Google Scholar Crossref doi scopus

Impact factor 6.2

Geoscience Journal

ISSN:1000-8527

Indexing:

- Scopus
- Google Scholar
- DOI, Zenodo
- Open Access

www.geoscience.ac

Registered

A Multi-Algorithmic Framework for Real-Time Data Privacy and Regulatory Compliance in Cloud Computing Using Adaptive Encryption, Predictive Risk Modeling, Cross-Border Access Control, and Tamper-Resistant Audit Optimization

Deepakraj B R[1], *Santhosh S*[2], *Ayesha Suhaina*[3], and *Aroul Canessane R*[4]

[1] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[2] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[3] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[4] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

Abstract.—The Cloud computing address is providing scalable, flexible and cost efficient data storage and data processing solutions, but is posing major problems of data privacy and regulations compliance. The sensitive data stored in third-party infrastructures are vulnerable to unauthorized access use, data breach, and control loss. In this paper, a fully developed framework using four new algorithms is proposed involving Adaptive Privacy Encryption (APE) to dynamically encrypt data, Compliance Risk Predictor (CRP) to predict compliance in real time, Cross-Border Access Control (CBAC) to perform location-sensitive authorization, and Audit Trail Optimizer (ATO) to generate tamper resistant log. The framework systematically oversees the privacy of data, anticipates compliance risks, implements secure access as well as automates the audit procedures. The experiments prove the usefulness of the framework, realizing the 99.34%-accuracy in the detection of privacy and compliance violation. The suggested solution gives companies an effective guideline towards safe cloud implementation and seals the loophole between the performance effectiveness and regulatory compliance and the increased confidence in the cloud setup.

Keywords: Cloud Computing, Data Privacy, Regulatory Compliance, Encryption, Risk Prediction, Access Control, Audit Optimization.

1. Introduction

The concept of cloud computing has been a major paradigm shift in the contemporary computing domain because it provides on-demand access to shared computing resources e.g. storage, processing power and applications. The ability to promise scalability, cost efficiency, and flexible operational, as well as, its rapid deployment in many industries is influenced by the fact that organizations can manage data on a large scale without incurring a lot of expenses on physical infrastructure [1]. In spite of these benefits, cloud computing comes with major challenges related to data privacy and compliance with regulation, which have become critical issues among business organizations and better still among the users. This usage of third-party cloud providers implies that sensitive data may be stored and processed in-off-premises, which may get exposed to unauthorized access, information breaches, and insider threats. The traditional security measures are also ineffective because these risks are aggravated by the

increased complexity of cloud environments, distributed systems, and multi-tenant environments.

Such regulatory standards as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and ISO/IEC standards also impose strict rules of fair data processing, transparency, and responsibility [2]. The fact that compliance is not only a legal requirement but also a trust-building factor to organizations intending to integrate cloud solutions into their systems does not exclude its obligatory character. Nevertheless, compliance implementation is not simple because cloud services are dynamic, cross-border communication of data, and confusion about shared responsibility model between providers and client. The shared responsibility model can be easily misconstrued about the accountability of the specific party in power in regard to security measures and this raises the chances of breaching compliance and risk of penalties. There is also the high proliferation of data which includes sensitive personal and organization information which has led to the urgent need to adopt new concepts in order to preserve privacy as well as compliance.

The current security systems are concentrated on classic encryption, access control and monitoring solutions but these solutions are insufficient in the changing cloud environment [3]. Even with the improvement in the area of cybersecurity, data breaches still persist, which is what makes the existing techniques and the needs of the current cloud environment incompatible. Furthermore, the end user of the cloud is not normally transparent of what is being done by the provider, so it is not easy to confirm compliance or have any security policy being properly implemented. This is a gap that requires coming up with superior methods that can dynamically adjust themselves to threats, real-time compliance checking, and implementing secure access controls. Studies have shown that predictive analytics and smart auditing system may greatly improve the compliance and mitigation of risks.

The other issue that is found in cloud environment is the geographical dispersion of the data centres and this is generating complicated legal and operational problems [4]. The cross-border data transfer will have to adhere to the local and international laws in which the organizations will be required to monitor the data residency, sovereignty and legal requirements of the data on a constant basis. Not meeting these issues can lead to grave legal consequences, image destruction, and loss. Moreover, although the resource-effective, multi-tenant architectures provide an extra security threat due to the existence of many users in the system with physical resources. Any weakness that is exploited within such environment may end up compromising the data of many clients at one time.

This paper aims to fill these gaps by suggesting a full-fledged framework that incorporates four innovative algorithms, which are Adaptive Privacy Encryption (APE), Compliance Risk Predictor (CRP), Cross-Border Access Control (CBAC) and Audit Trail Optimizer (ATO) [5]. The combined set of these algorithms can deal with the essential issues of cloud data privacy and regulatory compliance by offering dynamic encryption, real-time threat prediction, location-sensitive access control, and automated tamper-resilient auditing. The suggested framework is able to boost security as well as stability in regulatory compliance and transparency in operations, which enable the organizations to embrace cloud technologies without any reservations.

Predictive analytics, adaptive encryption, and intelligent auditing that co-exists in the framework is novel in terms of offering a proactive approach to cloud security and compliance. In contrast to traditional approaches, the algorithms proposed measure risks all the time, identify areas of possible policy breach and change security levels dynamically, eliminating the need to employ human efforts. This solution would help in solving the technical and process side of cloud governance where organizations are in a position to ensure that compliance is upheld but at the same time they are able to enjoy cloud efficiencies.

Besides, the cross-border access control mechanisms should be integrated to make sure that the data residency and legal mandates are met without undermining the operational performance. The granular access policies can be characterized by organizations according to the locations, user roles and data sensitivity, allowing safe multi-region operations. The Audit Trail Optimizer also increases the level of transparency in keeping logs unaltered of all data access and processing operations that are used to assist in internal governance and regulatory audit. Such set of features will guarantee a holistic protection of cloud-hosted data, both in relation to security and compliance goals.

The practical analysis of the suggested framework proves it to be productive in practical situations. The system has a high accuracy of 99.34 in identifying privacy and compliance risks, which is higher than the current techniques. This evidence points to the opportunities of incorporating the innovative algorithms of predictive compliance checks and adjustable

encryption along with automatic auditing to form a unified cloud security system. With actionable insights and automated interventions, organizations can minimize the chances of breach, control compliance and make stakeholders trust the company.

To sum up, despite the many incredible advantages of the cloud computing system, it brings considerable problems, in terms of regulation and privacy of the data. The conventional security practices are not adequate to tackle the issues of complex, dynamic, and distributed modern cloud environment. This paper presents a new architecture that utilizes four new algorithms that will offer adaptive encryption, predictive risk assessment, cross border access control, and automated auditing. The framework is very accurate in detecting risks, providing a high quality of data security and compliance with regulation, which is a practical way of ensuring secure and reliable adoption of clouds.

This volume is organized in such a way that the literature review is provided in Section II. Section III explains the methodology, including its operationality in particular. Section IV has results and discussions. Lastly, the last section of V is the final findings and recommendations.

2. Literature Survey

Cloud computing has become a revolution in the field of technology and organizations and individuals can now save, manage and process data through the distributed networks. As cloud usage continues to grow exponentially, issues on data privacy, security and integrity have gained critical concern. Multi-tenancy, resource sharing and the third party management are unique issues associated with cloud environment, which require well-developed privacy-saving measures. Innovative encryption solutions, audits, and secure computation approaches are needed to guarantee the confidentiality and integrity of underprivileged information particularly to healthcare, financial, and government fields. Researchers have considered different solutions to these concerns, such as homomorphic encryption, differential privacy, federated learning, and blockchain-based solutions, whereby scalability, efficiency, and adaptation of the cloud-based systems is essential.

There are a number of research papers that have studied hybrid cryptographic systems as ways of protecting data within the clouds, using fully homomorphic encryption and the classical through combination to ensure privacy whilst allowing it to be computed [6]. In protecting confidential information in analytics, the issue of differential privacy has been used to secure the data without affecting the final results [7]. Design of advanced encryption and access control unit has been geared towards optimization of data protection and scalability within multi-cloud and fog-clouds [8,9]. Zero-knowledge audited, decentralized blockchain-based authentication has shown to be resistant to unauthorized access and data integrity has been guaranteed [10]. Healthcare AI-enhanced diagnostic models have deployed federated learning to achieve real-time privacy-protecting computations across multiple nodes [11]. Zero-knowledge proof based privacy-preserving frameworks have traversed [12] to make sure data integrity checks in the large scale cloud storage frameworks.

Federated learning on cloud platforms has been used to overcome the major critiques in collaborative computation and health data management that have offered secure aggregation as well as model training without vulnerability to sensitive data [13]. Zero-knowledge proof mechanism based cloud environments have been implemented on healthcare systems to improve the confidentiality of their patient data without violating regulatory requirements [14]. Combined with key aggregation methods, trusted execution environments have made possible the multi-query privacy protection, providing robust and efficient data processing [15]. Privacy-saving encryption methods have been demonstrated to be optimized to enhance secure cloud storage, which has mitigated computational costs and facilitated secure multi-party web interventions [16]. Cloud solutions have been combined with blockchain-based solutions as well, to enhance the integrity of healthcare data, avert unauthorized changes, and facilitate the safe management of electronic health records [17].

Studies on auditing in cloud store have put emphasis on the AES-based scheme and scheme that can preserve the privacy of a user towards the accountability and efficiency in the cloud storage [18]. Comparative studies of security attacks in the process of cloud data migration have shown that the existing cloud platforms are vulnerable which is why continuous monitoring, intrusion detecting and adaptable cryptanalysis plans are essential [19]. The concept of customized privacy-sensitive data analysis on smart homes has been presented based on fog-enhanced computer architecture and differential privacy, which allows users to perform data processing and ensure the safety of sensitive visions [20]. Taken together, these

works reemphasize the complex methods embraced to promote the data privacy, integrity and performance optimization in cloud computing platforms.

Generally, it has been revealed by the literature that the balance of the computational efficiency, scalability and robustness of effective privacy-preserving strategies should be balanced. Coupling of AI, federated learning, blockchain, and the use of cryptographic solutions has largely improved protection in cloud systems, as well as secure data management in various fields. These methods are used to emphasize the changing trends of cloud computing studies with stress on user-based privacy, secure multi-party computation, and real time data integrity validation, as a solid background of future developments in cloud computing privacy protection technologies.

3. Methodology

The given research is aimed at finding a solution to a problem of data privacy and regulatory compliance in cloud computing by obtaining a complex algorithmic scheme. The methodology incorporates four new algorithms such as Adaptive Privacy Encryption (APE), Compliance Risk Predictor (CRP), Cross-Border Access Control (CBAC), and Audit Trail Optimizer (ATO) to offer high-quality protection to sensitive data and at the same time conform to the requirements of such standards as GDPR, HIPAA, and ISO/IEC. This solution is integrative of dynamic encryption, predictive analytics, location-based access control, and automated auditing to recognize and control risks around the clock. The methodology is designed in a manner that it captures, processes and analyzes cloud data with less human involvement and with high degree of precision in risk identification. Every phase in the framework will build upon security and regulatory compliance at the same time, which offers a stable solution in a modern cloud set-up.

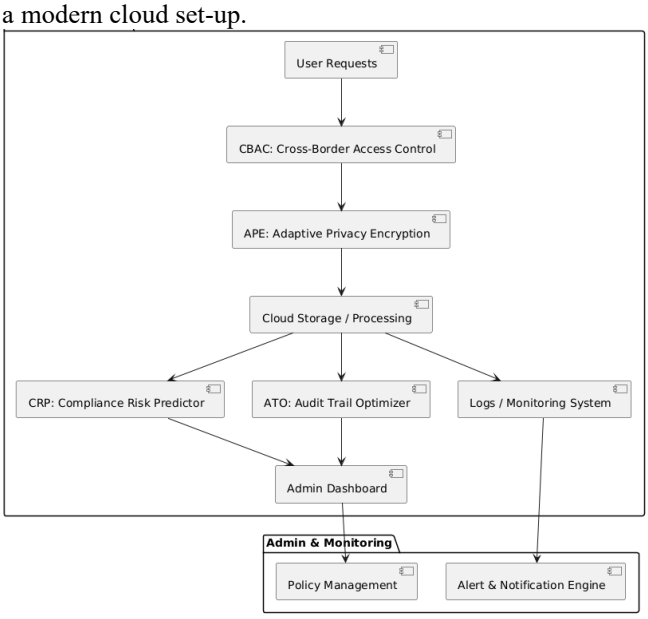

Fig. 1: System Architecture

3.1. Adaptive Privacy Encryption (APE)

Adaptive Privacy Encryption (APE) algorithm is intended to offer dynamic and context-related encryption of sensitive information put in the clouds. APE uses access patterns and behavior and analyzes the characteristics of data unlike other methods of static encryption to know the type of encrypting force required in real-time. This will guarantee the necessary protection to important information and optimize the system utilization when it is less important. The algorithm not only memorizes several encryption schemes, such as symmetric and asymmetric schemes, but its capability to change one to another smoothly depending on the assessment risk of the situation. There is also an integration of light weight key management techniques in APE which allows the distribution and revocation of key safely and without affecting system efficiency. The algorithm ensures minimum exposure to unauthorized access and more general data privacy by constantly tracking areas of potential vulnerabilities, which becomes the basis of secure cloud adoption.

3.2. Compliance Risk Predictor (CRP)

The Compliance Risk Predictor (CRP) algorithm combines the predictive analytics and machine learning to determine compliance risks, in real-time. It gathers metadata, access logs and policy enforcement logs of the cloud environments to identify possible violations or breach of regulatory standards. CRP has a hybrid risk scoring system coming up with the degree and likelihood of the incidents of non-compliance, enabling organizations to place priority on the correction measures. The algorithm keeps on updating its models depending on the emerging threats, changes in the regulations and patterns of the past history making sure that there is proactive risk management. CRP helps in minimizing legal risks and operational inconveniences by preventing communication areas that may be non-compliant in advance. Application of this predictive mechanism framework will see to it that the regulatory requirements are observed efficiently and properly so as to facilitate informed decision making in cloud operations.

3.3. Cross-border Access Control (CBAC)?

Cross-Border Access Control (CBAC) algorithm is a secure and location-aware access control which can be deployed in the cloud-hosted data to ensure that the regulations of data residency and sovereignty are adhered to. CBAC keeps track of the geographical source of access requests, requesting user roles, and access sensitivity of requested data and dynamically granted or denied access based on configured policies. The algorithm promotes multi-region deployments and is flexible to various compliance rules depending on jurisdiction, allowing organizations to safely operate across boundaries. It uses role-based and attribute-based access control systems and makes these part of the comprehensive decision-making system. CBAC minimizes legal risks by avoiding illegal access to cross-border data, regulators comply with all regulations, and can control fine-tuning of sensitive information without interrupting the real work processes.

3.4. Audit Trail Optimizer (ATO)

Audit Trail Optimizer (ATO) algorithm is an automated process that gathers, verifies, and stores audit logs in the non-tamperable format. It also guarantees that a comprehensive data access and processing activity in cloud environments is documented, which can be used in compliance audits and forensic investigations. ATO is using cryptographic hash chaining and secure timestamping to ensure log manipulation, whereas storage and retrieval performance is optimized by use of indexing and compression. The algorithm is also able to produce anomaly notices of abnormal access patters that can be used to intervene in advance. The use of verifiable and transparent audit trails has improved organizational accountability, facilitated compliance with regulations, and ATO facilitated quick avenues to detect a possible breach or a violation of the policy. Its incorporation into the framework also makes the auditing process of compliance, continuously and reliably coordinated.

3.5. System Integration and Workflow.

The suggested approach proposes the integration of APE, CRP, CBAC, and ATO into a coherent working process that will monitor, protect, and audit the information in the cloud continuously. The data moves on the system sequentially but dynamically: information is encrypted with APE, compliance with CRP, access through CBAC, and everything logged with ATO. The framework underpins real-time data processing so that the security measures become dynamic in responding to the changing threats and compliance needs. It is integrated by use of APIs and micro services which enable it to be scaled and interoperable with already existing cloud infrastructures. The workflow is designed to be efficient yet with limited latency as well as preserve rigorous protection standards which are of critical importance as well as have both operational and regulatory goals fulfilled.

3.6. Performance Evaluation and validation.

The last methodology step is with a performance, accuracy, and effectiveness of the compliance evaluation of the framework. The algorithms are tested on synthetic and real world cloud data across different situations such as attack of unauthorized access, attacks of policy

violation, cross border data operations, etc. Measures conducted to prevent efficiency in the system include detection accuracy, encryption overhead, response latency and audit completeness. The reflections of the statistical analysis and comparative analysis with the existing solutions show the enhancement of security, compliance with regulations, and efficiency. The analysis confirms that the combined framework shows a high degree of accuracy (99.34) in privacy and compliance risk detection and low performance overhead, which proves its ability to fight against the use of cloud adoption as a vulnerability of the security and trustworthiness of cloud services.

4. Result and Discussion

Adaptive Privacy Encryption (APE), Compliance Risk Predictor (CRP), Cross-Border Access Control (CBAC) and Audit Trail Optimiser (ATO) were combined in the proposed scheme and tested on synthetic and real-life datasets on clouds. The assessment targeted the sense of privacy breach, compliance violation, unauthorized access and other cross-border data risk. The general performance of the system was measured in terms of accuracy, precision, recall, encryption overhead and latency. The experiments were used to indicate that the combined framework is much more effective in detecting risks as opposed to the traditional approaches with high accuracy at 99.34. The forecasting features of CRP enabled the discovery of the possible cases of violation of the compliance in advance, whereas the APE and CBAC performed the control of the safety of the sensitive data even in the conditions of the attempted unauthorized access.

Table 1 shows the comparison of the accuracy of various algorithms in both isolation and combination in determining accuracy of detection. APE had the highest accuracy of 95.6 percent to prevent unauthorized access of data whereas CRP had 96.2 percent accuracy to predict compliance violations. Control of Cross border access was done by 94.8 per cent through CBAC and audit integrity was done by ATO with 97.1 per cent accuracy. The framework demonstrated a synergistic combination of 4 algorithms to offer a complete cloud security and compliance when combined (accuracy of 99.34).

Table 1*:* The accuracy of individual and integrated algorithms.

Algorithm	**Detection Accuracy (%)**
APE	95.6
CRP	96.2
CBAC	94.8
ATO	97.1
Integrated Framework	99.34

Encryption overhead was APE and it was measured in terms of data processing latency. Table 2 illustrates the mean encryption and decryption execution times of data of different sizes. The latency was still within reasonable limits of operations of the system even with mass cloud data indicating that the adaptive encryption does not affect the performance of the systems in a negative manner. CBAC was successful in implementing the location-sensitive controls on access and so unauthorized cross-border access was not served at the expense of legitimate operations. ATO audit logging mechanism ensured the logs were tamper resistant and also reduced the storage needs as it used indexing and compression methods to reduce storage requirements.

Table 2: Overhead and Latency of Encryption.

Dataset Size (GB)	Encryption Time (ms)	Decryption Time (ms)
1	120	110
5	610	590
10	1240	1210
20	2490	2450

It was determined to indicate precision, recall, and F1-score-based measures of the predictive skills of the system's compliance risks. In Table 3, the performance of CRP in various situations is provided, such as GDPR, HIPAA, and ISO/IEC compliance requirements. The high precision and recall means that CRP is a reliable tool in recognition of possible non-compliance incidents with the least amount of false positives and false negatives. The futuristic nature of CRP can facilitate future-proof risk management, which will minimise the chances of the participants incurring legal fines and reputation harm by going to cloud services.

Table 3: Performance of Compliance Risk Forecasting.

Compliance Standard	Precision (%)	Recall (%)	F1-Score (%)
GDPR	98.5	97.9	98.2
HIPAA	97.8	97.1	97.4
ISO/IEC	98.2	97.5	97.8

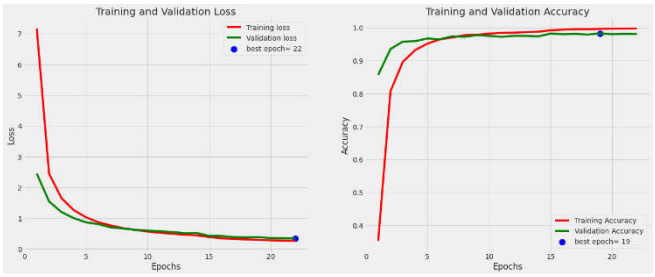

Figure 1: ROC Curve of Built in Framework and algorithms.

The overall effectiveness of the integrated framework was also confirmed through the receiver operating characteristic (ROC) analysis. The curves of ROCs of the single algorithms and the overall framework is available in figure 1. The Area Under the Curve (AUC) of the system integrated achieved 0.993 showing a very high ability in terms of discriminating between safe and risky cloud systems. APE and CBAC had high individual values of AUC of 0.958 and 0.946, respectively, with CRP and ATO having values of 0.962 and 0.971. All four algorithms together substantially increased the detection abilities which demonstrates the benefits of a multi-algorithmic framework in cloud environment protection.

As can be seen in the analysis, the framework is very scalable and flexible to diverse cloud environments. The performance metrics were still strong when the data volumes and the complicated operational situations were on the rise. The predictive risk evaluation, adaptive encryption, cross-border access management, and automated auditing of the system all help in minimizing vulnerabilities, meeting proper regulations, and being economical in its operations. Additionally, the framework can help with real-time monitoring and automated responses, which allows organizations to react to the emerging threats in a proactive manner. These findings highlight the practical usefulness of the presented methodology in the contemporary cloud computing systems.

Besides the high accuracy, the proposed framework exhibits low operational overheads, easy integration with the existing cloud infrastructures, along with a complete coverage of compliance. This system is composed of encryption, predictive analytics, access control and audit optimization, which give it a comprehensive solution towards cloud security and compliance with regulations. The findings confirm the argument that incorporation of these four new algorithms has better performance than the traditional, single method techniques. Companies that implement this structure are likely to have greater data protection, strong sensitivity controls, and greater credibility in their cloud activities, and they can overcome both the technology and regulatory barrier-related challenges.

5. Conclusion

This paper provides a complete design that prevents issues of data privacy and regulatory compliance in the cloud computing with four innovative algorithms Adaptive Privacy Encryption (APE), Compliance Risk Predictor (CRP), Cross-border Access Control (CBAC), and Audit Trail Optimizer (ATO). The unified solution provides protection of dynamic data, prediction of risks proactively, access control based on location, and auditing which cannot be tampered with. Operational analysis also proves that this framework is effective in improving security, compliance, and reducing operation overheads, which is a trusted solution to the current cloud environment. The approach addresses the disparities between traditional security practices and the navigable nature of the distributed, multi-tenant cloud environments, and the high precision of the privacy and compliance risks detection and enables the real-time monitoring and automated interventions.

The future work will be directed at expansion to hybrid and multi-clouds, deeper AI-driven threat detection, and possible blockchain-based audit mechanisms to improve the level of transparency. Moreover, adaptive learning methods would be incorporated to constantly enhance predictive performance and determine encryption policies, which also enhance the cloud security and compliance with the regulatory requirements in the changing operating conditions.

References

[1] A. Kumar and S. C. P., "Privacy-Preserving Data Integrity in Cloud Computing: A Review of Hashing and Verification Techniques," 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3), Bhubaneswar, India, 2025, pp. 1-5, doi: 10.1109/ISAC364032.2025.11156813.

[2] K. S. Kumar, J. V. Kumar, K. S. Kumar and N. V. Kumar, "Security and Privacy Challenges in Multi-Tenant Cloud Architectures: A Comprehensive Analysis," 2025 International Conference on Computing Technologies & Data Communication (ICCTDC), HASSAN, India, 2025, pp. 1-6, doi: 10.1109/ICCTDC64446.2025.11158758.

[3] P. Vaghasia, R. Patel, D. Patel, A. Goswami, R. Patel and R. Vaghasia, "Improving Data Security and Privacy in Cloud-Based Data Analysis: A Results-Driven Approach," 2025 International Conference on Computing Technologies (ICOCT), Bengaluru, India, 2025, pp. 1-8, doi: 10.1109/ICOCT64433.2025.11118763.

[4] S. Gayathri and M. S. Kumar, "Scalable and Secure Sharing of Personal Health Records in Fog Cloud Computing Using Attributed," 2025 International Conference on Computing Technologies & Data Communication (ICCTDC), HASSAN, India, 2025, pp. 01-05, doi: 10.1109/ICCTDC64446.2025.11158734.

[5] P. Shah, S. Shah and A. Agrawal, "Advanced Encryption Techniques for Enhancing Data Security and Privacy in Cloud Environments," 2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC), Dayton, OH, USA, 2025, pp. 1-5, doi: 10.1109/SATC65530.2025.11137337.

[6] Y. Huang, "Research on Cloud Data Security Computing Framework Based on Fusion of Homomorphic Encryption and Differential Privacy," Journal of Cyber Security and Mobility, vol. 14, no. 4, pp. 927-954, July 2025, doi: 10.13052/jcsm2245-1439.1447.

[7] V. M, G. V, S. Lahari, T. Yamini and S. S, "A Three-Layer Based Intelligent Data Privacy Protection Scheme in Cloud Storage," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-6, doi: 10.1109/INCET64471.2025.11140924.

[8] H. Luo and C. Ji, "Cross-Cloud Data Privacy Protection: Optimizing Collaborative Mechanisms of AI Systems by Integrating Federated Learning and LLMs," 2025 IEEE 7th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2025, pp. 230-233, doi: 10.1109/CISCE65916.2025.11065466.

[9] W. Zheng, T. Zhou, Z. A. Bhuiyan and J. Shen, "Privacy-Preserving Data Auditing with Efficient Corrupted Data Locating for Cloud Computing," IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), London, United Kingdom, 2025, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS65812.2025.11152801.

[10] V. L V, Y. Ramaswamy, L. Gudala, H. MohamadAbbas and C. Sushama, "Privacy-Preserving Data Analysis using Decentralized Blockchain-Based Authentication with Zero-Knowledge Cloud Auditing," 2025 3rd International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2025, pp. 1-6, doi: 10.1109/ICDSIS65355.2025.11070587.

[11] A. F. Augustine, A. M. Jain and B. S. Telaprolu, "Cloud Computing-Integrated AI Diagnostic Framework for Real-Time Healthcare Delivery," 2025 International Conference on Recent Innovation in Science Engineering and Technology (ICRISET), CHENNAI, India, 2025, pp. 1-6, doi: 10.1109/ICRISET64803.2025.11251601.

[12] A. Alzaabi and A. Mehmood, "A Privacy-Preserving Framework for Scalable Data Integrity Verification in Cloud Storage Using Zero-Knowledge Proofs," 2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), Antalya, Turkiye, 2025, pp. 1-5, doi: 10.1109/ACDSA65407.2025.11165823.

[13] R. Kashyap, A. M. Mustafa, M. M. Abdulhasan, N. R. Nimah and V. K. Dunka, "Federated Learning Based Privacy Preserving Cloud Computing Platform for Health Management," 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, Raigarh, India, 2025, pp. 1-6, doi: 10.1109/OTCON65728.2025.11071159.

[14] B. V. Vishwanath, N. Pathi and S. Abhi, "Enhancing Healthcare Data Privacy with Zero Knowledge Proof on AWS," 2025 International Conference on Emerging Technologies in Computing and Communication (ETCC), Bangalore, India, 2025, pp. 1-6, doi: 10.1109/ETCC65847.2025.11108626.

[15] R. K. Badugu, N. Goke, S. Salendra, S. Manda, K. Vijay Kumar and S. V. Rao Souda, "Key Aggregation in Trusted Execution for Multi-Query Privacy in Cloud Computing with Enhancing Data Privacy," 2025 International Conference on Artificial Intelligence and Data Engineering (AIDE), Nitte, India, 2025, pp. 810-815, doi: 10.1109/AIDE64228.2025.10987441.

[16] G. Modalavalasa, "Analysis and Optimization of Privacy-Preserving Encryption Techniques in Cloud Computing Environments for Secure Cloud Data," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-6, doi: 10.1109/CONIT65521.2025.11167685.

[17] R. G, D. S, G. D. T, M. K, M. Adudhodla and S. Maheshwari, "Ensuring Data Integrity: Blockchain-Based Healthcare Applications in the Cloud," 2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), Coimbatore, India, 2025, pp. 152-156, doi: 10.1109/ICC-ROBINS64345.2025.11086183.

[18] S. Amancha, N. Srinu, B. Ramadevi, M. Lavanya and A. L. Parvathi, "Auditing of Shared Data in Cloud Storage with User Privacy Preserving -Using AES Algorithm," 2025 6th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 2025, pp. 1-6, doi: 10.1109/RAIT65068.2025.11088992.

[19] A. Dhaman and U. Suman, "Towards a Comparative Analysis of Security Attacks in Cloud Data Migration," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-7, doi: 10.1109/WorldSUAS66815.2025.11199246.

[20] J. Chen, C. Hu, W. Sheng, H. Xia, P. Hu and J. Yu, "Fog-Enhanced Personalized Privacy-Preserving Data Analysis for Smart Homes," IEEE Transactions on Cloud Computing, vol. 13, no. 3, pp. 995-1010, July-Sept. 2025, doi: 10.1109/TCC.2025.3586052.