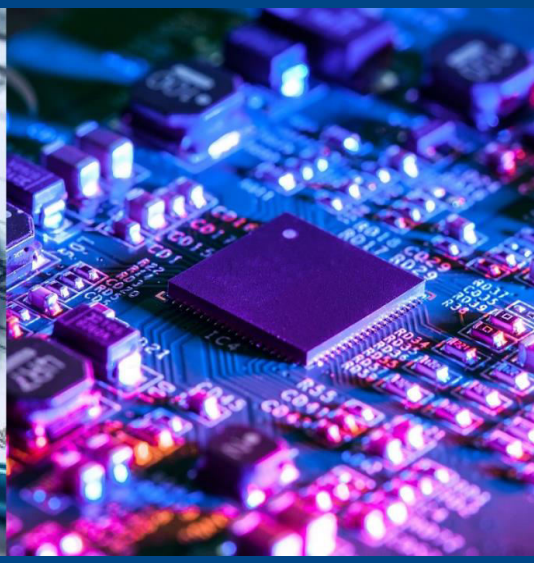
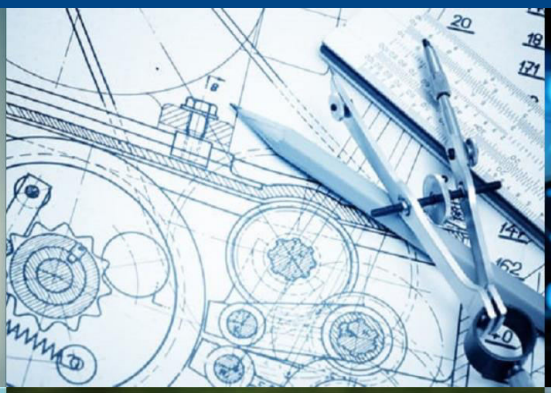
ISSN: 2582-7219

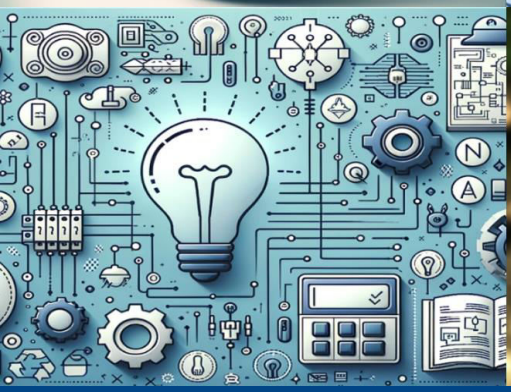




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(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.2025.0804183

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)

Comprehensive Security Strategies for Sensitive Data in Untrusted Multi-Cloud Environments

Swapnali S. Bhokare[1], Prof. Sachin B. Bhosale [2], Prof. Anand A. Khatri [3]

Department of Computer Engineering, Jai Hind College of Engineering, Kuran, Pune, Maharashtra, India[1-3]

ABSTRACT: The increasing reliance on multi-cloud environments for data storage and processing has introduced significant security challenges, particularly concerning the protection of sensitive data. This paper presents a comprehensive framework for securing sensitive data in untrusted multi-cloud environments, addressing the unique vulnerabilities associated with such architectures. We explore critical security challenges, including data fragmentation, inconsistent security policies, and the expanded attack surface that arises from utilizing multiple cloud providers. The proposed framework emphasizes a multi-layered security approach, integrating advanced techniques such as machine learning for threat detection, homomorphic encryption for data protection, and zero-trust architectures to ensure robust access control. Additionally, we highlight the importance of continuous monitoring and adaptive response mechanisms to mitigate security violations during workflow executions. By leveraging emerging technologies, such as blockchain for data integrity and AI-driven solutions for real-time threat analysis, organizations can enhance their security posture while maintaining compliance with regulatory requirements. The findings underscore the necessity for organizations to adopt proactive security measures that not only protect sensitive data but also foster trust in cloud services. This paper aims to provide actionable insights and strategies for organizations navigating the complexities of securing sensitive data in multi-cloud environments, ultimately contributing to the ongoing discourse on cloud security and data protection in an increasingly digital landscape. Through a detailed examination of current practices and future directions, this research serves as a valuable resource for practitioners and researchers alike, seeking to fortify their defenses against evolving cyber threats.

KEYWORDS: Multi-Cloud Security; Data Protection; Access Control; Encryption Techniques.

I. INTRODUCTION

The rapid adoption of cloud computing has revolutionized the way organizations store, process, and manage data. Cloud services offer scalability, cost efficiency, and high availability, making them an attractive choice for businesses across various sectors. However, with the growing reliance on cloud infrastructure, ensuring the security of sensitive data has become a critical challenge, especially in multi-cloud environments where data is distributed across multiple cloud providers. The presence of untrusted cloud environments exacerbates security concerns, as organizations have limited control over data governance, access management, and potential insider threats from cloud providers.

Multi-cloud environments involve leveraging services from multiple cloud vendors, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), to optimize performance, reduce vendor lock-in, and enhance disaster recovery strategies. While this approach offers flexibility and resilience, it also introduces significant security risks, including data breaches, unauthorized access, and compliance violations. The dynamic and distributed nature of multi-cloud environments necessitates robust end-to-end security mechanisms to protect sensitive data against various threats. Organizations are increasingly adopting multi-cloud strategies to avoid vendor lock-in, optimize costs, and improve service availability[1],[2]. However, this shift also introduces significant security challenges, particularly concerning the protection of sensitive data in untrusted environments[3]

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804183

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)

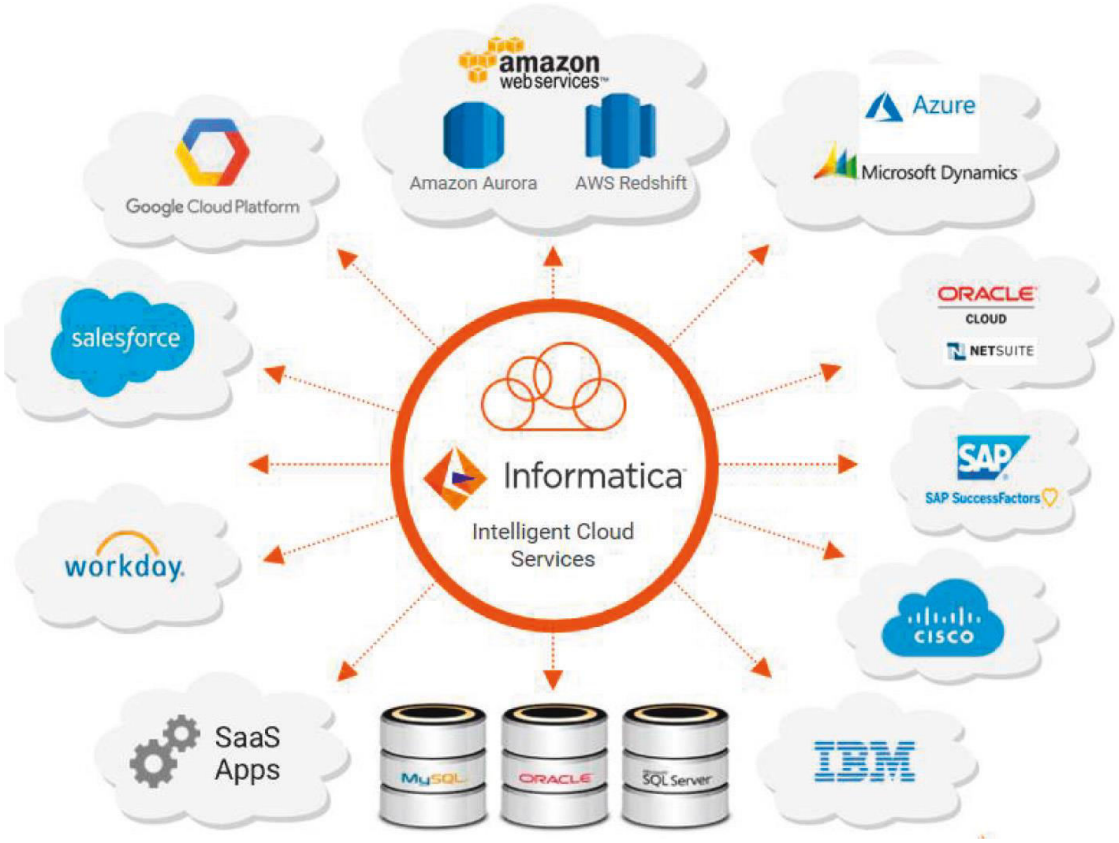


Figure 1. Multi-cloud integration mode [4]

1.1 Definition and Characteristics of Multi-Cloud Environments

Multi-cloud environments refer to the use of services from multiple cloud providers, which can include public, private, and hybrid clouds. This approach allows organizations to select the best services from various providers based on specific needs, such as performance, cost, and compliance[5] [6]. Key characteristics of multi-cloud environments include:

- **Diversity of Services**: Organizations can choose from a wide range of services offered by different providers, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[7][8]
- **Increased Flexibility**: Multi-cloud strategies enable organizations to quickly adapt to changing business requirements by leveraging the strengths of different providers.[9][10]
- **Enhanced Resilience**: By distributing workloads across multiple cloud providers, organizations can improve service availability and reduce the risk of downtime due to provider-specific outages[11]

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804183

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)

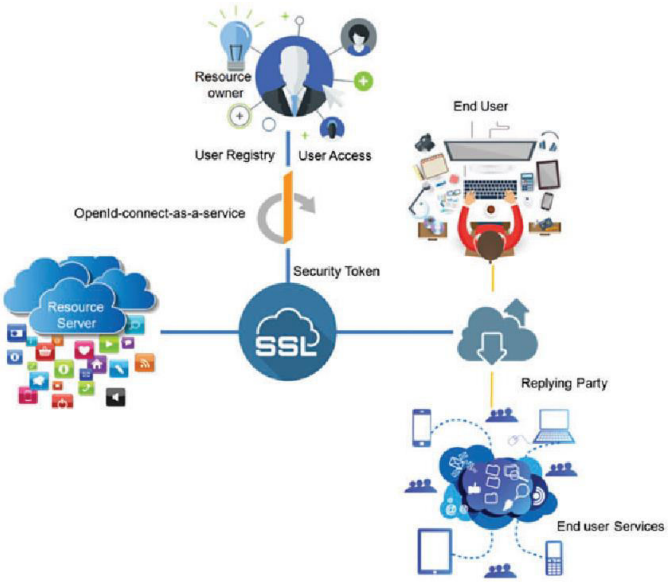


Figure 2. O-ID CaaS architecture[9]

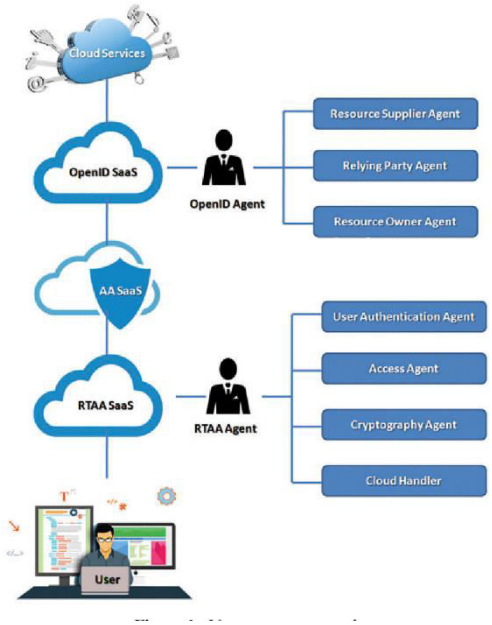


Figure 3. User Access Control[9]

1.2 Drivers of Multi-Cloud Adoption

Several factors drive the adoption of multi-cloud strategies, including:

- **Cost Optimization**: Organizations can take advantage of competitive pricing among cloud providers, optimizing their cloud spending[12]
- **Avoiding Vendor Lock-in**: By diversifying their cloud providers, organizations can mitigate the risks associated with vendor lock-in, allowing for greater negotiation power and flexibility[13]
- **Regulatory Compliance**: Multi-cloud environments can help organizations meet various regulatory requirements by allowing them to store data in specific geographic locations[14]

II. SECURITY CHALLENGES IN MULTI-CLOUD ENVIRONMENTS

While multi-cloud environments offer numerous benefits, they also present significant security challenges that organizations must address to protect sensitive data. The shared nature of cloud resources, combined with the complexities of managing security across multiple platforms, creates a unique set of vulnerabilities ([15].

2.1 Increased Attack Surface

The use of multiple cloud providers inherently increases the attack surface for organizations. Each additional service and integration point introduces new potential vulnerabilities that malicious actors can exploit[16]. This expanded attack surface necessitates a comprehensive security strategy that encompasses all cloud environments.

2.2 Data Fragmentation and Consistency

Distributing data across multiple cloud providers can lead to data fragmentation, making it challenging to maintain data consistency and integrity[17].Organizations must implement robust data synchronization and governance mechanisms to ensure that data remains accurate and up-to-date across all platforms.

2.3 Inconsistent Security Policies

Different cloud providers may have varying security policies and compliance standards, making it difficult for organizations to enforce consistent security measures across their multi-cloud environments[18]. A unified security framework is essential to address these inconsistencies and ensure comprehensive protection for sensitive data.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804183

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)

2.4 Shared Responsibility Model

The shared responsibility model in cloud computing complicates security management in multi-cloud environments. Organizations must clearly define their security responsibilities and ensure that appropriate measures are implemented at each level[19]. This model requires organizations to maintain vigilance over their data security while relying on cloud providers to secure the underlying infrastructure.

2.5 Lack of Centralized Visibility and Control

The distributed nature of multi-cloud environments can hinder centralized visibility and control over security posture. Organizations need robust security information and event management (SIEM) solutions to monitor and manage security across all cloud providers[20].Without centralized visibility, organizations may struggle to detect and respond to security incidents in a timely manner.

III. END-TO-END INFORMATION SECURITY: A MULTI-LAYERED APPROACH

To address the security challenges of untrusted multi-cloud environments, organizations must adopt a comprehensive, multi-layered approach to end-to-end information security. This approach should encompass the entire data lifecycle, from creation and storage to processing, transmission, and disposal[21].

3.1 Data Encryption

Data encryption is a fundamental component of end-to-end security. Organizations should employ robust encryption techniques for data at rest and in transit, utilizing strong encryption algorithms such as AES-256[22].Additionally, secure key management practices are essential to protect encryption keys from unauthorized access[23].

3.2 Access Control and Authentication

Implementing granular access control mechanisms is crucial to restrict access to sensitive data based on user roles, attributes, and context[24]. Multi-factor authentication (MFA) should be enforced to verify user identities and prevent unauthorized access[25]. Adopting a zero-trust security model, which assumes no implicit trust, is increasingly important in multi-cloud environments [26].

3.3 Data Loss Prevention (DLP)

Data loss prevention measures are essential to prevent sensitive data from leaving the controlled environment. Organizations should utilize DLP tools to monitor data movement and prevent unauthorized copying or transfer of sensitive information[27].

3.4 Intrusion Detection and Prevention

Deploying intrusion detection and prevention systems (IDPS) is crucial for monitoring network traffic and detecting malicious activities[28]. Organizations should implement both network-based and host-based IDPS, as well as AI-powered threat detection systems to enhance their security posture[29].

3.5 Secure Data Governance and Compliance

Establishing a robust data governance framework is essential for managing data access, usage, and disposal[30]. Organizations must define clear data ownership, access policies, and retention policies to ensure compliance with relevant regulations[31].

3.6 Secure Data Backup and Recovery

Implementing secure data backup and recovery mechanisms is essential to ensure business continuity in case of data loss or system failures. Organizations should utilize secure backup solutions and establish robust recovery procedures to restore data in the event of an incident[32].

3.7 Secure Inter-Cloud Communication

Organizations must implement secure communication protocols, such as TLS/SSL, to protect data in transit between different cloud environments. Utilizing virtual private networks (VPNs) or dedicated secure connections can further enhance the security of inter-cloud communication[33].

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804183

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)

3.8 Regular Security Audits and Assessments

Conducting regular security audits and assessments is essential to identify vulnerabilities and ensure compliance with security policies. Organizations should engage in penetration testing and vulnerability scanning to detect known vulnerabilities[34].

3.9 Incident Response Planning

Developing a comprehensive incident response plan is crucial for effectively handling security incidents[35]. Organizations should define procedures for detecting, responding to, and recovering from security incidents to minimize the impact of breaches[36].

3.10 Centralized Security Management

Implementing centralized security management tools and platforms is critical for gaining unified visibility and control across multiple cloud environments. This simplifies policy enforcement, monitoring, and incident response, enabling organizations to maintain a strong security posture[37].

3.11 Automation

Automating security tasks, such as configuration management, vulnerability scanning, and incident response, can improve efficiency and reduce human error. Organizations should leverage automation tools to streamline their security operations and enhance their overall security posture[38].

IV. EMERGING TECHNOLOGIES AND FUTURE DIRECTIONS

Several emerging technologies are transforming the landscape of end-to-end information security in multi-cloud environments. Organizations must stay abreast of these developments to enhance their security strategies.

4.1 Confidential Computing

Confidential computing technologies, such as Intel SGX and AMD SEV, provide hardware-level security by creating secure enclaves within processors. This allows sensitive data to be processed without being exposed to the underlying operating system or hypervisor, enhancing security in multi-cloud environments[39].

4.2 Blockchain Technology

Blockchain technology offers a decentralized and immutable solution for enhancing data security and transparency in multi-cloud environments. It can be utilized to create tamper-proof audit trails, secure data sharing, and manage digital identities[25].

4.3 Quantum-Resistant Cryptography

As quantum computing technology advances, existing cryptographic algorithms may become vulnerable. Developing and implementing quantum-resistant cryptographic algorithms is crucial to ensure long-term data security in multi-cloud environments[40].

4.4 AI and Machine Learning

AI and machine learning are increasingly used to enhance security in multi-cloud environments. These technologies can be employed for threat detection, anomaly detection, and security automation. However, their use also introduces new security challenges that organizations must address[41].

4.5 Serverless Computing

Serverless computing architectures can enhance security by reducing the attack surface and simplifying security management. By abstracting away server management, organizations can focus on application security and reduce the risk of vulnerabilities related to server configuration[42].

4.6 Zero Trust Security

The zero trust model assumes no implicit trust and requires continuous verification of every access request, regardless of location or network. This approach is particularly relevant in multi-cloud environments, where organizations must ensure that all access requests are authenticated and authorized[43].

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804183

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)

V. RESEARCH GAPS AND FUTURE RESEARCH DIRECTIONS

Despite significant advancements in end-to-end information security for sensitive data in untrusted multi-cloud environments, several research gaps remain. Addressing these gaps is essential for enhancing security in multi-cloud settings.

5.1 Unified Security Frameworks

Developing unified security frameworks that seamlessly manage security across diverse cloud providers and address the complexities of the shared responsibility model is crucial. Future research should focus on creating comprehensive frameworks that integrate security measures across multiple cloud environments.

5.2 Automated Security Management

Further research is needed to automate more security management tasks, improving efficiency and reducing human error. Organizations should explore advanced automation techniques to streamline their security operations and enhance their overall security posture.

5.3 Privacy-Preserving Analytics

Developing techniques for performing analytics on sensitive data without compromising privacy is a critical area of research. Future research should focus on exploring advanced cryptographic techniques, such as differential privacy and homomorphic encryption, to enable secure data analytics in multi-cloud environments.

5.4 Interoperability and Standardization

Improving interoperability between different cloud providers and establishing industry standards for multi-cloud security is essential. Future research should focus on creating standardized security protocols and frameworks that facilitate seamless integration across multiple cloud environments.

5.5 Quantum-Resistant Cryptography Implementation

The practical implementation and deployment of quantum-resistant cryptographic algorithms in multi-cloud environments require further research and development. Organizations should explore strategies for integrating quantum-resistant cryptography into their existing security frameworks.

5.6 Human Factors

Addressing the human element in security, including user training, awareness, and behavior, is crucial. Future research should focus on developing effective training programs and awareness campaigns to mitigate human-related security risks in multi-cloud environments.

5.7 AI-Driven Attacks and Defenses

Research into AI-driven attacks and the development of robust AI-based defenses is essential. Organizations should explore the implications of AI and machine learning on security and develop strategies to counteract potential threats.

5.8 Secure Data Migration and Interoperability

Developing secure and efficient methods for migrating data between different cloud environments and ensuring interoperability between different security tools and platforms is critical. Future research should focus on creating standardized protocols for secure data migration in multi-cloud settings.

5.9 Blockchain-Based Security Solutions

Exploring the potential of blockchain technology for enhancing security in multi-cloud environments, including secure data sharing, identity management, and audit trails, is an important area for future research.

5.10 Insider Threat Management

Developing better insider threat management strategies is essential for protecting sensitive data in multi-cloud environments. Future research should focus on identifying and mitigating insider threats through advanced monitoring and detection techniques.

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)

VI. CONCLUSION

The increasing adoption of multi-cloud environments presents both opportunities and challenges for organizations seeking to protect sensitive data in untrusted settings. A comprehensive, multi-layered approach to end-to-end information security is essential for addressing the unique security challenges posed by multi-cloud deployments. By leveraging emerging technologies and addressing existing research gaps, organizations can enhance their security posture and ensure the protection of sensitive data in an increasingly complex cloud landscape.

This introduction has provided a detailed overview of the key aspects of end-to-end information security for sensitive data in untrusted multi-cloud environments, highlighting the importance of a robust security framework and the need for ongoing research and innovation in this critical area.

REFERENCES

1. E. Kamau, T. Myllynen, S. D. Mustapha, G. O. Babatunde, and A. A. Alabi, "A Conceptual Model for Real-Time Data Synchronization in Multi-Cloud Environments," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 5, no. 1, pp. 1139–1150, 2024, doi: 10.54660/.IJMRGE.20247.5.1.1139-1150.
2. Y. Zhang and Z. Xu, "Neural Network-Powered Intrusion Detection in Multi-Cloud and Fog Envi ronments," International Journal of Advanced Computer Science and Applications, vol. 15, no. 6, 2024, doi: 10.14569/ijacsa.2024.0150625.
3. O. Bautista, K. Akkaya, and S. Homsi, "Outsourcing Secure MPC to Untrusted Cloud Environments with Correctness Verification," in 2021 IEEE 46th Conference on Local Computer Networks (LCN), IEEE, Oct. 2021, pp. 178–184. doi: 10.1109/LCN52139.2021.9524971.
4. T. Alyas et al., "Multi-Cloud Integration Security Framework Using Honeypots," Mobile Information Systems, vol. 2022, pp. 1–13, Aug. 2022, doi: 10.1155/2022/2600712.
5. P. Ramesh Naidu, N. Guruprasad, and V. Dankan Gowda, "A High-Availability and Integrity Layer for Cloud Storage, Cloud Computing Security: From Single to Multi-Clouds," J Phys Conf Ser, vol. 1921, no. 1, p. 012072, May 2021, doi: 10.1088/1742-6596/1921/1/012072.
6. W. J. K. Abraham, "A Comparative Survey On Various Provable Data Possession Schemes Of Integrity Verification In Single And Multi Cloud Environments," International journal of engineering research and technology, vol. 2, no. 7, Jul. 2013.
7. S. Medileh et al., "A Multi-Key with Partially Homomorphic Encryption Scheme for Low-End D evices Ensuring Data Integrity," Information, vol. 14, no. 5, p. 263, 2023, doi: 10.3390/info14050263.
8. E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, "Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks," IEEE Access, vol. 10, pp. 129520–129530, 2022, doi: 10.1109/ACCESS.2022.3228823.
9. D. Stalin David et al., "Cloud Security Service for Identifying Unauthorized User Behaviour," Computers, Materials & Continua, vol. 70, no. 2, pp. 2581–2600, 2022, doi: 10.32604/cmc.2022.020213.
10. N. S. Chaitanya and S. Ramachandram, "Implementation of security and bandwidth reduction in multi cloud environment," in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), IEEE, Dec. 2016, pp. 705–710. doi: 10.1109/IC3I.2016.7918053.
11. S. Shukla and S. J. Patel, "A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing," Computing, vol. 104, no. 5, pp. 1173–1202, May 2022, doi: 10.1007/s00607-021-01041-6.
12. H. S. Al-Qahtani, "A Taxonomy of Factors that Influence the Multiple-Cloud Computing Utilization," in 2024 13th International Conference on Computer Technologies and Development (TechDev), IEEE, Oct. 2024, pp. 91–95. doi: 10.1109/TechDev64369.2024.00024.
13. G. P. Kanna and V. Vasudevan, "A New Approach in Multi Cloud Environment to Improve Data Security," in 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), IEEE, Dec. 2017, pp. 7–12. doi: 10.1109/ICNGCIS.2017.23.
14. Nuruddin Sheikh, "Securing the cloud: A comprehensive analysis of data security challenges and solutions," International Journal of Science and Research Archive, vol. 13, no. 1, pp. 3471–3483, Oct. 2024, doi: 10.30574/ijsra.2024.13.01.1779.
15. M. H. Diallo, "User-Centric Security and Privacy Approaches in Untrusted Environments.," 2018.

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)

16. B. Qian et al., "Edge-Cloud Collaborative Streaming Video Analytics With Multi-Agent Deep Reinforcement Learning," IEEE Netw, vol. 39, no. 1, pp. 165–173, Jan. 2025, doi: 10.1109/MNET.2024.3398724.
17. P. R. V. -, "Securing Patient Data in Healthcare Cloud Systems: A Technical Overview," International Journal on Science and Technology, vol. 16, no. 1, Mar. 2025, doi: 10.71097/IJSAT.v16.i1.2754.
18. J. Singh, G. Singh, and A. Badhan, "Integrated Cloud and Blockchain Framework: A Secure Solution for Healthcare Data Management," in 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), IEEE, Nov. 2024, pp. 1259–1266. doi: 10.1109/ICAICCIT64383.2024.10912123.
19. K. J. Merseedi and Dr. S. R. M. Zeebaree, "Cloud Architectures for Distributed Multi-Cloud Computing: A Review of Hybrid and Federated Cloud Environment," Indonesian Journal of Computer Science, vol. 13, no. 2, Apr. 2024, doi: 10.33022/ijcs.v13i2.3811.
20. M. Abur, S. Junaidu, and A. Obiniyi, "Personal identifiable information privacy model for securing of users' attributes transmitted to a federated cloud environment," International Journal of Information Technology, vol. 14, no. 1, pp. 421–435, Feb. 2022, doi: 10.1007/s41870-021-00750-7.
21. C. Awasthi et al., "Preservation of Sensitive Data Using Multi-Level Blockchain-based Secu red Framework for Edge Network Devices," J Grid Comput, vol. 21, no. 4, 2023, doi: 10.1007/s10723-023-09699-2.
22. C. T. D. Pravina, N. Arya, S. Sharma, K. Chakraborty, S. K. Rakesh, and A. K. Singh, "Image Based Security System in cloud resource Scheduling," in Proceedings of the 5th International Conference on Information Management & Machine Intelligence, New York, NY, USA: ACM, Nov. 2023, pp. 1–6. doi: 10.1145/3647444.3647861.
23. A. S. Mattoo, D. Upadhyay, A. K. Dubey, and M. K. Shukla, "An approach to analyse and protect data on Untrusted Cloud Network," in 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, Jan. 2020, pp. 139–144. doi: 10.1109/Confluence47617.2020.9058012.
24. S. Salvi, Sanjay H.A., Deepika K.M, and Rangavittala S.R., "An encryption, compression and key(ECK) management based data security framework for infrastructure as a service in Cloud," in 2015 IEEE International Advance Computing Conference (IACC), IEEE, Jun. 2015, pp. 872–876. doi: 10.1109/IADCC.2015.7154830.
25. H. Y. Lin, "Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles," Sensors, vol. 23, no. 5, p. 2664, 2023, doi: 10.3390/s23052664.
26. K. Nandakumar et al., "Securing data in transit using data-in-transit defender architecture for cloud communication," Soft comput, vol. 25, no. 18, pp. 12343–12356, Sep. 2021, doi: 10.1007/s00500-021-05928-6.
27. Srujan Reddy Anugu, "Optimizing Data Flow in Multi-Cloud Environments: A Technical Deep Dive," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 1, pp. 1466–1473, Feb. 2025, doi: 10.32628/CSEIT251112154.
28. Giechaskiel, K. B. Rasmussen, and J. Szefer, "Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs," in 2019 29th International Conference on Field Programmable Logic and Applications (FPL), IEEE, Sep. 2019, pp. 45–50. doi: 10.1109/FPL.2019.00017.
29. Giechaskiel, K. B. Rasmussen, and J. Szefer, "Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs," in 2019 29th International Conference on Field Programmable Logic and Applications (FPL), IEEE, Sep. 2019, pp. 45–50. doi: 10.1109/FPL.2019.00017.
30. Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy," Applied Sciences, vol. 12, no. 23, p. 12441, Dec. 2022, doi: 10.3390/app122312441.
31. M. Beggas, M. A. Yagoub, and O. Kazar, "A multi-agent system approach based on cryptographic algorithm for securing communications and protecting stored data in the cloud-computing environment," International Journal of Information and Computer Security, vol. 11, no. 4/5, p. 413, 2019, doi: 10.1504/IJICS.2019.10023472.
32. C. Awasthi et al., "Preservation of Sensitive Data Using Multi-Level Blockchain-based Secured Framework for Edge Network Devices," J Grid Comput, vol. 21, no. 4, p. 69, Dec. 2023, doi: 10.1007/s10723-023-09699-2.
33. M. Elsayed and M. Zulkernine, "IFCaaS: Information Flow Control as a Service for Cloud Security," in 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, Aug. 2016, pp. 211–216. doi: 10.1109/ARES.2016.27.
34. M. Hosseini Shirvani, "Bi-objective web service composition problem in multi-cloud environment: a bi-objective time-varying particle swarm optimisation algorithm," Journal of Experimental & Theoretical Artificial Intelligence, vol. 33, no. 2, pp. 179–202, Mar. 2021, doi: 10.1080/0952813X.2020.1725652.

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)

35. D. R. M S, R. A, and A. Agarwal, "The Innovative Cloud Security Environment for Data Privacy," in 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), IEEE, Dec. 2023, pp. 748–751. doi: 10.1109/PEEIC59336.2023.10450434.
36. M. Madanan, P. Patel, P. Agrawal, P. Mudholkar, M. Mudholkar, and V. Jaganraja, "Security Challenges in Multi-Cloud Environments: Solutions and Best Practices," in 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, Sep. 2024, pp. 1608–1614. doi: 10.1109/IC3I61595.2024.10828949.
37. Srujan Reddy Anugu, "Optimizing Data Flow in Multi-Cloud Environments: A Technical Deep Dive," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 1, pp. 1466–1473, Feb. 2025, doi: 10.32628/CSEIT251112154.
38. J. Merseedi and Dr. S. R. M. Zeebaree, "Cloud Architectures for Distributed Multi-Cloud Computing: A Review of Hybrid and Federated Cloud Environment," Indonesian Journal of Computer Science, vol. 13, no. 2, Apr. 2024, doi: 10.33022/ijcs.v13i2.3811.
39. Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Distributed Denial of Service Attacks against Cloud Computing Environm ent: Survey, Issues, Challenges and Coherent Taxonomy," Applied Sciences, vol. 12, no. 23, p. 12441, 2022, doi: 10.3390/app122312441.
40. M. Chanodiya* and Dr. M. Potey, "Compositional Defence of Application Privacy in Resistant to Physical and Software Attacks in Untrusted Cloud Environment," Int J Eng Adv Technol, vol. 10, no. 6, pp. 70–78, 2021, doi: 10.35940/ijeat.f3024.0810621.
41. Y. Wang, Y. Guo, Z. Guo, W. Liu, and C. Yang, "Securing the Intermediate Data of Scientific Workflows in Clouds With ACISO," IEEE Access, vol. 7, pp. 126603–126617, 2019, doi: 10.1109/access.2019.2938823.
42. F. Abazari, M. Analoui, H. Takabi, and S. Fu, "MOWS: Multi-objective workflow scheduling in cloud computing based on heuristic algorithm," Simul Model Pract Theory, vol. 93, pp. 119–132, 2019, doi: 10.1016/j.simpat.2018.10.004.
43. X. Ye, S. Liu, Y. Yin, and Y. Jin, "User-oriented many-objective cloud workflow scheduling based on an imp roved knee point driven evolutionary algorithm," Knowl Based Syst, vol. 135, pp. 113–124, 2017, doi: 10.1016/j.knosys.2017.08.006.

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