Enhancing Data Security in Public Cloud with Blockchain and Biometric Authentication

1st Dr. M. Senthil Kumar
Dep. Of Cyber Security
SRM Valliammai Engineering College
Kattankulathur,India
msen1982@gmail.com

2nd Akilash A
Dep. Of Cyber Security
SRM Valliammai Engineering College
Kattankulathur,India
aakilash05@gmail.com

3rd Alagu Sruthi Bharathi A
Dept. of Cyber Secuirty
SRM Valliammai Engineering College
Kattankulathur, India
alagusruthibharathi@gmail.com

4th Aloy Gnalan A
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur,India
gnalanaloy2@gmail.com

***Abstract*—This Ensuring safe storage and access control of cloud-based data has become crucial due to the quick digitization of IT infrastructures. This analysis examines several methods for blockchain- based integrity verification, NoSQL database storage, multimodal authentication (biometric and facial recognition), and security measures in public cloud settings. Recent developments in biometric and facial authentication, deduplication encryption, dashboard-based real-time monitoring, and privacy-preserving strategies for industrial applications are all examined. Before storing fragmented data in a NoSQL database, we employ Random Pattern Fragmentation (RPF) to improve data security and ChaCha20 encryption to secure it. The goal of this study is to present a thorough analysis of new technologies that improve the integrity, security, and accessibility of data in IT management systems.**

Keywords—Multimodal Authentication, Biometric Authentication, Face Recognition, Blockchain, Random Pattern Fragmentation, ChaCha20 Encryption

I. Introduction

Nowadays, IT infrastructures are growing rapidly, so to protect business data we need robust security. There are some traditional methods, like centralized encryption, password-based authentication and conventional access control, but these methods do not help in attacks like ransomware attacks, insider threats, advanced persistent threats(APTs) and data breaches. To overcome these challenges, improvised security solutions are being implemented, such as blockchain for ensuring data integrity, NoSQL databases for secure storage and reducing latency and authentication methods that combine facial recognition and time-based One-Time Password. By using these technologies, the security, usability and reliability of public cloud environments are improved. In this research, the latest security strategies across different IT domains focus on integrity assurance, storage solutions and authentication mechanisms. Also, here we use Random Pattern Fragmentation (RPF) as a secure method for distributing data and the fragmented data is encrypted using ChaCha20 and stored in a NoSQL database for more security purposes.

II. Literature Review

Cloud-based IT systems are becoming common, so they require more data security and integrity. To improve security, researchers consider different methods like facial recognition and using multiple authentication techniques together. Blockchain technology helps maintain data integrity, while Random Pattern Fragmentation (RPF) ensures that data is safely distributed across different storage locations. Additionally, ChaCha20 encryption provides strong protection to keep data secure. By using these technologies, the public cloud environment will be secured.

A. *Multimodal Authentication*

Multimodal authentication is a solution for secure authentication. Combining face recognition and time-based one-time passwords (TOTP), it provides strong security for authenticating user identity [4]. Face recognition is more secure, while TOTP adds an extra layer of protection by generating random passcodes that change over time. Face authentication and time-based onetime passwords (TOTP) have improved remote identity authentication [16]. To keep biometric data safe, secure storage systems have been used [8]. Some methods use special classification techniques to improve accuracy and privacy [8]. Recently, using advanced deep learning has made facial recognition systems more accurate and less vulnerable to spoofing attempts [9]. Additionally, smart authentication methods analyze user behavior to detect suspicious activity. Moreover, it has been suggested that cloud-based authentication frameworks can guarantee security and privacy by combining biometric modalities with cryptographic approaches like homomorphic encryption.

Besides these developments, multimodal authentication also undergoes continuous development with the addition of more complex methods. Convolutional neural networks (CNNs) and generative adversarial networks (GANs) are being used to facilitate face recognition accuracy and liveness detection to prevent attempts of spoofing by using pictures, video or masks. In addition, behavioral biometrics, like the keystroke pattern, mouse movement, and consistency in the location, are being implemented to offer on-going authentication after initial log-in. Such a stratified system proves to be safe in case one of the factors is impaired where other modalities and behavioral examination serves as backup measures. In addition, scalable solutions to enterprises are provided by cloud-based architectures based on highly developed cryptographic techniques such as homomorphic encryption and secure multiparty computation, so that the data can be processed without exposing raw biometric data. With all of these innovations, the future of secure, privacy maintaining, and easy to use authentication systems is becoming a reality.

The other factor that needs to be taken into consideration in multimodal authentication is the usability and user acceptance. Although the main objective is security, the authentication systems should be also convenient and easy to use otherwise the users will resist adoption and find a way of evading the system. The need to strike a balance between security and smooth user experience is therefore important. Due to the example, face recognition provides hands-free and fast access, but the introduction of TOTP needs to be entered manually, and in some cases, it may be perceived as inconvenient. To overcome this, there is a discussion on adaptive authentication where the system dynamically changes the factors required dependent on the riskiness of the activity. In the case of low-risk activity, one modality might be adequate, whereas the high-risk transaction can cause multiple authentication layers. This trade off of security, efficiency, and user comfort makes multimodal systems effective and acceptable.

B. *Blockchain for Data Integrity in Public Cloud*

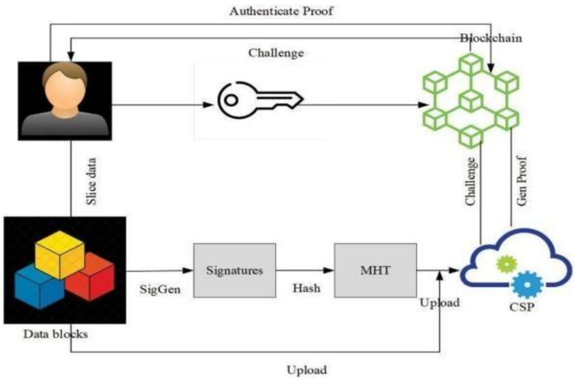


Fig 1. Integrity Authentication Scheme Flow

In cloud contexts, blockchain technology has proven to be a potent way to guarantee data security, transparency, and trust. Blockchain reduces the danger of illegal changes and data breaches by utilizing its decentralized and tamper-resistant characteristics. A blockchain-based public cloud data integrity verification system is shown in Figure 1, where user data is safely uploaded, hashed, signed, and sliced. By using challenge-response protocols with the cloud service provider (CSP), blockchain guarantees proof production and verification. It offers a trustworthy framework for confirming the legitimacy of data, stopping fraud, and guaranteeing adherence to security guidelines. Blockchain preserves unchangeable records of transactions, improving the integrity of stored IT data. For cloud storage, tamper-proof logs are offered by public blockchain-based data verification frameworks [13]. Blockchain-based auditing systems improve data integrity and reduce storage costs [5]. Blockchain-based methods help save cloud storage space while keeping data confidential [15]. Additionally, blockchain helps verify data integrity and keeps encrypted cloud data secure [15].

In addition to integrity checks, blockchain offers an effective tool of auditing and accountability in cloud storage systems. Because all operations done on the data are registered as an immutable transaction, the organization acquires a dependable audit trail which cannot be erased or altered. This not only enhances the adherence to the regulatory controls but also lowers reliance on third-party audit services decreasing financial and operation overheads. In addition, blockchain systems increase the level of confidence of users, because clients will be able to verify the authenticity of their information without depending entirely on the cloud service provider.

The other current trend is that blockchain should be integrated with other sophisticated technologies to improve security of cloud data even more. To provide an example, blockchain and artificial intelligence (AI) will be used to automatically detect anomalies and recognize suspicious patterns of access, whereas homomorphic encryption will allow a person to process data without revealing raw information.

C. *NoSQL Storage and Data Fragmentation Security*

NoSQL database manages IT fragmented data efficiently, making easy way for data handling. In NoSQL database-as-a-service models, query processing is done using priority- based performance improvements [11]. Distributed NoSQL systems give a solution for managing and scaling large IT databases [19]. Blockchain technology helps verify that encrypted cloud data is real and hasn’t been tampered with [1]. In shared cloud environments, smart data placement improves speed and saves storage space [14]. Before saving data in a NoSQL database, it is split into smaller pieces using Random Pattern Fragmentation (RPF), and each piece is protected with ChaCha20 encryption [6].

NoSQL systems are important to process unstructured and semi-structured data which the conventional relational databases are not always able to handle. Distributed nature of these systems provides horizontal scalability, whereby, as the data increase, one can add more servers without reducing the system performance. This renders NoSQL especially suitable with cloud-based deployments where it cannot be erased, is resilient and can withstand failures.

The other significant issue in cloud data storage is security, and the use of Random Pattern Fragmentation (RPF) in combination with ChaCha20 encryption can solve this issue. RPF provides higher levels of confidentiality by dividing the data into smaller fragments and randomly allocating the fragments thus making it extremely difficult to reconstruct meaningful information even when a fragment is compromised by attackers. Modern stream cipher ChaCha20 also provides a secure encryption of each fragment with lightweight but very strong encryption, which means that it does not affect the performance as much as the security of the cipher. Combined with blockchain-based verification, organizations can be provided with an end-to-end guarantee that its cloud data is authentic and full of tamper evasion. This is a hybrid solution, which combines NoSQL scalability, fragmentation and encryption protocol, and blockchain validation, and it is a strong framework of operating secure, large-scale, and high-performance cloud databases.

D. *Cloud Security and Access Control*

Due to the growing need for cloud computing, strong identity management and data protection has to be ensured. Privacy issues, illegal access, and credential theft are some of the issues related to traditional identity management systems. Sophisticated cryptographic methods and decentralized frameworks are being integrated to enhance the cloud environment's access control and authentication. Solutions

based on blockchain, and encryption are crucial for anticipating identity theft and guaranteeing safe data transfers. Secure identity management is the basic for cloud apps that depend on IT. In commercial IoT environments, secure authentication is guaranteed through privacy-preserving blockchain identity management systems [18]. Encrypted deduplication techniques improve cloud security while reducing redundancy [12]. Algorithms for workflow scheduling maximize the cost reduction of security-conscious cloud services [3]. Frameworks for remote signcryption have been developed to increase cloud security data confidentiality [17].

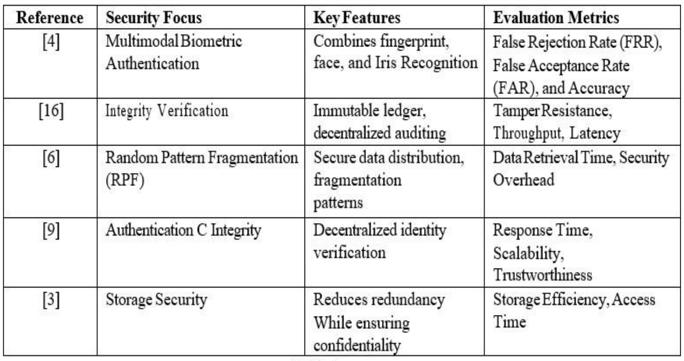
The identity management within the cloud environments is at the centre of preserving trust and security within the cloud environment, as organizations continue to rely on cloud-based applications. Conventional approaches that have centralized authorities are prone to single points of failure, which are easy to attack by hackers. As a way of overcoming these constraints, decentralized identity models are coming into practice, where users have the ability to manage their online identities without depending on third-party contributors. Such systems are usually based on a combination of a public key infrastructure (PKI) and a blockchain, so that identity credentials are not tampered with, can be traced and verified. Meanwhile, encryption-based access control will ensure that sensitive data are not obtained by unauthorized users regardless of the compromise of the infrastructure.

Besides the protection of identity, researchers are working on the more sophisticated cryptographic methods to enhance the overall security of cloud-based data. Privacy-sensitive schemes like encrypted deduplication lessen the redundancy of data and retain the confidentiality of data, enhancing storage efficiency without interfering with security [12]. On the same note, remote signcryption systems provide a two-fold security level through integrating digital signatures with encryption that ensures the safety of data confidentiality and authenticity in the transmission [17]. Moreover, smart scheduling algorithms keep the cost-efficiency and security needs, making sure that the use of cloud resources is optimized and the vulnerability is minimized [3]. Together, these additions are the basis of the next-generation cloud identity and data management systems, focusing on resilience, scale, and high resistance to new threats such as identity theft and insider attacks.

E. *Real-Time Monitoring and Network Security*

Maintaining the security and functionality of cloud-based infrastructures requires efficient system monitoring and threat detection. Organizations may identify irregularities, proactively address threats, and maximize resource use with the help of real-time analytics. Real-time dashboards offer crucial information for security event detection and system monitoring. Security event visualization is enhanced by an organized dashboard design style [20]. Additionally, network security is improved by VPN traffic service identification methods that use sampled data [7]. By increasing the effectiveness of VPN traffic classification, the RT- CBCH technique helps reduce unwanted access attempts [7]. Predictive security measures are improved by combining real-time dashboards with AI- driven anomaly detection. Additionally, by facilitating quicker incident resolution and lowering system vulnerabilities, automated response systems aid in the mitigation of cyber threats.

Security Mechanisms and Evaluation Metrics



Reference	Security Focus	Key Features	Evaluation Metrics
[4]	Multimodal Biometric Authentication	Combines fingerprint, face, and Iris Recognition	False Rejection Rate (FRR), False Acceptance Rate (FAR), and Accuracy
[16]	Integrity Verification	Immutable ledger, decentralized auditing	Tamper Resistance, Throughput, Latency
[6]	Random Pattern Fragmentation (RPF)	Secure data distribution, fragmentation patterns	Data Retrieval Time, Security Overhead
[9]	Authentication C Integrity	Decentralized identity verification	Response Time, Scalability, Trustworthiness
[3]	Storage Security	Reduces redundancy While ensuring confidentiality	Storage Efficiency, Access Time

Table 1

The identity management within the cloud environments is at the centre of preserving trust and security within the cloud environment, as organizations continue to rely on cloud-based applications. Conventional approaches that have centralized authorities are prone to single points of failure, which are easy to attack by hackers. As a way of overcoming these constraints, decentralized identity models are coming into practice, where users have the ability to manage their online identities without depending on third-party contributors. Such systems are usually based on a combination of a public key infrastructure (PKI) and a blockchain, so that identity credentials are not tampered with, can be traced and verified. Meanwhile, encryption- based access control will ensure that sensitive data are not obtained by unauthorized users regardless of the compromise of the infrastructure.

Besides the protection of identity, researchers are working on the more sophisticated cryptographic methods to enhance the overall security of cloud-based data. Privacy- sensitive schemes like encrypted deduplication lessen the redundancy of data and retain the confidentiality of data, enhancing storage efficiency without interfering with security [12]. On the same note, remote signcryption systems provide a two-fold security level through integrating digital signatures with encryption that ensures the safety of data confidentiality and authenticity in the transmission [17]. Moreover, smart scheduling algorithms keep the cost- efficiency and security needs, making sure that the use of cloud resources is optimized and the vulnerability is minimized [3]. Together, these additions are the basis of the next-generation cloud identity and

III. Discussion

In verified IT infrastructures, the capability, trustability and scalability of different plans are evaluated. It’s possible to effectively compare different approaches objectively, identifying their advantages and disadvantages through a clear evaluation framework. Data fragmentation patterns, access control methods, biometric authentication techniques, and cryptography approaches are considered crucial elements in this study. We find feebleness and areas for development by systematically analyzing these security measures, paving the way for more secure cloud security solutions. We also look at the computational overhead they introduce, to advance these approaches feasibility in resource-restricted settings. Under various deployment circumstances and loads, system performance is ensured to evaluate scalability. The creation of stronger and more effective security models that are reluctant to new threats and changing attacker tactics are the results of this comparison study.

IV. Conclusion

This survey comprehensively analyzed the authentication, integrity and storage methods that are used in non-vulnerable IT infrastructure management. The growing need of cloud computing focus on enhancing data security, access control and verification of integrity. Unauthorized access, loss of data, and vulnerabilities in systems are the major issues that have been brought to notice while trying to improve cloud-based IT management. A number of security models and methodologies have been examined. Among the components to securing an IT system, authentication is pivotal. To provide a strong and trustable way to verify users, access control is upgraded by including multimodal authentication, which is a combination of facial recognition and biometric recognition (fingerprint and iris scan). Multimodal techniques lower the risk of credentials theft and unauthorized access, which is done by utilizing behavioral and physiological characteristics. Optimized storage solutions to adequately deal with large-scale IT records are also discussed in the survey. Distributed architecture and data management across cloud environments is carried out seamlessly by NoSQL databases, which also have features such as high-performance, flexibility and scalability for data storage and retrieval. Unstructured and semi-structured data can be handled by NoSQL solutions, which stands as a contrast to traditional relational databases, making them relevant for managing large volumes of IT records in real-time. Integrating these technologies into a single, coordinated framework that efficiently blends with NoSQL storage options, blockchain-based integrity verification for tamper-proof security and multimodal authentication should be future studies to be indulged in.

References

[1] D. Bringhenti, R. Sisto, and F. Valenza, ‘Automating VPN Configuration in Computer Networks,’IEEE Transactions on Dependable and Secure Computing, Vol. 22, No. 1, pp. 561-576, 2025.

[2] W. Li, W. Susilo, C. Xia, L. Huang, F. Guo, and T. Wang, ‘Secure Data Integrity Check Based on Verified Public Key Encryption With Equality Test for Multi-Cloud Storage,’IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 6, pp. 5359-5374, 2024.

[3] M. Ali and X. Liu, ‘A Novel Framework in Cloud Security: Remote Signcryption,’IEEE Internet of Things Journal, Vol. 11, No. 24, pp. 41207-41218, 2024.

[4] D. Jeong, E. Choi, H. Ahn, E. Martinez-Martin, E. Park, and A. P. del Pobil, ‘Multi- modal Authentication Model for Occluded Faces in a Challenging Environment,’ IEEE Transactions on Emerging Topics in Computational Intelligence, Vol. 8, No. 5, pp. 3463- 3477, 2024.

[5] Y. Miao, K. Gai, L. Zhu, K.-K. R. Choo, and J. Vaidya, ‘Blockchain-Based Shared Data Integrity Auditing and Deduplication,’IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 4, pp. 3688-3702, 2024.

[6] L. Li, C. Zhou, P. Cong, Y. Shen, J. Zhou, and T. Wei, ‘Makespan and Security- Aware Workflow Scheduling for Cloud Service Cost Minimization,’IEEE Transactions on Cloud Computing, Vol. 12, No. 2, pp. 609-624, 2024.

[7] H. Wu, Y. Liu, G. Cheng, and X. Hu, ‘RT-CBCH: Real-Time VPN Traffic Service Identification Based on Sampled Data in High-Speed Networks,’ IEEE Transactions on Network and Service Management, Vol. 21, No. 1, pp. 88-102, 2024.

[8] D. Osorio-Roig, L. J. González-Soler, C. Rathgeb, and C. Busch, ‘Privacy- Preserving Multi-Biometric Indexing Based on Frequent Binary Patterns,’IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 4835-4850, 2024.

[9] G. Ha, C. Jia, Y. Chen, H. Chen, and M. Li, ‘A Secure Client-Side Deduplication Scheme Based on Updatable Server-Aided Encryption,’ IEEE Transactions on Cloud Computing, Vol. 11, No. 4, pp. 3672-3683, 2023.

[10] M. Song, Z. Hua, Y. Zheng, H. Huang, and X. Jia, ‘Blockchain-Based Deduplication and Integrity Auditing Over Encrypted Cloud Storage,’ IEEE Transactions on Dependable and Secure Computing, Vol. 20, No. 6, pp. 4928-4941, 2023.

[11] R. Andreoli, T. Cucinotta, and D. B. De Oliveira, ‘Priority-Driven Differentiated Performance for NoSQL Database-as-a-Service,’IEEE Transactions on Cloud Computing, Vol. 11, No. 4, pp. 3469-3481, 2023.

[12] R. Ding, Y. Xu, H. Zhong, J. Cui, and G. Min, ‘An Efficient Integrity Checking Scheme With Full Identity Anonymity for Cloud Data Sharing,’ IEEE Transactions on Cloud Computing, Vol. 11, No. 3, pp. 2922-2936, 2023.

[13] J. H. Khor, M. Sidorov, M. T. Ong, and S. Y. Chua, ‘Public Blockchain-Based Data Integrity Verification for Low-Power IoT Devices,’ IEEE Internet of Things Journal, Vol. 10, No. 14, pp. 13056-13067, 2023.

[14] J. Liu, L. Mo, S. Yang, J. Zhou, S. Ji, H. Xiong, and D. Dou, ‘Data Placement for Multi-Tenant Data Federation on the Cloud,’ IEEE Transactions on Cloud Computing, Vol. 11, No. 2, pp. 1414-1430, 2023.

[15] S. Jiang, J. Liu, J. Chen, Y. Liu, L. Wang, and Y. Zhou, ‘Query Integrity Meets Blockchain: A Privacy-Preserving Verification Framework for Outsourced Encrypted Data,’IEEE Transactions on Services Computing, Vol. 16, No. 3, pp. 2100-2113, 2023.

[16] Y. Liu, T. Zhou, Z. Yue, W. Liu, Y. Han, Q. Li, and X. Yang, ‘Secure and Efficient Online Fingerprint Authentication Scheme Based on Cloud Computing,’ IEEE Transactions on Cloud Computing, Vol. 11, No. 1, pp. 564-576, 2023.

[17] S. Li, C. Xu, Y. Zhang, Y. Du, and K. Chen, ‘Blockchain-Based Transparent Integrity Auditing and Encrypted Deduplication for Cloud

Storage,'IEEE Transactions on Services Computing, Vol. 16, No. 1, pp. 134-148, 2023.

[18] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, 'PBIDM: Privacy- Preserving Blockchain-Based Identity Management System for Industrial Internet of Things,' IEEE Transactions on Industrial Informatics, Vol. 19, No. 2, pp. 1524-1537,2023.

[19] R. Li, H. He, R. Wang, S. Ruan, T. He, J. Bao, J. Zhang, L. Hong, and Y. Zheng, 'TrajMesa: A Distributed NoSQL-Based Trajectory Data Management System,' IEEE Transactions on Knowledge and Data Engineering, Vol. 35, No. 1, pp. 1013-1026, 2023.

[20] B. Bach, E. Freeman, A. Abdul-Rahman, C. Turkay, S. Khan, Y. Fan, and M. Chen, 'Dashboard Design Patterns,' IEEE Transactions on Visualization and Computer Graphics, Vol. 29, No. 1, pp. 342-357, 2023.