ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhancing Data Security within Multi-Cloud Environments

Hritik Raj

PG Scholar, Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, India

ABSTRACT: Multi-cloud deployments are now trendy due to their cost-effectiveness, scalability, and agility. Organizations deploy them to enhance performance, escape vendor lock-in, and enhance resilience. The distribution of data across multiple CSPs, however, poses huge security and privacy concerns. Multi-cloud systems need strong security frameworks to guarantee data integrity, confidentiality, and regulatory compliance, in contrast to single-cloud deployments. Among the challenges are fragmented security regulations, poor encryption, data access vulnerabilities, and an expanded attack surface for cyber threats. Data breaches, unauthorized access, insider attacks, and compliance failures all threaten sensitive data. These challenges demand stronger assurances to ensure data remains secure across domains.

KEYWORDS: - Multi-cloud security, Cloud computing security, Identity and Access Management (IAM), Blockchain for cloud security, Secure data transmission, Attribute-Based Encryption (ABE)

I. INTRODUCTION

Cloud computing has fundamentally altered how companies manage, store, and process enormous volumes of data. As businesses and organizations rely more and more on digital infrastructures, multi-cloud strategies have emerged as a desirable way to take advantage of the advantages offered by various CSPs (cloud service providers). Multi-cloud tactics assist businesses in avoiding vendor lock-in, increasing operational effectiveness, optimizing resource use, and ensuring service redundancy. Multi-cloud architecture enables enterprises to spread workloads across several platforms while leveraging the distinctive strengths of each CSP, including cost, niche services, and regional presence. However, with these benefits, the complexity of data security in multi-cloud systems has increased significantly. A primary obstacle in multi-cloud security is coordinating various security frameworks as well as policies put in place by various cloud providers. Each CSP has its own security protocols, encryption standards, and access control mechanisms, which makes it difficult for organizations to enforce uniform security measures. This variation introduces potential security loopholes and vulnerabilities that malicious actors can exploit. Furthermore, data in multi-cloud systems is frequently transferred between different cloud platforms, which raises the possibility of illegal access and interception. To stop data breaches and leaks, it is essential to secure these data exchanges.

Additionally, regulatory compliance is a major issue for organizations with multiple cloud infrastructures. Organizations must adhere to strict data protection rules and many regulatory regulations, including the CCPA, GDPR, and HIPAA. The lack of consistency in the enforcement of compliance among cloud providers also makes it difficult, raising the stakes for noncompliance penalties and possible legal consequences. All these issues can be addressed with a completeSecurity solution that includes encryption methods, IAM (identity and access management), AI-based threat detection, blockchain technology, and global regulatory compliance standards.

The most important security concerns in multi-cloud are examined in the present research, in addition to suitable risk-mitigation strategies. The topic includes safe access controls to stop unauthorized access, blockchain-based security tools to provide more data integrity and transparency, and state-of-the-art encryption methods to protect data both in transit as well as at rest. The research also looks into how well AI-powered cybersecurity technologies can detect as well as respond to security events instantly. Companies can strengthen security of their multi-cloud systems while preserving data integrity, confidentiality, and compliance with international security requirements by using these security measures and best practices.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

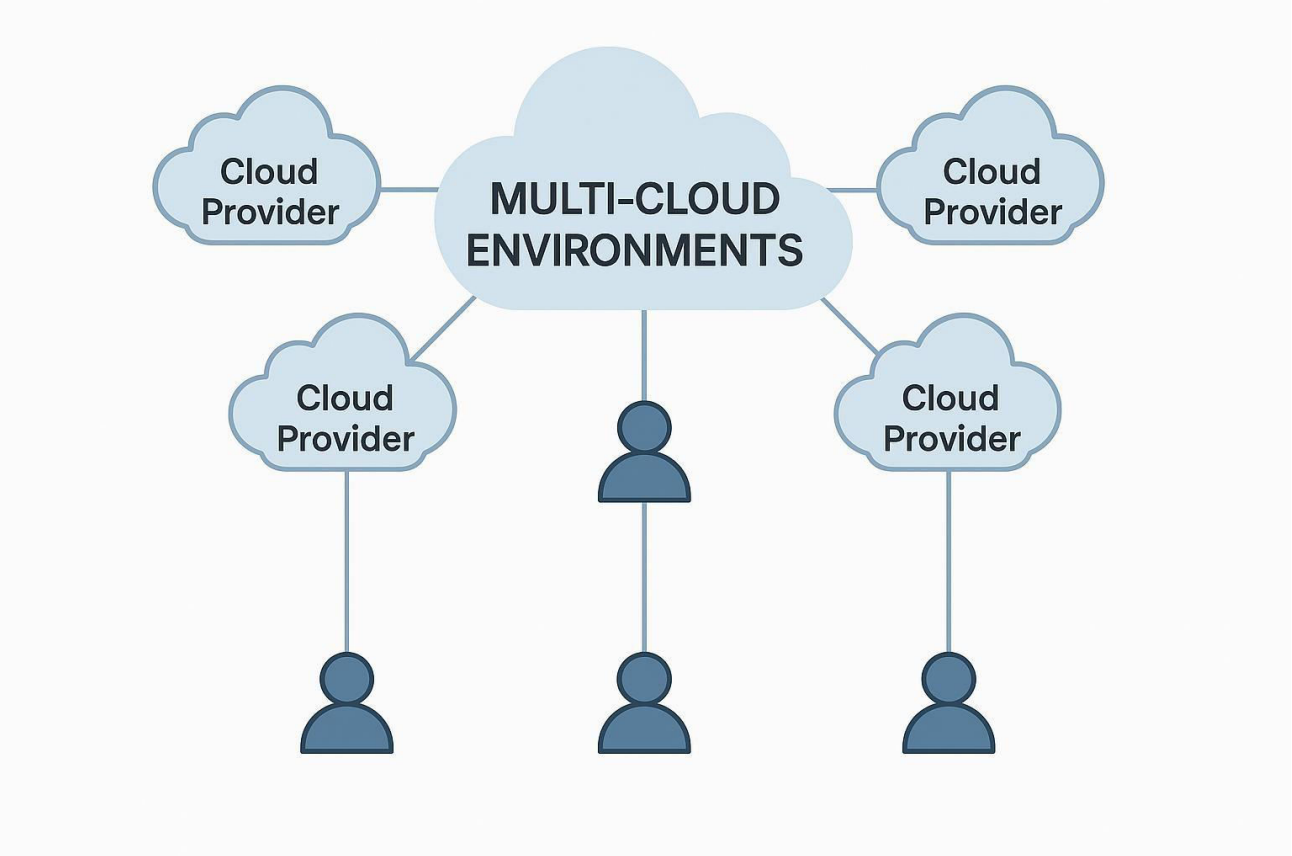

Figure 1: Multi-cloud environment structure

II. LITERATURE SURVEY

Enhancing Security in Multi-Cloud Environments Through Federated Access Control
Author: Prakash Somasundaram
This research proposes a FAC (federated access control) architecture after analyzing security concerns in multi-cloud systems. As businesses embrace multi-cloud deployments for greater scalability and resilience, managing security across multiple cloud providers becomes more complicated. Conventional access control is typically decentralized, and this creates security issues like unauthorized access and data leakage.
The research defines FAC as a single framework that combines identity management, authentication, and authorization across various cloud platforms. Security limitations are dynamically enforced by FAC using ABAC (attribute-based access control) and RBAC (role-based access control). The paradigm presented improves security by providing uniform access control, eliminating redundancy, and halting insider threats.

Enhancing Security and Privacy in Multi-Cloud Environments: A Comprehensive Study on Encryption Techniques and Access Control Mechanisms
Author: S. S. R. K. Prasad

As businesses become increasingly dependent on multi-cloud environments for redundancy and flexibility, data security and limited access across the providers become the main agenda.
The research classifies the encryption algorithms into three categories of symmetric, asymmetric, and homomorphic encryption and analyzes their efficiency, security strength, and computational complexity. Homomorphic encryption is particularly admired for having the ability to process encrypted data without decryption, thus increasing privacy, but with the disadvantage of high processing overhead. The research also examines ABE (attribute-based encryption),

which is a flexible method for accomplishing fine-grained access control.

Aside from encryption, the research considers access control models involving RBAC, ABAC, and Zero Trust paradigms. The paper suggests a hybrid model combining Attribute-Based Encryption (ABE) and ABAC that guarantees more security through dynamic, policy-enforced access control and efficient system performance.

Enhancing Data Security in Mobile Cloud Using Novel Key Generation
Authors: S. S. Manvi et al.

With mobile devices becoming more dependent on cloud services for processing and storage, secure access and data transfer become more challenging with limited device resources and inherent security weaknesses.

The paper proposes a new key generation method for improving encryption security in Mobile Cloud Computing (MCC). Conventional encryption methods sometimes suffer from key management and computational complexity issues, thus becoming less secure in mobile scenarios. The proposed method uses biometric authentication, device-specific attributes, and dynamic key generation methods to generate highly secure, user-specific encryption keys. The method reduces the likelihood of key compromise while improving data confidentiality at the same time.

Emergent (In)Security of Multi-Cloud Environments"
Authors: Morgan Reece et al.

Organizations using multi-cloud approaches for scalability, redundancy, and cost savings face greater security risks due to diverse security regulations, interoperability issues, and a growing attack surface.

Major risks in multi-cloud setups are identified in the paper, including inadequate identity management, data exfiltration, misconfiguration, and unauthorized access. The authors explore how security vulnerabilities occur due to the intricacies of integrating many cloud providers that have varying security needs. They also underscore the risks posed by API attacks, cross-cloud privilege escalation attacks, and insider attacks.

The research considers security best practices such as Zero Trust Architecture (ZTA), federated identity, and automated security orchestration to address these risks. To improve cloud security, the study emphasizes the necessity of AI-based anomaly detection, adaptive encryption techniques, and ongoing monitoring.

Enhancing Workflow Security in Multi-Cloud Environments through Monitoring and Adaptation upon Cloud Service and Network Security Violations"
Authors: Nafiseh Soveizi, Dimka Karastoyanova

As cloud-based distributed processes gain more popularity, ensuring security for multiple cloud services and networks has become tougher. The research aims at detecting and reacting to security breaches in real time to maintain process integrity as well as data security.

The authors introduce a security-conscious workflow
management approach that integrates continuous monitoring with adaptive measures. This system detects violations like service outages, unauthorized access, and insecure data flows at the network and cloud levels. When a violation is detected, the system dynamically adapts the workflow by substituting insecure services, redirecting processes, or modifying security policies to guarantee functioning and compliance.

III. TECHNIQUES FOR ENHANCING DATA SECURITY

Data protection across platforms has become essential as more companies use multi-cloud systems. With sensitive information constantly being stored, transferred, and processed across multiple cloud providers, robust security is needed. This section describes several cutting-edge techniques, including blockchain integration, identity and access management, encryption schemes, AI (artificial intelligence), and secure data transmission protocols, for improving data security in multi-cloud systems.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.1 Advanced Encryption Mechanisms

Encryption is imperative to data security across all phases, including in transit, at rest, and in processing. Encryption makes plaintext data unintelligible ciphertext, which makes it impossible for unauthorized recipients to understand and misuse the data.

3.1.1 Homomorphic Encryption

One of the most fascinating advances in cryptography technology is homomorphic encryption, which enables computation on encrypted material without first decrypting it. This guards data confidentiality even as it is being used, particularly important in cloud environments where third-party services can perform processing functions. While computationally intensive, ongoing research aims to render homomorphic encryption more feasible for large-scale implementation.

3.1.2 Attribute-Based Encryption (ABE)

ABE offers more granular access control solution. Rather than relying on pre-defined keys or roles, ABE grants access rights based on user attributes like department, clearance level, or job function. It is particularly helpful in dynamic settings with changing user roles and data access needs, such as multi-cloud systems.

3.2 Identity and Access Management (IAM)

Controlling who accesses what resources is paramount to cloud security. IAM systems ensure that only authorized people handle sensitive data by authenticating users, granting access, and auditing usage.

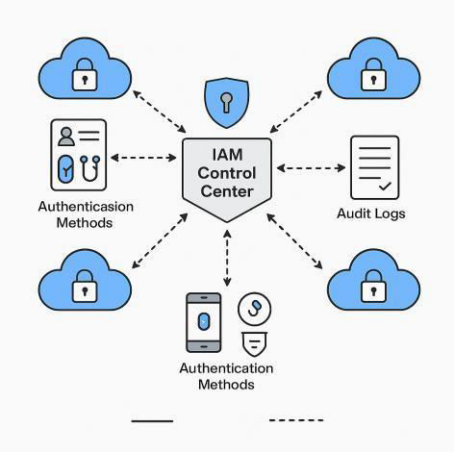

Figure 2: Identity and Access Management in a Multi-cloud environment

3.2.1 Zero Trust Security Model

The foundation of Zero Trust security approach is the tenet "never trust, always verify." This methodology guarantees that all access requests, regardless of their source, are put through rigorous verification processes in a multi-cloud setting. Every user or device has to be verified and authorized on an ongoing basis to minimize the chances of attackers laterally moving within a network.

3.2.2 Multi-Factor Authentication (MFA)

MFA improves security by requiring the user to provide several pieces of identification before granting access. The user may be able to identify themselves by biometric information, a security token, or something they know (password). Even in the event of a password leak, MFA dramatically lowers the likelihood of unwanted access.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

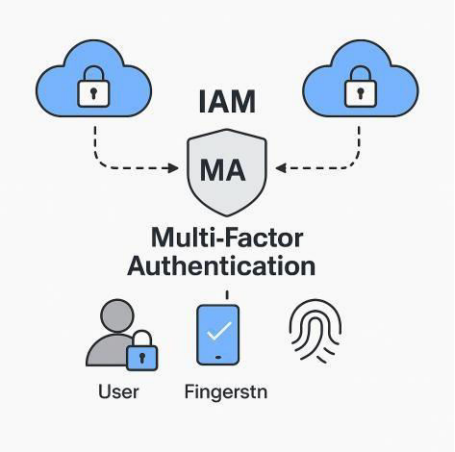

Figure 3: Multi-Factor Authentication in a Multi-cloud environment

3.3 Blockchain for Secure Multi-Cloud Transactions

Blockchain technology offers a decentralized and tamper-evident way of protecting information and transactions in multi-cloud environments. Blockchain enhances trust across scattered cloud environments by creating unalterable records and eliminating single points of failure.

3.3.1 Decentralized Identity Management

Decentralized identity management does not put user credentials into a single central database, where they could potentially be hacked. Rather, identity authentication is distributed across a blockchain network, so it becomes much harder for attackers to steal or alter credentials. It also gives individuals more control over their identities.

3.3.2 Smart Contracts for Security Enforcement

Smart contracts are autonomous contracts with security measures embedded in the code. Smart contracts across multiple clouds can automate the enforcement of access controls, ensuring consistent compliance across platforms. For instance, a smart contract can automatically withdraw access if a user violates a policy or the contract senses unusual activity.

3.4 Artificial Intelligence in Multi-Cloud Security

As the amount and intensity of cloud data increase, AI (Artificial Intelligence) plays more important role in identifying as well as reacting to security threats. AI-enabled technologies can analyze enormous data sets in real-time, detecting threats that would be difficult to identify manually.

3.4.1 AI-Based Threat Detection

Machine learning algorithms that have been trained on network traffic and user behavior can recognize anomalies that indicate a security incident, like an unusual time of login or unauthorized file access. Such systems improve with experience, becoming increasingly accurate as they become aware of emerging patterns and attack vectors.

3.4.2 Automated Incident Response

The automated incident response system is capable of quick action once it has recognized a threat, for instance, by quarantining affected systems, cancelling access tokens, or alerting security experts. Real-time action reduces the damage wrought by attacks and speeds up the recovery process.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804457

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. REGULATORY COMPLIANCE IN MULTI-CLOUD ENVIRONMENTS

Maintaining compliance with regional as well as sector-specific data protection laws is of utmost importance as companies use multi-cloud solutions more frequently to improve scalability, flexibility, and cost savings. Multi-cloud systems complicate regulatory compliance since data is dispersed across multiple cloud platforms, each of which is governed by a different set of laws and operates in a different nation. Organizations need to know their countries of operation's regulatory requirements and ensure that their cloud service providers facilitate and enforce them.

4.1 General Data Protection Regulation (GDPR)

European Union has published a comprehensive privacy policy called the GDPR (General Data Protection Regulation), which applies to any business that handles the data of EU citizens, whether or not they are based in the EU. In multi-cloud environments, GDPR compliance requires strict data protection controls, including strong encryption at rest and in transit, an accurate permission management process, and the ability to act rapidly against data breach notifications. Moreover, businesses need to ensure that data processing and storage activities occur in nations with similar data protection laws, which often requires data localization or specific cross-border transfer processes.

4.2 Health Insurance Portability and Accountability Act (HIPAA)

Protected Health Information (PHI), or sensitive health data, is regulated by the HIPAA, an American law. HIPAA compliance requires robust access control, audit trails, encryption of data, and regular security risk analysis for healthcare organizations operating multi-cloud environments. For shared responsibility in safeguarding patient information, cloud providers and covered entities need to execute Business Associate Agreements (BAAs). Because of the severe legal and financial consequences that could result from any breach or violation of PHI, secure cloud configuration and proper role-based access are essential.

V. CHALLENGES AND FUTURE DIRECTIONS

The tools and approaches to protecting multi-cloud systems need to evolve alongside these environments. Organizations are faced with both new challenges and opportunities for securing these complex infrastructures due to their increasing reliance on numerous cloud service providers (CSPs) to offload workloads and data. Emerging developments suggest that smart automation, seamless integration, and preparedness for new technologies such as quantum computing are becoming critical.

5.1 Integration Complexity

The intricacy of integration is among the most urgent issues in multi-cloud security. Businesses frequently use various cloud platforms to implement a wide range of security technologies, regulations, and compliance frameworks. Maintaining consistent protection can be challenging since different CSPs may have different proprietary security products, interfaces, and compliance criteria. Interoperability, centralized monitoring, and orchestration technologies that unify security visibility and control are necessary for the seamless integration of various systems. To minimize blind spots, decrease manual settings, and guarantee consistent policy enforcement across all cloud environments, security teams must use cloud-agnostic solutions and established procedures.

5.2 AI-Driven Adaptive Security

The future of multi-cloud security lies in AI-powered adaptive security technologies, which can handle the distributed and dynamic character of contemporary cloud settings. These systems use artificial intelligence and machine learning to monitor risks continuously, identify anomalies, and react to hazards instantly. AI is capable of identifying threats that have not yet been identified and modifying defenses in response by analyzing vast quantities of data from many sources, including network traffic, user behavior, and access patterns. Response times are reduced and human mistakes are minimized through automated threat mitigation methods, such as adjusting access.

Thresholds or quarantining compromised systems. Adaptive AI-driven security will be essential for maintaining resilience and active defence as attacks become more sophisticated.

VI. CONCLUSION

Multi-cloud systems, in which businesses use services from many CSPs, are becoming more and more popular because of their adaptability, affordability, risk sharing, and capacity to handle a range of workloads. However, these environments pose serious security and privacy concerns alongside operational advantages. The heterogeneous nature of cloud platforms often leads to disjointed security practices, inconsistent policy enforcement, and increased vulnerability to intrusion. As a result, multi-cloud deployment security requires a robust, tiered, and integrated strategy.

To get past these challenges, companies must adopt state-of-the-art encryption methods that protect data when it's at rest, in transit, and in processing. Technology like ABE and homomorphic encryption, which enable safe computing and fine-grained access control, reduces the likelihood of unauthorized access to data. By using these techniques, the data is protected and rendered incomprehensible even in event of a breach.

Other crucial step involves implementing Identity and Access Management (IAM) ideas. Organizations can uniformly design and enforce user roles, authentication protocols, and access control across multiple cloud environments through IAM. Two strategies that improve user authentication and lower the possibility of credential compromise are Zero Trust Security Models and MFA.

By enabling decentralized, impenetrable identity management and transaction verification, blockchain technology provides an additional layer of security to multi-cloud environments. Through automated enforcement of security rules, smart contracts could offer homogeneous governance and compliance across cloud environments.

Artificial Intelligence (AI) is yet another revolutionary tool. AI-based security systems can identify anomalies, analyze patterns in behaviour, and respond to threats automatically and instantly.
Companies can better predict and prevent potential intrusions using machine learning algorithms than they could be able to using traditional security technologies.

Adaptive security models—systems that have the ability to dynamically adjust to changing threat environments and expanding cloud architectures—should be a major focus of future research and development. Present encryption protocols would be made obsolete if quantum computing emerges. Therefore, creating and deploying quantum-resistant encryption techniques will be crucial to protecting cloud data in the post-quantum future.

In summary, although multi-cloud environments expose specific security and privacy challenges, a comprehensive strategy utilizing state-of-the-art encryption, IAM, blockchain, and AI can significantly enhance organizational resistance. Long-term data protection and law compliance can be guaranteed through the use of post-quantum cryptography and adaptive models to get ready for hypothetical attacks.

REFERENCES

1. Somasundaram, P. (2023). *Enhancing Security in Multi-Cloud Environments Through Federated Access Control*. International Journal of Computer Engineering and Technology (IJCET).
2. Prasad, S. S. R. K. (2023). *Enhancing Security and Privacy in Multi-Cloud Environments: A Comprehensive Study on Encryption Techniques and Access Control Mechanisms*.
3. Manvi, S. S., & Shyam, G. (2022). *Enhancing Data Security in Mobile Cloud Using Novel Key Generation*. Procedia Computer Science, 190, 367–374.
4. Reece, M., et al. (2023). *Emergent (In)Security of Multi-Cloud Environments*. arXiv preprint arXiv:2301.11233.
5. Soveizi, N., & Karastoyanova, D. (2023). *Enhancing Workflow Security in Multi-Cloud Environments through Monitoring and Adaptation upon Cloud Service and Network Security Violations*. arXiv:2303.15742.
6. Subashini, S., & Kavitha, V. (2011). *A survey on security issues in service delivery models of cloud computing*. Journal of Network and Computer Applications, 34(1), 1-11.
7. Singh, A., & Chatterjee, K. (2017). *Cloud security issues and challenges: A survey*. Journal of Network and Computer Applications, 79, 88-115.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

8. Sood, S. K. (2012). *A combined approach to ensure data security in cloud computing*. Journal of Network and Computer Applications, 35(6), 1831-1838.
9. Liu, W., et al. (2018). *Attribute-based encryption for cloud data sharing*. Future Generation Computer Systems, 86, 914-923.
10. Saxena, N., & Griss, M. (2020). *Security in multi-cloud platforms using blockchain-based identity management*. Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom).
11. Krutz, R. L., & Vines, R. D. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley.
12. Chappell, D. (2020). *Multi-Cloud Strategy for Dummies*. Wiley Special Edition.
13. Rountree, D., & Castrillo, I. (2013). *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice*. Syngress.
14. National Institute of Standards and Technology (NIST). (2011). *NIST SP 800-145: The NIST Definition of Cloud Computing*.
15. Cloud Security Alliance (CSA). (2019). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*.
16. NIST. (2020). *SP 800-207: Zero Trust Architecture*.
17. IBM Security. (2021). *Securing the Multi-Cloud Enterprise: Best Practices for a Secure Digital Transformation*.
18. Microsoft Azure. (2022). *Security in a Multi-Cloud World: How to Build Unified Protection*.
19. Gartner. (2023). *Top Security and Risk Trends in Cloud Computing*.
20. Palo Alto Networks. (2022). *The State of Cloud-Native Security: Insights into Multi-Cloud Adoption and Risk Mitigation*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com