Transactions on Engineering and Computing Sciences - Vol. 12, No. 02
Publication Date: April 25, 2024
DOI:10.14738/tecs.1202.18544.
Thangaraju, V. (2024). Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats. Transactions on Engineering and Computing Sciences, 12(02). 226-238.

Services for Science and Education

Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats

Vigneshwaran Thangaraju
CGI Technology and Solutions, Aldie, Virginia, USA

ABSTRACT

Organizations in today's digital ecosystem that want to improve their operational efficiency, flexibility, and scalability must have multi-cloud environments. Combining several cloud servers has positive effects such as minimizing vendor lock-in, enhancing functional service quality, and meeting various customers' demands. However, this entails numerous security perils such as, data leakage, cross-system operating ambiguities, and strong compliance demands. Hence, this paper focuses on the security issues associated with multicloud models, and measures as the ZTA, higher encryption protocols, and Artificial Intelligence-based continuous monitoring. The place of compliance, specifically GDPR and CCPA, in protecting data sovereignty across areas is also underscored. In particular, the present work seeks to present aspects of secure and integrated multi-cloud, which will help organizations reduce risks, enhance compatibility and manage multi-cloud environments to address emerging business requirements. This study reviews emerging threats, identifies critical gaps, and proposes future directions for multi-cloud security frameworks.

Keywords: Multi-Cloud Environments, Seamless Integration, Zero Trust Architecture, Data Security, Regulatory Compliance, Interoperability, Encryption Standards, AI in Cybersecurity, RealTime Monitoring, Cloud Computing.

INTRODUCTION

Today, organizations are looking at multi-cloud adoption to leverage the features of multiple cloud service providers in the digital domain. In multi-cloud computing, several cloud environments work independently of one another, without any kind of logical contract with a third party or cloud provider. The foundation of cloud computing is the PaaS, which is built on modules and aims to increase the availability, scalability, portability, and resource provisioning of multi-cloud systems. Companies are today adopting a multi-cloud strategy to engage multiple CSPs in the cloud system today. Multi-cloud systems can improve processes and service delivery for organizations because the systems are scalable, redundant, and flexible [1].

End users may integrate systems hosted by two or more cloud providers to form a multi-cloud environment. Currently, over 75% of contemporary businesses use multi-cloud setups. Increased availability and dependability are two benefits of multi-cloud settings that fuel this trend. Organizations may choose the finest services and features from several cloud providers to suit their unique needs when there are many available. Besides, helping to withstand outages, multi-cloud configurations could be useful in avoiding vendor lock-in.

Additionally, if one cloud fails or has an outage, employing different providers may assist disperse workloads and prevent service interruptions [2].

Multi-cloud environments are inherently complex, requiring seamless interoperability between diverse cloud infrastructures [3]. This intricacy increases the likelihood of security flaws, particularly when paired with the shared responsibility paradigm, which often misinterprets the security responsibilities of cloud providers and users. Because different cloud providers have different security features and capabilities, the environment is more difficult to integrate and maintain [4][5]. Interoperability is hindered by the fact that different cloud platform providers have developed different APIs, identity management systems, automation settings, configurations, logging technologies, network security protocols, orchestration choices, and automation. A highly compartmentalized approach to multi-cloud security has resulted from this fragmentation of security capabilities, which may lead to new attack vectors and vulnerabilities. Because of this, security experts often face the difficulty of developing their own unique cloud automation solutions or utilizing third-party solutions to accomplish interoperability [6].

Structure of the Paper

The structure of this paper is as follows: Section II provides an overview of multi-cloud environments and their significance; Section III discusses the security challenges in multi-cloud environments; Section IV explores best practices for seamless integration and robust security; Section V presents relevant literature and case studies; and Section VI offers conclusions and suggestions for future research directions.

MULTI-CLOUD ECOSYSTEM: A SECURITY PERSPECTIVE

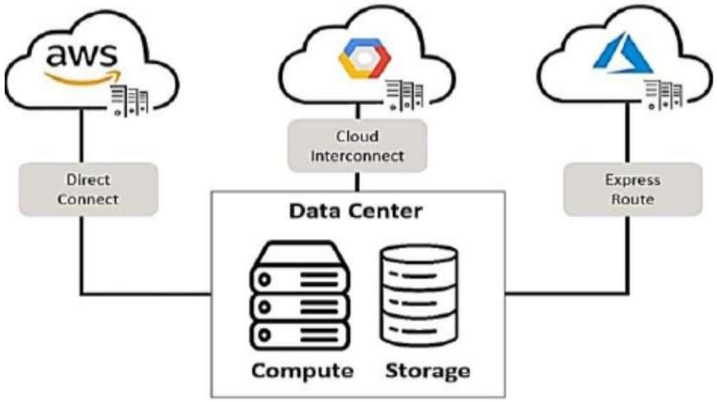


Fig 1: Multi-cloud Environment

A multi-cloud environment describes in Figure 1, how an enterprise uses many cloud services simultaneously. When the demand for virtual resources, especially during peak hours,

becomes too great for a single cloud environment to manage, a multi-cloud computing environment is born [7][8]. A multicloud computing environment has arisen in response to the inefficiency of a single cloud environment in meeting the massive demand for virtual resources during peak hours. In a multi-cloud setup, each cloud provider offers their own virtual

machines with varying specs and pricing points; furthermore, none of the virtual resources offered by these cloud services are freely shared or collaborated. It may make users' and providers' dreams of integrated cloud resource utilization a reality [9].

The Advantages of Multi-Cloud Environment

The multi-cloud environment avoids the drawbacks of single-cloud lock-in by combining the features of many cloud providers and offering consumers a variety of options. The benefits of a multi-cloud system compared to a conventional single-cloud setup [10].

- Performance assurance: The resources of different cloud providers may be used to sustain server performance once a single cloud has issues like service interruptions, inadequate resources, etc.
- Accessibility: Scheduling performance is enhanced, and geographical disparities across cloud providers are accommodated via the movement of virtual machines and data.
- Diversified customer needs: Improving the customer experience requires maintaining customer satisfaction. Customers may choose from a variety of services since various suppliers are diverse.
- Regional workloads: It is possible to shift workloads to the cloud nearer to the client due to geographic dispersion.
- Convenience: Facilitates user experience with services by means of integrated virtual resources that are not active.

Inherent Challenges

Multi-cloud will emerge as one of the most popular options for the majority of users, marking a significant trend in the evolution of cloud computing. Data security, modeling complexity, and scheduling resilience are only a few of the major issues that multi-cloud scheduling confronts, notwithstanding the benefits of a multi-cloud system over a single cloud.

- Security: Initially, because multi-cloud requires collaboration between many cloud providers, security is a critical concern. It raises the danger of the provider being attacked, even while it indirectly lowers the chance of privacy leakage by dispersing the same usersubmitted tasks among several clouds.
- Modeling: Second, multi-cloud scheduling involves complicated limitations on scheduling activities, such as the intricacy of pricing models across multiple clouds or the performance variances of different services inside the same cloud.
- Robustness: A common issue that arises during multicloud scheduling is job transfer between clouds. A practical and quick fix must be created to increase the scheduling's resilience in the event of a transmission interruption, task execution failure, or virtual machine failure [11].

Security Challenges in Multi-Cloud Environments

Below is a detailed discussion of these challenges, categorized by key aspects [12]:

- Complexity of Security Management: Managing security in a multi-cloud environment is inherently complex due to the diverse tools, interfaces, and frameworks offered by different providers. Each cloud platform comes with its unique set of security configurations, making centralized management difficult.

- Data Security and Privacy: One of the biggest issues that arise with the use of multiple clouds is ensuring info security and confidentiality. Based on data and experience on different cloud platforms it is crucial to secure data in transit and data at rest often requiring high levels of encryption and key management.
- Identity and Access Management (IAM): Another major issue that it faces is the issue of universal identification/access control in the different clouds. Cross-cloud IAM integration is very difficult as a way to standardize cloud services, while the violation of access control confuses the tracking and prevention of unauthorized access and privilege escalation.
- Misconfigurations: According to the findings, misconfigurations are one of the most significant factors in multi-cloud security risks. One of the main risks is configuration drift, that is settings are changed over time and is no longer aligned with the intended configuration.
- Threat Detection and Incident Response: A cloud environment, by nature, tends to provide a larger attack surface as threats are noticed to be diverse and incidents complicated to handle. Security tools integrations across various providers might be complex, and therefore when handling the security threats, it ends up taking a lot of time.
- Cost of Security: Securing many cloud infrastructures entails redundancy in security measures and products mainly because most cloud providers offer access to common tools.

Addressing the Challenges

To overcome these challenges, organizations must adopt a single security management platform that would maintain a consistent policy across the organization and monitor all the cloud providers. It can be suggested that adopting the zerotrust model will help reduce the threats connected with unauthorized access. Technology is useful in helping in threatening detection and also managing incidents once detected. The first level of protection requires training and awareness programs for IT organizations and security teams and using solutions created for multi-cloud purposes.

Without sacrificing security, organizations may take advantage of multi-cloud systems' scalability and flexibility by proactively tackling these concerns.

SECURITY IN MULTI-CLOUD ENVIRONMENTS WITH SEAMLESS INTEGRATION

Since organizations continue to use multi-cloud solutions to capture the essence of the different cloud systems, then the safety of such systems must be guaranteed [13]. Integration across these environments not only holds the organizational operations to higher levels but also brings in new kinds of security risks. Figure 2 shows the security considerations in a multi-cloud.

Safeguarding sensitive information, staying in compliance, and keeping the IT infrastructure running smoothly all depend on these factors being addressed. Below, they explore the key security considerations in multi-cloud environments with seamless integration.



Fig 2: Security consideration in a multi-cloud

Consistent Security Policies Across Platforms

Maintaining uniform security rules across several cloud service providers is a major obstacle in a multi-cloud setup. Every cloud platform comes with its security tools and frameworks, making it critical to standardize policies for:

- Access Control: Make sure users have the right amount of access to all clouds by implementing rolebased access control (RBAC).
- Encryption Standards: Encrypt all data, both while in motion and while stored.
- Policy Automation: Leverage policy-as-code tools to automate and enforce consistent security configurations.

Identity and Access Management (IAM)

Seamless integration requires robust IAM practices to prevent unauthorized access and data breaches. Key considerations include:

- Federated Identity Management: Implement federated identity solutions to provide a unified authentication mechanism across all cloud platforms.
- Multi-Factor Authentication (MFA): Strengthen IAM systems with MFA to add an extra layer of protection.
- Zero Trust Architecture: Adopt Zero Trust principles to minimize risks by verifying all access attempts, regardless of their origin.

Data Security and Privacy

Data security is critical in multi-cloud setups, especially during integration processes that involve data transfer and synchronization. Key strategies include:

- Data Encryption: Ensure end-to-end encryption during data transfers between clouds and for data at rest.
- Key Management: Use centralized key management solutions to simplify encryption practices and prevent key exposure.
- Data Residency Compliance: Monitor and enforce data residency rules to comply with regulations like GDPR and CCPA.

Secure Integration and API Management

Seamless integration relies on APIs to connect services and platforms, making API security critical [14].

Considerations include:

- API Gateway Security: Use API gateways to monitor and control API traffic across clouds.
- Rate Limiting and Authentication: Implement rate limiting, authentication, and authorization for API endpoints to prevent abuse.
- Regular API Audits: Periodically review API configurations to identify and patch vulnerabilities.

Incident Response and Recovery

Integrated environments require a unified approach to incident response to minimize downtime and damage during a breach. Key considerations include:

- Centralized Response Plans: Develop a centralized incident response strategy that covers all cloud providers.
- Backup and Recovery Systems: Implement robust backup and disaster recovery systems with cross-cloud redundancy.
- Tabletop Exercises: Regularly conduct simulated breach scenarios to test and refine incident response protocols

SECURITY THREATS IN MULTI-CLOUD ENVIRONMENTS

Cloud computing systems are susceptible to various threats such as data breaches, loss and unauthorized access. To reduce these risks: Tight access control and intrusion prevention systems are deployed [15][16]. More sophisticated encryption technologies [17][18], such as Advanced Encryption Standard or AES, are employed to protect data, both at rest and during transmission. Data anonymization deletes personally identifiable data from datasets thus minimizing the risk of identity theft.

- Encryption Standards: Encryption protocols like (Advanced Encryption Standard) AES, and PKI (Public Key Infrastructure) are advanced and adequate measures for preventing data loss through unauthorized access. Homomorphic encryption is pointed out as a type of technology that enables the processing of encrypted information without decrypting it, thus keeping sensitive data confidential even while in the course of computation.
- Data Residency and Sovereignty: Data Residency pertains to the physical location where the data is kept. To maintain sovereignty, it is important to follow local laws and regulations concerning data. Strategies that target multi-clouds should be customized and obliged to compliance jurisdictions, for example, GDP in the
- EU, in safeguarding data that is stored across a number of regions with different privacy protection requirements.

Network Security

With multi-clouds, organizations can choose a variety of cloud providers, which adds to the positives of their solution, as well as complexity of security, integration and management [19][20]. The Zero Trust Architecture (ZTA)[21] assumes no trust in by default, and also demands identity authorization and authentication to halt the movement of the cyber threat actors and data exfiltration.

Zero Trust Architectures (ZTA)

ZTA operates on the principle that an attacker could be present, applying continuous verification of users, devices, and applications through:

- Pinpointing to micro-segment the critical assets.
- IAM for the strong multi-factor authentication.
- Antecedent threat identification and constant surveillance.
- Seven key tenets of ZTA include Data, Devices,
- Users, Network/Environment, Automation/Orchestration, Visibility/Analytics and Workloads.

Secure Inter-Cloud Communication

- Inter-cloud communication in multi-cloud systems faces challenges due to:
- Having distributed networks in different regions and platforms.
- Threats of compromised credentials, DDoS, and MALWARE to the SEC platform.
- ZTA ensures secure inter-cloud communication by:
- Ensuring that data is encrypted when being sent across networks and when stored in computers.
- Factoring such means as fine-grained access controls to help minimize exposure.
- Archiving of the access requests to improve the levels of transparency and compliance.

BEST PRACTICES FOR SEAMLESS INTEGRATION AND SECURITY

Seamless integration and robust security are essential for leveraging the full potential of multi-cloud environments. Organizations may improve their multi-cloud architecture's efficiency, interoperability, and risk management by adhering to best practices.

Adopting Zero Trust Principles

Zero Trust operates on the assumption that all users are inherently unreliable. No computer or user should be immediately trusted in a zero-trust network since the fundamental idea is that there are possible attackers everywhere. Forrester Research states that the Zero Trust Model is based on the following principles: Segmenting the network and activating Layer 7 policy will guarantee that only valid application or traffic will be permitted to communicate.

- Employ a least-privileged access approach and be very stringent with access control. This indicates that people should only be granted access according to their needs and requirements, using a need-to-know approach.
- Keep track of all traffic going to and from the cloud. Subsequently, a department's network may be seen of as being easily accessible by an attacker.
- Micro-segmentation is a notion that zero-trust networks use. Breaking down security perimeters into smaller zones and ensuring separate access for different sections of the network is known as microsegmentation.
- The zero-trust paradigm also relies on multi-factor authentication (MFA). To access a protected resource using MFA, all it takes is more than just a password.
- Strict restrictions on device access are necessary for zero trust in addition to user access control. Zero-trust systems must keep an eye on how many different devices are attempting to connect to their network and confirm that each one is authorized [3].

Real-Time Monitoring and Incident Response

To ensure that organizations can quickly identify, evaluate, and react to new security risks, current cybersecurity plans include real-time monitoring and incident response. Proactively securing systems and infrastructure using AI and sophisticated monitoring technologies allows organizations to minimize the effect of threats and reduce reaction times[22].

Streamlined Incident Handling with AI:

- Employment of AI in management enhances the speed of dispatching incidents and overall reduction of the impact along with recovery phases.
- When it comes to threat detection it functions autonomously and can even address the threats found without the help of any human.
- Improves the capacity to arrange incidents in a way that streamlines usage of security tools and methods.
- It supports smooth and enhanced threat identification and reaction [23].

Continuous Monitoring and Intrusion Detection:

- It is recommended that Organizations embrace the use of Cloud security monitoring as a continuous process.
- Other categories include AI-integrated intrusion detection systems where the threat is detected and analyzed in real-time.
- Technologies based on the agent enhance the ability to respond to automated incidents [24].

Real-Time Threat Responses:

- When threats are perceived AI triggers immediate nervous system reactions.
- Offers fast and flexible reaction to threats in order to manage them efficiently.
- Preserves the data in systems that must share information dynamically throughout complex cloud networks[25].

Quick Threat Identification and Response:

- Real time threat detection reduces the effects of security incidents as implemented by AI.
- Can isolate end-point with the infection or rolls back any changes made on it by the hackers.
- It guarantees a rapid and effective counter-response to new threats without human intervention.

Improved Security Framework with AI:

- Enhances response times and reduces the likelihood of errors.
- Ensures a more agile and effective security posture.
- Contributes to continuous security improvement in multi-cloud environments [26].

Ensuring Compliance with Regulatory Standards

GDPR, CCPA, and other regional privacy laws impacting cloud deployments. Various legal standards, including GDPR, HIPAA, or PCI DSS, have different methods for each cloud provider.

GDPR:

Any organization that gathers or keeps personal information about EU citizens is subject to this European legislation. The GDPR requires organizations to:

- Use personal data in an open and responsible manner.
- Only collect personal data that's clearly related to a business objective.
- Maintain accurate and up-to-date personal data.
- Prohibit the export of personally identifiable information to countries outside of the EU 2) CCPA:

A US law that protects the data and privacy of California residents. The CCPA outlines several key consumer privacy rights, including

- Data subject rights, such as the right to access, rectify, and delete personal data
- awful processing, such as having a lawful basis for processing data, like consent or legitimate business interests [27].

Other regional privacy laws that impact cloud deployments include:

- Personal Information Protection and Electronic Documents Act (PIPEDA): A Canadian law
- Data Protection Act 2018: A UK law
- Payment Card Industry Data Security Standard (PCI DSS): A standard for the payment card industry
- Children's Online Privacy Protection Act of 1998 (COPPA): A statute mandating parental notification when data gathering from minors occurs on websites.

LITERATURE REVIEW

This section presents a literature review on Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats. A summary of the reviewed studies is provided in Table I for a concise overview. Harish Naik and Kannan. (2023) this report provides a concise overview of the key points, challenges, needs, and future outlook for settings that use multiple clouds. In addition, the paper examines traditional approaches and solutions provided by different multi-cloud frameworks, and it discusses the pros and cons of each. The concept of several clouds is gaining traction, and researchers are working hard to develop a multi-cloud architecture that can withstand all kinds of challenges, including simple setup, security concerns, administrative headaches, and more [28].

Yue et al. (2023) the article explain how bilinear mapping technology is used to safeguard user data while it is being processed and sent in the multi-cloud. In addition, the terminal is linked to several cloud service providers using trustworthy middleware, which guarantees better administration and security verification of user data through merging and segmentation. Data

integrity and security for users in a multi-cloud setting may be successfully guaranteed by the system, according to experimental findings and performance studies [29].

Shukla and Patil. (2023) the ability of multiple cloud service providers to seamlessly collaborate is known as interoperability in the context of multi-cloud. This allows customers to deploy applications across different cloud platforms without encountering compatibility issues or experiencing significant performance degradation. The proposed MCIF has all the necessary components to construct a robust and adaptable framework. Through the usage of a common cloud ontology, the MCIF guarantees that customers have a consistent and fruitful cloud computing experience across all cloud providers [30]

Shirvani. (2018) There was a lot of buzz about web service composition technology because of its potential to lower software development expenses. Each of the identical atomic web services made available by multiple cloud providers in a multi-cloud environment (MCE) has its own unique pricing and quality-of-service (QoS). According to the literature analysis in this area, most existing solutions focus only on QoS and network characteristics without considering security principles, which means it seldom resolve mission-critical business processes [31].

Allakonda and Sagar. (2021) examines current security solutions that use several clouds in order to find the gaps, problems, and opportunities for growth. Businesses must prioritize the safety and privacy of their cloud-based data. Using a unified user interface, multi-cloud services include public, private, and managed clouds. In multi-cloud, data is divided up across many clouds according to the data's sensitivity and the cloud's trustworthiness [32]

Table I: Summary of The Above-Related Work for Multi-Cloud Environments

Ref.	Area of Focus	Techniques	Key Findings	Future Work & Limitations
[28]	Overview of MultiCloud Environments	Analysis of existing multi-cloud frameworks	Identified challenges, requirements, and solutions for multi-cloud frameworks.	Emphasized the need for a unified multi-cloud framework addressing security, management, and configuration.
[29]	Security in MultiCloud Environments	Bilinear mapping, trusted middleware	Ensures data integrity and security through segmentation and merging techniques.	Highlights performance improvements but suggests further studies for real-time application and scalability.
[30]	Interoperability in Multi-Cloud Frameworks (MCIF)	Shared cloud ontology	Proposed MCIF to enhance communication and resource utilization.	Calls for deeper exploration of compatibility issues and optimization strategies for cross-cloud deployment.
[31]	Web Service Composition in Multi-Cloud	QoS analysis, security tenets	Discussed challenges in balancing QoS and security in business processes.	Suggests integrating cybersecurity measures with QoS considerations

				for mission-critical applications.
[32]	Security and Privacy in Multi-Cloud	Data partitioning across clouds	Demonstrated improved security and high availability for enterprise data.	Future work includes refining partitioning methods and addressing dynamic reliability concerns of cloud providers.

CONCLUSION AND FUTURE WORK

Multi-cloud environments offer organizations unparalleled flexibility, scalability, and resilience by enabling the integration of diverse cloud platforms. However, their very nature poses a multitude of security concerns which include data privacy, secure cloud-cloud communications and meeting regulatory measures. This review pointed out few of the challenges that need to be eliminated through the implementation of best practices like Zero Trust Architectures, better encryption techniques and real-time monitoring. Effective utilizing multi cloud and avoiding risks requires solid security measures and clarity of the integration processes possible within this strategy. This is possible through the progressive advancement of standard-based architectures and always advancing artificial intelligence and security solutions that will enhance the efficiency and security of multi-cloud environments. The future of multi-cloud environment is to focus on the long-standing challenges that include security compliance, cloud interoperability, as well as integration. There should be an attempt to research and bring out common security features to be adopted in multi-cloud environments to make them secure with little complications of handling them. This research includes the integration of artificial intelligence and machine learning for real-time threat detection, the automation of incidents, and the management of prediction and response.

References

[1]. J. Chen, P. Chen, X. Niu, Z. Wu, L. Xiong, and C. Shi, “Task offloading in hybrid-decision-based multi-cloud computing network: a cooperative multi-agent deep reinforcement learning,” J. Cloud Comput., 2022, doi: 10.1186/s13677-022-00372-9.

[2]. S. O. Afolaranmi, B. R. Ferrer, and J. L. M. Lastra, “A framework for evaluating security in multi-cloud environments,” in Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018. doi: 10.1109/IECON.2018.8591454.

[3]. A. and P. Khare, “Cloud Security Challenges : Implementing Best Practices for Secure SaaS Application Development,” Int. J. Curr. Eng. Technol., vol. 11, no. 6, pp. 669–676, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[4]. P. P. Ray, “A survey of IoT cloud platforms,” Futur. Comput. Informatics J., vol. 1, no. 1–2, pp. 35–46, 2016, doi: 10.1016/j.fcij.2017.02.001.

[5]. Suhag Pandya, “Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System,” Int. J. Adv. Res. Sci. Commun. Technol., pp. 865– 876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.

[6]. R. Duncan, “A multi-cloud world requires a multi-cloud security approach,” Comput. Fraud Secur., 2020, doi: 10.1016/S13613723(20)30052-X.

[7]. T. Shi, H. Ma, G. Chen, and S. Hartmann, “Location-Aware and Budget-Constrained Service Deployment for Composite Applications in Multi-Cloud Environment,” IEEE Trans. Parallel Distrib. Syst., 2020, doi: 10.1109/TPDS.2020.2981306.

[8]. R. Arora, S. Gera, and M. Saxena, “Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications,” in 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 458– 463.

[9]. Z. H. Md Emran Hossain1, Md Farhad Kabir2, Abdullah Al Noman3, Nipa Akter4, Zakir Hossain5Md Emran Hossain1, Md Farhad Kabir2, Abdullah Al Noman3, Nipa Akter4, “ENHANCING DATA PRIVACY AND SECURITY IN MULTI CLOUD ENVIRONMENTS,” Futur. Gener. Comput. Syst., vol. 107, no. 05, pp. 102–115, 2022.

[10]. B. Pang, F. Hao, Y. Yang, and D. S. Park, “An efficient approach for multi-user multi-cloud service composition in human–land sustainable computational systems,” J. Supercomput., 2020, doi: 10.1007/s11227-019-03140-w.

[11]. Q. Zhang, S. Geng, and X. Cai, “Survey on Task Scheduling Optimization Strategy under Multi-Cloud Environment,” C. - Comput. Model. Eng. Sci., vol. 135, no. 3, pp. 1863–1899, 2023, doi: 10.32604/cmes.2023.022287.

[12]. S. Murri, “Data Security Challenges and Solutions in Big Data Cloud Environments,” Int. J. Curr. Eng. Technol., vol. 12, no. 6, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.11.

[13]. V. S. Thokala, “A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications,” Int. J. Res. Anal. Rev., vol. 8, no. 4, pp. 383–389, 2021.

[14]. Vasudhar Sai Thokala, “Efficient Data Modeling and Storage Solutions with SQL and NoSQL Databases in Web Applications,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 470–482, Apr. 2022, doi: 10.48175/IJARSCT-3861B.

[15]. N. Abid, “Enhanced IoT Network Security with Machine Learning Techniques for Anomaly Detection and Classification,” Int. J. Curr. Eng. Technol., vol. 13, no. 6, p. 2023, 2023.

[16]. M. Gopalsamy, “Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection,” Int. J. Res. Anal. Rev., vol. 8, no. 1, pp. 187–193, 2021.

[17]. Ramesh Bishukarma, “Privacy-preserving based encryption techniques for securing data in cloud computing environments,” Int. J. Sci. Res. Arch., vol. 9, no. 2, pp. 1014–1025, Aug. 2023, doi: 10.30574/ijsra.2023.9.2.0441.

[18]. R. Bishukarma, “The Role of AI in Automated Testing and Monitoring in SaaS Environments,” Int. J. Res. Anal. Rev., vol. 8, no. 2, pp. 846–852, 2021, [Online]. Available: https://www.ijrar.org/papers/IJRAR21B2597.pdf

[19]. Suhag Pandya, “Innovative blockchain solutions for enhanced security and verifiability of academic credentials,” Int. J. Sci. Res. Arch., vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.

[20]. M. Gopalsamy, “Scalable Anomaly Detection Frameworks for Network Traffic Analysis in cybersecurity using Machine Learning Approaches,” Int. J. Curr. Eng. Technol., vol. 12, no. 06, pp. 549–558, 2022.

[21]. Ramesh Bishukarma, “Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 1308–1319, Jul. 2023, doi: 10.48175/IJARSCT-14000S.

[22]. S. C. -, “Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry,” Int. J. Multidiscip. Res., vol. 3, no. 4, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[23]. S. Cataldo Basile Leonardo Regano Candidate Francesco Settanni, “POLITECNICO DI TORINO Towards intelligence driven automated incident response,” 2022.

[24]. S. Theis, S. Jentzsch, F. Deligiannaki, C. Berro, A. P. Raulf, and C. Bruder, “Requirements for Explainability and Acceptance of Artificial Intelligence in Collaborative Work,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023. doi: 10.1007/978-3-031-35891-3_22.

[25]. I. Mustafa, L. Nahmatwlla, W. Ali Ahmed, and R. Saeed, “DEEP LEARNING EFFECTS ON IOT APPLICATIONS VIA CLOUD COMPUTING AND DISTRIBUTED SYSTEMS,” J. Biomech. Sci. Eng., vol. April 2023, pp. 95–116, 2023, doi: 10.17605/OSF.IO/HZ5TQ.

[26]. S. Tatineni, “AI-Infused Threat Detection and Incident Response in Cloud Security,” Int. J. Sci. Res., vol. 12, pp. 998–1004, 2023, doi: 10.21275/SR231113063646.

[27]. B. Boddu, “CLOUD DBA STRATEGIES FOR SQL AND NOSQL DATA MANAGEMENT FOR BUSINESS-CRITICAL APPLICATIONS,” https://ijcem.in/wp-content/uploads/CLOUDDBA-STRATEGIES-FOR-SQL-AND-NOSQL-DATA-MANAGEMENT-FOR-BUSINESS-CRITICAL-APPLICATIONS.pdf, vol. 7, no. 1, p. 8, 2022.

[28]. B. M. Harish Naik and J. Kannan, “A Research on Various Security Aware Mechanisms in Multi-Cloud Environment for Improving Data Security,” in 2nd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2023, 2023. doi: 10.1109/ICDCECE57866.2023.10151135.

[29]. R. Yue, G. Yang, P. Li, J. Xie, F. Jiao, and L. Zhan, “A Security Verification System Based on Bilinear Maps in the Multi-cloud Environment,” in 2023 4th International Conference on Computer Engineering and Intelligent Control, ICCEIC 2023, 2023. doi: 10.1109/ICCEIC60201.2023.10426646.

[30]. P. R. Shukla and V. M. Patil, “A Comprehensive Review of Frameworks for Achieving Interoperability in Multi-Cloud Environments,” in Proceedings of 2023 2nd International Conference on Informatics, ICI 2023, 2023. doi: 10.1109/ICI60088.2023.10421703.

[31]. M. H. Shirvani, “Web Service Composition in multi-cloud environment: A bi-objective genetic optimization algorithm,” in 2018 IEEE (SMC) International Conference on Innovations in Intelligent Systems and Applications, INISTA 2018, 2018. doi: 10.1109/INISTA.2018.8466267.

[32]. M. Allakonda and K. Sagar, “A Survey on data security challenges in multi cloud environment,” in Proceedings of CONECCT 2021: 7th IEEE International Conference on Electronics, Computing and Communication Technologies, 2021. doi: 10.1109/CONECCT52877.2021.9622722.