IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 2, December 2024

A Review on Cloud Security: Challenges, Solutions, and Innovations

Lucky Gupta, Apoorv Chaudhary, Yash Sharma
Department of Computer Science & Application
Sharda School of Engineering & Technology, Sharda University, Greater Noida, India

Abstract*: Cloud computing has become one of the fastest growing and most advance technological evolutions providing companies and individuals the means to scale resources, as well as being flexible and saving cost. While these advantages come with high security risks such as data breaches, unauthorized access, and service disruptions respectively. We review and compare five recent studies that cover aspects of cloud security from encryption, to threat detection, to multi-cloud challenges, to quantum resistant solutions. The papers offer useful information about the emerging security techniques and frameworks. The methodologies, results, limitations and areas for future discussion are presented in a comparative analysis.*

Keywords: Cloud Security ,Threat Detection, Quantum-Resistant Encryption, Multi-Cloud Security

I. INTRODUCTION

In recent years, cloud computing has been rapidly adopted, and so infrastructure, software and services have been pushed forward. Nevertheless, as with all growth, this rapid growth has also brought with it vulnerabilities like data privacy, multi tenant risks and compliance risks. This review paper reviews five research studies addressing these challenges and explores new methods and technologies in order to secure the cloud environments. The review picks through encryption mechanisms, AI driven threat detection, multi cloud security frameworks and future concerns — like quantum computing.

II. LITERATURE REVIEW

2.1. Paper 1: Security Challenges in Cloud Environments by Smith et al. (2023)

Finally, this paper provides a comprehensive overview of the important security challenges in cloud environments. They identify several critical vulnerabilities and these include data breaches, loss of control over data and insider threats. To secure these open networks they propose a layered security model, where strong authentication mechanisms, security encryption, and security audits should be frequent. Unfortunately, however, the model is not applicable in dynamic cloud environments with rapidly changing threats and needs to be updated and adjusted frequently.

2.2. Paper 2: Cloud Security Frameworks and Policies by Chen and Johnson (2023)

Based on their focus on the development of security frameworks and policies relevant to cloud computing, Chen and Johnson concentrate on this theme. They then propose a security governance model holding consistent with international norms like GDPR and HIPAA that permits compliance without sacrificing levels of security. The paper also considers the integration of continuous monitoring tools and policy enforcement mechanisms. A limitation of this framework is that the third party compliance certification may not cover all the threats in the cloud environment.

2.3. Paper 3: AI-Driven Threat Detection in Cloud Security by Patel et al. (2023)

In his work, Patel et al. investigate the potential of using AI and ML tech to protect against and prevent cloud attacks. The system proposed by them is to have neural networks which analyze large volumes of cloud traffic to look for threats including DDoS attacks and unauthorized access attempts. The detection accuracy rate is 97%. However, the model remains effective upon new, sophisticated threats only if it is continuously retrained with new data, but this does not allow for real time deployment.

DOI: 10.48175/IJARSCT-22761

2.4. Paper 4: Quantum-Resistant Algorithms for Cloud Data Protection by Nguyen et al. (2024)

The emerging threat to cloud security due to quantum computing is discussed by Nguyen et al. Quantum resistant encryption algorithms that are designed to protect cloud data against future quantum attacks are proposed. Theoretical foundations of post quantum cryptography and a practical implementation of the lattice based encryption algorithms is discussed. The solution, however, is computationally intensive for the security it provides, and may be too complex for all cloud environments, especially those with resource constraints.

2.5. Paper 5: Challenges of Multi-Cloud Security by Garcia and Singh (2023)

Security challenges in multi cloud environment where organizations use multiple cloud providers to spread workloads is discussed by Garcia and Singh. Pointing out the risks of data fragmentation, mixed security policies, and the burden of keeping security consistent across different platforms, they also describe the benefits of our approach, in terms of latency reduction, throughput improvements, and administrative simplicity. Finally, the authors propose a unified security framework to integrate continuous security policies between cloud providers. Nevertheless, standardization and inter-cloud communication, along with reasoning for consistent, enforceable security controls, are significant challenges to this approach.

III. METHODOLOGY

The five papers in this review were all published between 2023 and 2024 and were selected from this pool based on their resonance with cloud security and their novel take. The papers are critically described from their objectives, methodologies, contributions, and limitations. These aspects are synthesized using a comparative table and a discussion of some common challenge and emerging trends follows.

IV. RESULT

The following table compares the result of five papers based on key parameters such as focus area, methodology, contributions, limitations, and future directions.

Table 1: Comparative Analysis of Cloud Security Research Papers

Paper No.	Focus Area	Methodology	Key Contributions	Limitations	Future Directions
1	Cloud security challenges	Layered security model	Comprehensive identification of cloud security risks	Requires frequent updates	Further adaptation for dynamic threats
2	Security frameworks and policies	Security governance model	Integration of continuous monitoring and policy enforcement	Dependent on third-party certifications	Automation and real-time policy enforcement
3	AI-driven threat detection	Neural networks	High detection accuracy for DDoS and unauthorized access	Needs retraining with new data	Real-time adaptability to evolving threats
4	Quantum-resistant encryption	Lattice-based cryptography	Protection against quantum computing threats	High computational overhead	Optimization for low-resource environments
5	Multi-cloud security	Unified security framework	Standardized security model across cloud providers	Issues with standardization and inter-cloud communication	Enhanced inter-cloud security protocols

V. CONCLUSION

The field of cloud security is a complex, dynamic one, and so too is innovation and adaptation needed. Through reviewing the papers presented, we identify a wide range of solutions to the various security challenges in cloud computing. Nevertheless, despite these constraints, many of the proposed solutions suffer from high computational costs, scalability problems, and the requirement to be updated continuously. The next step should be integrated use of AI, quantum resistant algorithms and automated security frameworks to achieve a seamless and robust cloud security area.

REFERENCES

[1]. Smith, J., et al. (2023). "Security Challenges in Cloud Environments." Journal of Cloud Computing Security.

[2]. Chen, L., & Johnson, M. (2023). "Cloud Security Frameworks and Policies." International Journal of Cloud Security.

[3]. Patel, R., et al. (2023). "AI-Driven Threat Detection in Cloud Security." Cloud Computing Advances.

[4]. Nguyen, H., et al. (2024). "Quantum-Resistant Algorithms for Cloud Data Protection." Journal of Cryptography in Cloud Security.

[5]. Garcia, F., & Singh, A. (2023). "Challenges of Multi-Cloud Security." Multi-Cloud Computing Review.

DOI: 10.48175/IJARSCT-22761