IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Survey on Various Privacy Preservation Techniques for Multi-cloud Environment

[1]Mitul Patel, [2]Mitul Raj
[1]Assistant Professor, [2]Assistant Professor
[1]School of Engineering,
[1]P P Savani University, Surat, India

Abstract : With the rapid adoption of cloud computing, organizations increasingly rely on multicloud environments to meet their diverse needs. Multicloud architectures offer numerous benefits, such as improved scalability, fault tolerance, and cost optimization. However, the distributed and interconnected nature of multiclouds introduces significant challenges in preserving user privacy and ensuring data confidentiality. This paper presents an overview of the key considerations and techniques for multicloud environments. Next, the paper explores various privacy-preserving techniques that can be employed in a multicloud environment. Finally, the paper presents the advantages and disadvantages of various privacy preservation techniques with respect to different type of cloud environments**.**

IndexTerms **– Multi-cloud, privacy-preservation, cloud computing.**

I. INTRODUCTION

Cloud computing refers to the delivery of computing services over the internet, enabling users to access and utilize a variety of resources and applications without the need for on-premises infrastructure. Instead of running software or storing data on local computers or servers, cloud computing allows users to access these resources remotely via the internet.
The concept of cloud computing encompasses a range of services, including:

Infrastructure as a Service (IaaS): This model provides virtualized computing resources, such as virtual machines, storage, and networks, which users can manage and control. Users have more flexibility and scalability compared to traditional physical infrastructure [2].

Platform as a Service (PaaS): PaaS offers a platform and environment for developers to build, deploy, and manage applications without worrying about the underlying infrastructure. It provides tools, development frameworks, and runtime environments [2].

Software as a Service (SaaS): With SaaS, users can access software applications hosted on the cloud without the need for local installation. The provider manages the infrastructure, security, and maintenance, while users focus on using the software [2].

Cloud computing offers several advantages, including:
Scalability [2]: Cloud services can easily scale up or down to accommodate changing demands. Users can provision additional resources as needed, ensuring efficient utilization and cost savings.

Cost savings [3]: By leveraging cloud resources, organizations can reduce the need for large upfront investments in hardware and infrastructure. Cloud services typically operate on a pay-as-you-go or subscription model, allowing users to pay only for the resources they use.

Flexibility and accessibility [2]: Cloud services can be accessed from anywhere with an internet connection, allowing users to work remotely and collaborate effectively. It enables seamless access to applications and data across multiple devices.

Reliability and redundancy [3]: Cloud providers often have redundant systems and data centers, ensuring high availability and reliability. They employ backup and disaster recovery mechanisms to minimize the risk of data loss or service disruptions.

Maintenance and updates [2]: Cloud service providers handle infrastructure maintenance, security patches, and software updates, relieving users of these tasks and allowing them to focus on their core business activities.

However, there are also considerations to keep in mind when using cloud computing, including data security, regulatory compliance, dependency on internet connectivity, and potential vendor lock-in. Organizations need to assess their specific requirements and choose appropriate cloud services and providers accordingly.

1.1Multicloud Environment

A multicloud environment refers to the use of multiple cloud computing platforms or providers to meet an organization's computing needs. Instead of relying on a single cloud provider, businesses can distribute their workloads across different cloud services, combining the strengths and capabilities of various providers.[3] In a multicloud environment, organizations may use different cloud providers for different purposes, such as running specific applications or workloads, leveraging specialized services, or achieving geographical redundancy and resilience. For example, a company might use one cloud provider for data storage and another for running virtual machines, depending on the specific requirements of each workload [3].

Benefits of a multicloud environment include:

Avoiding vendor lock-in [4]: By using multiple cloud providers, organizations can prevent being tied to a single vendor's technology stack or pricing structure. This provides flexibility and negotiation power.

Enhanced reliability and resilience [3]: Distributing workloads across multiple clouds allows businesses to achieve higher levels of redundancy and fault tolerance. If one cloud provider experiences an outage or service disruption, workloads can be seamlessly shifted to another provider to maintain service continuity.

Optimizing costs [4]: Different cloud providers offer varying pricing models and discounts. With a multicloud strategy, organizations can select the most cost-effective options for each workload or service, optimizing their cloud spending.

Leveraging specialized services [3]: Different cloud providers have unique strengths and offerings. By utilizing multiple providers, organizations can access specialized services and features that best fit their requirements, such as AI/ML capabilities, database services, or IoT platforms.

Geographical proximity and compliance [3]: Multicloud environments enable organizations to host their data and applications in different regions or countries to comply with specific data sovereignty regulations or reduce latency by being closer to end-users.

Multi-cloud environments can be categorized based on various criteria. Here are some common categories for classifying multi-cloud environments:

Public Cloud Multi-cloud [1]: This category involves using multiple public cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), to distribute workloads and services across different cloud providers.

Private Cloud Multi-cloud [1]: In this category, organizations maintain their own private cloud infrastructure and use multiple private cloud environments from different vendors or cloud software solutions, such as OpenStack or VMware, to achieve a multi-cloud setup.

Hybrid Cloud Multi-cloud [1]: Hybrid cloud refers to the combination of public and private cloud environments. A hybrid multi-cloud environment involves the use of multiple public cloud providers and private cloud deployments, either on-premises or hosted in a data center.

Multi-cloud for Disaster Recovery [2]: This category focuses on utilizing multiple cloud providers for disaster recovery purposes. Organizations replicate their data and applications across different cloud platforms to ensure business continuity in the event of a disaster or outage.

Multi-cloud for Data Sovereignty [2]: This category emphasizes compliance with data protection and privacy regulations by leveraging multiple cloud providers in different geographic regions. Data is stored and processed in specific regions or countries to meet local data sovereignty requirements.

Multi-cloud for Vendor Lock-in Avoidance [2]: This category aims to prevent vendor lock-in by using multiple cloud providers. Organizations distribute their workloads across different cloud platforms to avoid being dependent on a single provider and to maintain flexibility in terms of pricing, features, and services.

Multi-cloud for Best-of-Breed Services [3]: This category focuses on selecting the most suitable services and solutions from different cloud providers. Organizations choose specific cloud platforms for different use cases or applications, optimizing for the strengths and capabilities of each provider.

However, managing a multicloud environment also comes with challenges, such as increased complexity in governance, security, and workload management [4]. Organizations need to establish robust strategies, monitoring systems, and tools to effectively manage and integrate multiple cloud platforms while ensuring data security, interoperability, and seamless communication between different cloud services.

Overall, a multicloud environment offers flexibility, resilience, cost optimization, and access to a wide range of cloud services, enabling organizations to leverage the best capabilities from multiple cloud providers based on their specific needs and goals[5]. It highlights the importance of understanding the shared responsibility model between organizations and Cloud Service Providers to establish effective privacy protection measures.

3.2 Privacy preservation in a mulicloud environment

Privacy preservation in a multicloud environment is a crucial concern when it comes to safeguarding sensitive data and ensuring compliance with privacy regulations [5]. Multicloud refers to the use of multiple cloud service providers to host and manage different parts of an organization's infrastructure and data. Here are some key considerations for privacy preservation in a multicloud environment:
Data Classification [5]: Classify your data based on its sensitivity and regulatory requirements. This classification helps in determining the appropriate level of privacy protection for different types of data.

Encryption [6]: Implement strong encryption mechanisms to protect data both in transit and at rest. Encryption ensures that even if data is compromised, it remains unreadable without the appropriate decryption keys.

Access Controls [5]: Implement strict access controls to limit data access to authorized personnel only. Use strong authentication mechanisms, such as multi-factor authentication, and implement role-based access control (RBAC) to enforce granular access permissions.

Data Residency and Sovereignty [6]: Understand the data residency and sovereignty requirements imposed by relevant privacy regulations. Ensure that data is stored and processed in compliance with these requirements, particularly when dealing with cross-border data transfers.

Data Minimization [5]: Only store and process the minimum amount of data necessary for business purposes. Avoid collecting or retaining unnecessary personally identifiable information (PII) to minimize privacy risks.

Transparent Data Handling [5]: Maintain transparency regarding how data is handled, processed, and stored across different cloud providers. Understand the data protection practices and policies of each cloud service provider and ensure they align with your privacy requirements.

Data Portability and Vendor Lock-in [5,6]: Evaluate the data portability options provided by each cloud service provider. Being able to easily move data between different cloud providers can offer flexibility and reduce the risk of vendor lock-in.

Monitoring and Auditing [5]: Implement robust monitoring and auditing mechanisms to track data access, modifications, and transfers within the multicloud environment. Regularly review logs and conduct audits to identify any potential privacy breaches or vulnerabilities.

Contractual Agreements [6]: Establish clear contractual agreements with each cloud service provider that outline their responsibilities regarding data privacy and security. Ensure the agreements address areas such as data protection, breach notification, data handling, and compliance with privacy regulations.

Regular Assessments and Risk Management [5]: Conduct regular privacy assessments and risk management exercises to identify potential privacy risks within the multicloud environment. Stay updated with evolving privacy regulations and adapt your privacy preservation strategies accordingly.

It's important to note that privacy preservation is a comprehensive and ongoing process. It requires a combination of technical measures, organizational policies, and legal compliance to effectively protect privacy in a multicloud environment.
.

3.3 Advantages and Limitations of Privacy Preservation Techniques

The table outlines the advantages and limitations of each approach, emphasizing the need for a comprehensive privacy framework that combines multiple techniques to address different privacy concerns.

Table 1.1 Privacy Preservation Techniques for different types of clouds
1* - Public Cloud Multi-cloud,2* - Private Cloud Multi-cloud,3* - Hybrid Cloud Multi-cloud,4* - Muli-cloud for Disaster Recovery,5*-Multi-cloud for Data Sovereignty,6*-Multi-cloud for Vendor Lock-in Avodanace,7*-Multi-cloud for Best-of-Breed Services

Privacy Preservation Techniques			1*	2*	3*	4*	5*	6*	7*
Classification	Advantages	Enhanced Data Security [7]	Y	Y	Y	N	N	N	Y
		Regulatory Compliance [7]	Y	Y	Y	Y	Y	N	Y
		Efficient Resource Allocation [7]	Y	Y	Y	N	N	N	Y
		Data Lifecycle Management [8]	N	Y	Y	N	N	N	N
		Improved Data Governance [7]	Y	N	Y	N	Y	N	N
		Simplified Data Migration [8]	N	N	N	N	N	N	N
	Limitations	Lack of Standardization [8]	N	N	N	Y	N	Y	Y
		Interoperability Challenges [7]	N	Y	N	N	N	N	N
		Limited Visibility [7]	Y	Y	N	Y	Y	N	N
		Data Movement [7]	Y	Y	Y	Y	Y	N	Y
		Vendor Lock-in [7]	Y	Y	Y	Y	Y	Y	Y
		Regulatory Compliance [8]	Y	Y	N	Y	N	Y	N

Encryption	Advantages	Data Protection [9]	Y	N	Y	N	Y	N	Y
		Confidentiality [10]	N	Y	Y	Y	N	N	Y
		Compliance with Regulations [10]	Y	N	Y	Y	Y	Y	Y
		Control and Ownership [9]	N	Y	Y	N	N	Y	N
		Data Integrity [9]	Y	Y	Y	Y	Y	Y	N
		Flexibility and Interoperability [10]	Y	N	N	N	N	N	N
	Limitations	Key Management [10]	Y	N	Y	Y	Y	N	Y
		Interoperability [9]	N	Y	Y	Y	N	Y	N
		Data transfer [10]	Y	Y	Y	N	N	N	Y
		Compliance and regulatory requirements [10]	Y	Y	N	N	N	N	N
		Complexity and management overhead [9]	N	Y	Y	Y	Y	Y	Y
Access Controls	Advantages	Security [11]	Y	N	Y	Y	Y	Y	N
		Compliance [11]	Y	Y	N	Y	Y	N	Y
		Granular Control [12]	Y	N	N	N	N	N	N
		Centralized Management [11]	N	Y	Y	N	Y	Y	Y
		Flexibility and Scalability	N	Y	N	Y	N	N	N
		Auditing and Accountability [11]	Y	N	Y	Y	Y	Y	Y
	Limitations	Vendor-specific access controls [11]	Y	Y	N	N	Y	N	Y
		Lack of standardized access control protocols [12]	N	Y	Y	Y	N	Y	Y
		Limited visibility and control [12]	Y	N	N	N	N	N	Y
		Identity and authentication challenges [11]	N	Y	Y	Y	Y	Y	Y
		Synchronization and coordination issues [11]	Y	Y	Y	N	Y	N	N
		Compliance and regulatory considerations [12]	Y	N	N	Y	N	Y	N
		Complexity in authorization and entitlements [11]	N	Y	N	N	N	Y	N
Data Residency and Sovereignty	Advantages	Compliance with local regulations [13]	N	Y	Y	Y	Y	N	Y
		Enhanced data privacy and security	N	Y	Y	Y	Y	N	N
		Improved performance and latency [13]	Y	N	N	N	Y	Y	Y
		Data sovereignty and intellectual property protection [14]	Y	N	Y	Y	N	N	N
		Business continuity and disaster recovery [14]	Y	Y	Y	N	N	Y	Y
		Flexibility and vendor lock-in avoidance [14]	Y	Y	N	Y	N	N	N
	Limitations	Jurisdictional Regulations [14]	N	N	Y	N	Y	Y	Y
		Cloud Service Provider Policies [13]	N	Y	N	Y	Y	N	N
		Data Transfer and Cross-Border Issues [14]	Y	Y	Y	N	Y	Y	Y
		Data Protection Mechanisms [14]	Y	N	Y	Y	N	N	Y
		Compliance and Governance [13]	Y	Y	N	Y	N	Y	Y
		Vendor Selection [13]	N	N	Y	Y	N	N	N
		Data Classification and Lifecycle Management [14]	N	Y	Y	N	Y	Y	N
Data Minimization	Advantages	Privacy and Compliance [15]	Y	N	N	N	Y	N	Y
		Reduced Attack Surface [16]	Y	Y	Y	Y	N	Y	N
		Cost Optimization [16]	Y	Y	N	Y	N	N	Y
		Enhanced Data Management [15]	N	N	Y	N	N	Y	Y
		Improved Performance [16]	N	Y	N	N	Y	N	N
		Simplified Data Subject Rights [16]	Y	Y	Y	Y	Y	Y	N
	Limitations	Data redundancy [15]	Y	Y	N	N	Y	N	Y
		Data movement [16]	Y	N	Y	Y	Y	Y	N
		Lack of control [15]	Y	Y	N	Y	N	N	Y
		Compliance challenges [15]	Y	Y	Y	Y	N	Y	N
		Integration complexity [15]	N	N	Y	Y	N	N	Y
Transparent Data Handling	Advantages	Data Portability [17]	N	Y	Y	N	Y	Y	Y
		Redundancy and Resilience	N	Y	Y	N	N	N	N
		Cost Optimization [17]	Y	N	N	Y	Y	Y	Y
		Compliance and Data Sovereignty [18]	Y	Y	Y	Y	N	N	Y
		Performance and Scalability [18]	N	N	Y	N	Y	Y	N
		Enhanced Security and Data Protection [17]	Y	Y	N	N	Y	N	N
	Limitations	Data Governance [18]	N	Y	Y	Y	N	Y	Y
		Data Visibility [17]	N	Y	Y	Y	N	Y	Y
		Data Movement and Integration [18]	Y	N	N	N	Y	N	Y
		Compliance and Regulatory Issues [18]	N	Y	Y	N	Y	N	N
		Vendor Lock-In [17]	Y	N	Y	Y	N	N	N
		Security and Data Protection [17]	N	Y	N	Y	N	Y	Y

Data Portability and Vendor Lock-in	Advantages	Flexibility [19]	N	Y	Y	Y	Y	Y	N
		Cost optimization [19]	Y	Y	Y	N	N	Y	Y
		Risk mitigation [19]	Y	N	N	Y	Y	N	Y
		Negotiating power [20]	Y	Y	Y	N	N	N	Y
		Innovation and agility [20]	N	Y	Y	N	Y	N	N
		Continuity and resilience [20]	Y	N	N	Y	N	Y	N
		Exit strategy [19]	Y	Y	Y	N	Y	Y	N
	Limitations	Data Formats [20]	N	Y	Y	Y	N	Y	Y
		Interoperability [20]	Y	Y	Y	Y	Y	N	N
		Service Dependencies [20]	Y	Y	N	N	N	N	Y
		Service Integration [20]	Y	N	Y	N	Y	N	N
		Data Gravity [20]	Y	Y	N	Y	Y	Y	Y
		Training and Expertise [20]	N	N	N	Y	N	Y	Y
Monitoring and Auditing	Advantages	Centralized Visibility [21]	Y	Y	Y	N	N	N	N
		Performance Optimization	Y	Y	Y	N	N	Y	Y
		Cost Optimization [21]	Y	N	N	Y	Y	Y	N
		Compliance and Security [22]	Y	Y	Y	Y	Y	N	N
		Proactive Issue Detection [22]	Y	N	N	N	Y	Y	Y
		Capacity Planning and Scalability [21]	N	Y	Y	N	Y	N	N
		Vendor Management [22]	N	Y	N	Y	N	Y	Y
	Limitations	Lack of centralized visibility [22]	Y	N	Y	Y	N	N	N
		Inconsistent monitoring capabilities [22]	Y	Y	N	N	Y	Y	Y
		Data integration and correlation [21]	Y	Y	N	Y	Y	N	N
		Limited interoperability [21]	Y	N	N	N	N	Y	Y
		Compliance and governance challenges [22]	Y	Y	Y	Y	Y	N	N
		Cost implications [22]	Y	Y	Y	N	N	Y	Y
		Security considerations [22]	Y	Y	N	Y	Y	N	Y
		Complexity of data analysis [21]	N	Y	N	Y	N	Y	Y
Contractual Agreements	Advantages	Service Level Agreements (SLAs)[23]	N	Y	Y	Y	Y	N	Y
		Flexibility and Scalability	N	N	N	N	Y	Y	N
		Cost Optimization	N	Y	Y	N	Y	Y	N
		Risk Mitigation [23]	Y	Y	N	Y	Y	Y	N
		Vendor Lock-In Avoidance [24]	N	N	Y	Y	N	N	Y
		Governance and Performance Monitoring [24]	N	Y	N	N	N	N	N
	Limitations	Vendor-specific terms and conditions [23]	Y	N	Y	Y	N	N	Y
		Lack of standardization [23]	Y	Y	N	N	N	Y	Y
		Data sovereignty and compliance [24]	Y	Y	Y	Y	Y	Y	Y
		Service-level agreements (SLAs) [24]	N	N	N	Y	N	N	Y
		Interoperability and integration [24]	Y	Y	Y	Y	Y	Y	Y
		Vendor lock-in [23]	Y	Y	Y	N	Y	N	N
		Complexity and management overhead [23]	Y	N	Y	N	N	Y	N
Regular Assessments and Risk Management	Advantages	Enhanced Security [25]	N	Y	N	Y	N	N	N
		Compliance with Regulations [26]	N	N	Y	Y	N	Y	N
		Optimal Resource Allocation [25]	Y	Y	Y	Y	Y	N	N
		Business Continuity and Disaster Recovery [26]	Y	Y	N	N	N	Y	Y
		Vendor Risk Management [25]	N	Y	Y	N	Y	N	Y
		Proactive Issue Identification and Mitigation [26]	Y	N	Y	N	N	Y	Y
		Continuous Improvement [26]	N	Y	Y	N	Y	N	Y
	Limitations	Lack of Standardization [26]	Y	Y	N	Y	N	Y	N
		Complexity and Scale [25]	N	N	Y	Y	Y	N	N
		Limited Visibility [26]	Y	N	Y	Y	N	Y	N
		Integration Challenges [25]	N	Y	Y	N	Y	N	N
		Regulatory Compliance [25]	Y	N	N	N	N	Y	N
		Vendor Lock-in [25]	N	Y	Y	N	Y	N	N
		Skill and Resource Gaps [26]	N	N	Y	Y	Y	Y	Y

II. CONCLUSION

In conclusion, privacy preservation in multicloud environments presents significant challenges due to the distributed nature of the cloud infrastructure. This paper provides a high-level overview of the key considerations, techniques, and future directions for protecting user privacy and ensuring data confidentiality in multicloud environments.As every techniques comes with their pros and cons for different cloud environments,it requires a holistic approach that combines encryption, access control, anonymization, secure computation, auditing, and privacy-preserving machine learning to establish robust privacy frameworks in multicloud architectures.

REFERENCES

[1] Zhang, Q., Cheng, L. & Boutaba, R. Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1, 7–18 (2010).

[2] abrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020)

[3] Paul, J.J. (2023). Multicloud Architectures. In: Distributed Serverless Architectures on AWS. Apress, Berkeley, CA.

[4] Li, J., Zhu, S. Service composition considering energy consumption of users and transferring files in a multicloud environment. J Cloud Comp 12, 43 (2023). https://doi.org/10.1186/s13677-023-00423-9

[5] Wang, Q., Ren, K., Wang, C., Lou, W., & Li, J. (2013). Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22(5), 847-859.

[6] Kumar, R., & Latha, M. M. (2014). Secure multi-cloud data storage using hybrid encryption technique. International Journal of Computer Science and Mobile Computing, 3(9), 621-629.

[7] Gupta, S., & Babu, S. M. (2016). A novel secure multi-cloud storage architecture with load balancing. International Journal of Advanced Research in Computer Science, 7(7), 203-209.

[8] Wang, S., Wang, C., Li, J., Ren, K., & Lou, W. (2019). Privacy-preserving outsourced computation for multiple users in cloud computing. IEEE Transactions on Dependable and Secure Computing, 16(4), 578-591.

[9] Rawat, N., & Kaur, K. (2018). A secure multi-cloud data storage using multi-keyword search and proxy re-encryption. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 73-77). IEEE.

[10] Bhatia, S., & Rani, P. (2019). Privacy-preserving multi-cloud storage using attribute-based encryption. In 2019 International Conference on Sustainable Energy, Electronics, and Computing Systems (SEECOM) (pp. 315-318). IEEE.

[11] Liu, H., Liu, J., Xiang, Y., Liu, R., & Liu, X. (2019). Privacy-preserving encrypted big data sharing scheme in multi-cloud storage environment. IEEE Transactions on Cloud Computing, 7(4), 1100-1112.

[12] Chen, J., Lin, X., & Niu, B. (2020). A privacy-preserving dynamic searchable encryption scheme for multi-cloud storage. Future Generation Computer Systems, 103, 1-10.

[13] Guo, S., Guo, H., Hu, X., Li, Z., & Dong, W. (2020). Privacy-preserving federated learning with enhanced model efficiency and data security for cloud-based IoT. IEEE Internet of Things Journal, 8(12), 9720-9730.

[14] Zhang, H., Wang, H., & Qin, Z. (2020). Privacy-preserving multi-cloud storage auditing with attribute-based searchable encryption. IEEE Transactions on Services Computing, 13(2), 278-291.

[15] Su, J., Yang, J., Huang, X., Cui, L., & Yang, L. T. (2020). Efficient privacy-preserving multi-cloud storage auditing scheme with verifiable delegation. IEEE Transactions on Information Forensics and Security, 15, 781-793.

[16] Zhang, R., Liu, Q., Jiang, J., & Xie, Y. (2014). A novel privacy-preserving data outsourcing scheme based on multi-cloud. Future Generation Computer Systems, 36, 354-362.

[17] Wang, X., Sun, X., Cao, G., Li, Y., & Liang, H. (2014). An efficient privacy-preserving ranked keyword search method in the multi-cloud environment. Journal of Network and Computer Applications, 42, 118-127.

[18] Zhang, Y., Guo, H., Qin, B., & Zhang, Y. (2016). Privacy-preserving and efficient multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 27(6), 1719-1732.

[19] Bhatia, S., & Rani, P. (2019). Privacy-preserving multi-cloud storage using attribute-based encryption. In 2019 International Conference on Sustainable Energy, Electronics, and Computing Systems (SEECOM) (pp. 315-318). IEEE.

[20] Bansal, M., & Rani, P. (2020). Secure multi-cloud storage using proxy re-encryption and searchable encryption. In 2020 International Conference on Innovative Trends in Computer Engineering (ITCE) (pp. 1-6). IEEE.

[21] Goyal, A., & Khurana, S. (2020). Privacy-preserving multi-cloud data storage using homomorphic encryption. In 2020 3rd International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 423-428). IEEE.

[22] Rani, M., & Juneja, D. (2021). Secure multi-cloud data storage using hybrid encryption technique. In 2021 International Conference on Sustainable Computing and Intelligent Systems (ICSCIS) (pp. 1199-1204). IEEE.

[23] Wang, X., Yao, X., Xu, L., Liu, Y., & Liang, X. (2023). Privacy-preserving multi-cloud storage with ciphertext conversion and dynamic user access control. Journal of Supercomputing, 79(3), 2314-2334.

[24] Chen, Z., Shen, L., & Sun, S. (2023). Privacy-preserving multi-cloud data sharing and access control using blockchain. IEEE Transactions on Services Computing. Advance online publication. doi: 10.1109/TSC.2023.3149687.

[25] R. Nagarajan, P. Raj, and R. Thirunavukarasu, Eds., "Operationalizing Multi-Cloud Environments," EAI/Springer Innovations in Communication and Computing, 2022, doi: 10.1007/978-3-030-74402-1.

[26] J. Alonso et al., "Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review," Journal of Cloud Computing, vol. 12, no. 1, Jan. 2023, doi: 10.1186/s13677-022-00367-6.