiguration-2023. [Accessed: Apr. 4, 2025]

[12] Google Cloud, "AI security trials," 2024. [Online]. Available: https://cloud.google.com/security/ai-threat-detection. [Accessed: Apr. 1, 2025]

[13] Hyperledger, "Financial sector case study," 2024. [Online]. Available: https://www.hyperledger.org/case-studies/finance. [Accessed: Apr. 1, 2025]