Review of Cyber security Threats and Defense Mechanisms in Cloud Computing

Ms.Heena Patel[1], Ms.Priti Dhimmar[2]

[1]Lecturer, Department of Computer& Information Technology& VICAIT Surat, Gujarat.

[2]Lecturer, Department of Computer& Information Technology& VICAIT Surat, Gujarat.

---***---

Abstract - As cloud computing presents scalable, flexible, and flexible technology, it has totally rewritten way organizations store, process, and manage data. Still, there are currently serious security problems due to the growing use of cloud services. The confidentiality, integrity, and availability of cloud-based systems are at risk by challenges involving data breaches, insecure application programming interfaces (APIs), insider threats, malware attacks, account hijacking, and denial-of-service attacks. The major weaknesses in cyber security the cloud computing environments experience are reviewed in detail in this study, along with the defence strategies employed to minimize those risks. It involves an in-depth review of security solutions, such identity and access management, intrusion detection and prevention systems, encryption techniques, secure authentication methods, and respect in security standards. In order to improve trust and dependability in cloud computing platforms, the work presents current research trends and stresses the significance of put reliable safety frameworks and proactive security strategies in effect.

***Key Words*:** Cloud Computing, Cyber security Threats, Cloud Security, Data Breach, Encryption, Access Control, Intrusion Detection System

1.INTRODUCTION

An emerging trend in information technology is cloud computing, that allows users to access computing resources as well as storage, processing power, and applications over the internet on a pay-as-you-use basis. Scalability, flexibility, low infrastructure costs, and improved collaboration include only few of its many advantages. So, industries, educational institutions, healthcare organizations, and government sectors are all having embraced cloud computing.

As sensitive data stored in cloud environments can be accessed regularly remotely, it is additionally susceptible to cyber threats such denial-of-service attacks, malware infections, account and data breaches. Such threats may affect cloud-based systems' availability, confidentiality, and integrity, leading to financial damage, damage to an individual's reputation, and legal issues. Therefore, ensuring strong security in cloud computing is important for both cloud service providers and users. To reduce the risks, many of safety features have been developed, including identity and access management, encryption, secure authentication, intrusion detection systems, and compliance to security standards.

The goal of the review is to discuss the main security threats the cloud computing environments present and look at how to protect for those risks. This study provides insights into today's challenges and emphasizes the significance of putting in place efficient and thorough security frameworks to improve confidence and reliability in cloud computing systems through reviewing current research and security practices.

2. Body of Paper

Cloud computing includes service models as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) to deliver computing services on the internet. while these models are accessible and movable, they also establish particular safety requirements on users and cloud service providers. Ensuring data confidentiality, integrity, and availability becomes an urgent security requirement as the cloud systems work on shared and virtualized infrastructure. Network security, data protection, identity management, and daily surveillance are all fundamental parts of effective cloud security.

2.2 Cloud Computing Cyber security Threats

As cloud computing environments are distributed and open, it is sensitive to many cyber security risks.

2.2.1 Breach of Data

Data breaches happen when outsiders gain access to private data stored in the cloud. Weak authentication, properly designed storage, and poor encryption are some of the causes.

2.2.2 Insecure Interfaces and APIs

APIs serve a major role in online services' management and communication. Attackers can be able gain unauthorized access by making to the vulnerabilities presented by insecure APIs.

2.2.3 Safety to Inside

Authorized users who carefully or naturally use their access privileges present an insider threat in that they can compromise networks or leak data.

2.3 Cloud Computing Defense Mechanisms

Cloud environments include a variety of security techniques to reduce security issues.

2.3.1 Encryption of Data

Encryption provides privacy even in the event of illegal access by securing data in transit and at rest.

2.3.2 Secure Identification and Authorization

By ensuring proper identity verification, advanced systems for authentication reduce the risk of account hijacking.

2.4 Comparative Analysis of Cyber security Threats and Defense Mechanisms

Table 1: Cyber security Threats and Corresponding Defense Mechanisms in Cloud Computing.

Cyber security Threat	Description	Defense Mechanisms
Data Breaches	Unauthorized access to sensitive cloud data	Encryption, IAM, Access Control
Account Hijacking	Compromise of user credentials	Multi-factor Authentication, Secure Login
Insecure APIs	Vulnerable interfaces exposed to attackers	API Security, Authentication, Monitoring
Malware / Ransom ware	Malicious software affecting cloud resources	Anti-malware Tools, IDPS, Regular Updates
DoS / DDoS Attacks	Overloading cloud resources to disrupt services	Traffic Filtering, Load Balancing
Insider Threats	Misuse of access by authorized users	Role-based Access Control, Auditing

2.5 Discussion and Security Challenges

Although various security mechanisms are available, cloud security remains a challenging task due to evolving attack techniques, complex cloud architectures, and limited user awareness. A single security solution is insufficient to protect cloud environments. Therefore, a layered security approach combining multiple defense strategies is essential.

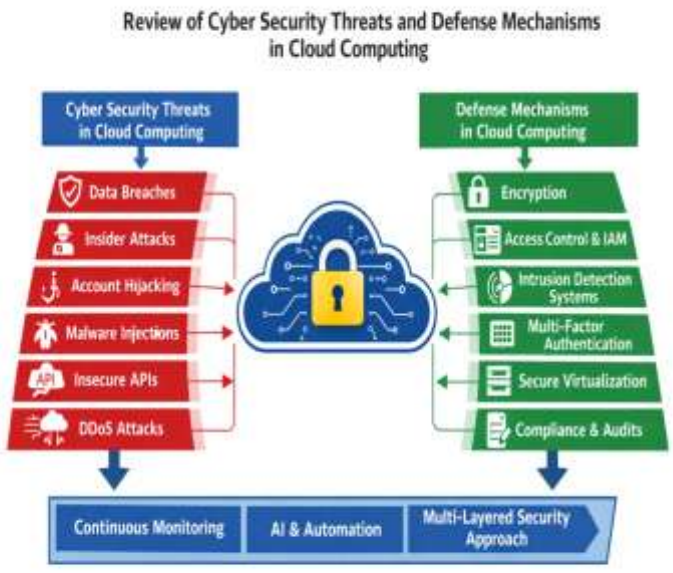
Review of Cyber Security Threats and Defense Mechanisms in Cloud Computing
Cyber Security Threats in Cloud Computing
Data Breaches
Insider Attacks
Account Hijacking
Malware Injections
Insecure APIs
DDoS Attacks
Defense Mechanisms in Cloud Computing
Encryption
Access Control & IAM
Intrusion Detection Systems
Multi-Factor Authentication
Secure Virtualization
Compliance & Audits
Continuous Monitoring
AI & Automation
Multi-Layered Security Approach

Fig -1: Figure

3. CONCLUSIONS

Cloud computing is very efficient, scalable and flexible and has immense benefits, but it also creates vital cyber security challenges. This review has identified significant dangers faced by the cloud environments and discussed the key defense mechanisms used in cloud environments including encryption, access control, authentication, intrusion detection systems and secure virtualization. Nevertheless, the presence of these security measures does not eliminate the issue of cloud security since cyber threats are constantly changing. Monitoring, risk assessment and implementation of advanced security model are thus critical. Cloud protection can also gain more strength, as the use of artificial intelligence and automated security solutions can be integrated. All in all, cloud computing environments require a multi-layered security reaction in order to guarantee data confidentiality, integrity and availability.

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to all individuals who contributed to the successful completion of this review paper. The author also acknowledges the researchers and authors whose published work provided essential insights and references for this study. Additionally, appreciation is given to the Vidhyadeep Institute of Computer and Information Technology, Anita (Kim) Surat for providing the necessary resources and academic environment.

REFERENCES

1. **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.
2. **Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023).** *Cyber attacks and Security of Cloud Computing: A Complete Guideline*. Symmetry.
3. **Krishna, G. & T. S., J. (2024).** Defensive Security Mechanisms for Cloud Computing Security Risks – A Review. International Journal of Science and Research (IJSR).
4. **Cloud Security: Counteracting Evolving Threats in a Digital Age (Preprint). (2025).** Explores threats such as account hijacking, malware, social engineering, and advanced countermeasures.
5. **Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022).** *Security of Zero Trust Networks in Cloud Computing: A Comparative Review*. Sustainability, 14(18), 11213.
6. ***An Analysis of Security Issues for Cloud Computing*.** Journal of Internet Services and Applications, 4(5), 2013.