AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

Data Shield Vault: A Secure Exchange Framework Combining MFA, RSA-AES Hybrid Cryptography, and SHA-256-Based Integrity with Role Logging

P. Vamshi Krishna[1], Chinthala Sahithya[2], Bandari Manohar[2], Dandu Abhinaya Sri[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

Secure data management has become a critical requirement in modern digital systems due to the rapid growth of sensitive information and increasing cybersecurity threats. Traditional systems mainly rely on single-layer authentication and basic encryption techniques, making them vulnerable to unauthorized access, data breaches, and lack of data integrity. These systems often fail to implement advanced mechanisms such as Multi-Factor Authentication (MFA), secure key management, and proper activity logging. To address these challenges, the proposed system introduces a secure data management framework that integrates MFA with advanced encryption and integrity techniques. The authentication process combines password-based login, biometric verification using OpenCV (Open-Source Computer Vision Library), and One-Time Password (OTP) validation to ensure strong user authentication. For data protection, ChaCha20-Poly1305 is used for efficient and secure encryption, while RSA (Rivest–Shamir–Adleman) and AES (Advanced Encryption Standard) hybrid encryption ensures secure key exchange and data sharing. Additionally, SHA-256 (Secure Hash Algorithm 256-bit) is implemented to maintain data integrity by generating unique hash values. The system also incorporates Role-Based Access Control (RBAC) along with logging mechanisms to monitor user activities such as login, data access, sharing, and downloads, ensuring accountability and traceability. This layered approach overcomes the limitations of traditional systems by providing enhanced security, controlled access, and reliable data protection. The solution is lightweight, scalable, and efficient, making it suitable for real-world applications. It significantly improves data confidentiality, integrity, and security, offering a robust and practical framework for secure digital data management.

Key words: Secure Data Management, Multi-Factor Authentication (MFA), Hybrid Encryption, ChaCha20-Poly1305, RSA, AES, SHA-256, Role-Based Access Control (RBAC).

1.INTRODUCTION

Today, the process of cyber-physical systems incorporates both processing and data transmission. The significant challenge here is the legal and ethical perspective. Hence, for these systems, data security needs to be addressed. Recently, researchers have been interested in global cyber-physical systems. As per the US National Science Foundation (NSF) report, sensing, computations, and networking are involved [1]. As the number of cloud users increases, data sharing grows, and data auditing becomes crucial. To address this issue, various public key infrastructure-based techniques are applied. Despite this, there exists the issue of certificate management. Although a certificate-shared auditing scheme was proposed, it is inefficient in handling dynamic data and protecting data privacy. Due to security, the verifier cannot access the information and ensure its integrity. With the rise of cloud services, storage services are provided without human interaction [2]. Therefore, ensuring data integrity is vital. In the case of cloud users, they download thinking integrity is maintained [3]. When a member of the group uploads a file, other members can access and modify it. Applications such as Dropbox are used in many companies for employees to work together. Whereas the cloud service provider (CSP) ensures data integrity. As shown as figure 1 The possibility of data corruption exists due to hardware or software

failure. Hence, the integrity of stored data applies RDPC schemes to generate an authentication tag for each block.

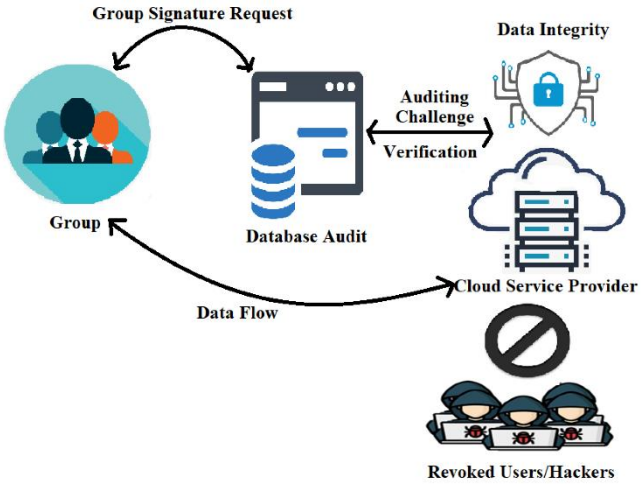

Figure 1: Enhanced storage system with Encryption.

The status of the data is verified by the correctness of the tag. In block updating, the regeneration of the tag is another challenge. They generate the authentication tags while auditing, which increases the checking complexity. Additionally, the group is dynamic, so the user revocation must be addressed. Those who revoke all their public/private keys are to be made invalid [3]. Cloud computing benefits the user in terms of scalability, cost, and ease of access. A massive amount of cloud providers is finding difficulties in handling malicious attackers [4]. A security-enhanced cloud storage and retrieval mechanism (ECRM) to improve the storage and retrieval mechanisms for cloud users. To evaluate the performance of the proposed ECRM through various metrics and show its effectiveness in the cloud environment. To carry out the analysis in terms of the upload, download, encryption, and decryption times by varying the file size and formats. Finally, the performance of the proposed technique is compared with the existing model [5].

2.LITERATURE SURVEY

Kautish, et al. [6] proposed a novel technique to ensure the integrity and improve the access control. A novel enhanced storage retrieval mechanism is used to improve the performance of the cloud's storage and retrieval mechanisms to achieve this. The technique is evaluated in concern of the upload, download, encryption, and decryption time. As the file size grows, so does the time it takes to upload it. Similarly, the time taken to encrypt files of various formats and sizes evidenced that it depends on the file size and format. Thus, the encryption time increases as the file sizes increases, demonstrating the performance of the proposed system. Chen, et al. [7] proposed a user-friendly encrypted storage scheme named EStore, which is based on the Hadoop distributed file system. Users can make use of cloud-based distributed file systems to collaborate with each other. However, most data are processed and stored in plaintext, which is out of the owner's control after it has been uploaded and shared. Meanwhile, simple encryption guarantees the confidentiality of uploaded data but reduces availability. Furthermore, it is difficult to deal with complex key management as there is the problem whereby a single key encrypts different files, thus increasing the risk of leakage.

Al Lail, et al. [8] proposed a new approach that utilizes the Generalized Spatio-Temporal Role-Based Access Control Model (GSTRBAC) within the context of LBS. GSTRBAC grants access based on user credentials, authorized locations, and access times, providing a detailed approach to securing LBS data. They introduced an optimized cloud-based GSTRBAC implementation suitable for deployment in modern LBS architectures. The system uses two secure communication protocols tailored to different

security requirements. This allows for efficient communication for less-sensitive data while offering robust protection for highly sensitive information. Saxena, et al. [9] explored particularly through integration with emerging technologies such as the Metaverse, Augmented Reality (AR), and Virtual Reality (VR). As the number of service users increases, so does the demand for computational resources, leading data owners to outsource processing tasks to remote cloud servers. The internet-based delivery of cloud computing services consequently expands the attack surface and impacts the trust relationship between the service user and the service provider.

Zhang, et al. [10] proposed approach is highly secure against adaptive selective ciphertext attacks and has excellent resistance to message attacks. A comprehensive performance evaluation, including time measurements, is conducted and the protocol is compared to other protocols, revealing the efficient file upload and download processes of the proposed approach. The results demonstrate the protocol's strong security, practicality, and operational efficiency. Zhou, et al. [11] proposed a secure data storage and access control scheme for the supply chain ecosystem based on the enterprise-level blockchain platform Hyperledger Fabric. The design incorporates a dual-layer attribute-based auditable access control model for access control, with four smart contracts aimed at coordinating and implementing access policies. The experimental results demonstrate that the proposed approach exhibits significant advantages under large-scale data and multi-attribute conditions. It enables fine-grained, dynamic access control under ciphertext and maintains high throughput and security in simulated real-world operational scenarios.

Ramachandra, et al. [12] proposed TDES methodology provides a relatively simpler technique by increasing the sizes of keys in Data Encryption Standard (DES) to protect against attacks and defend the privacy of data. The experimental results showed that the proposed TDES method is effective in providing security and privacy to big healthcare data in the Cloud environment. The proposed TDES methodology showed less encryption and decryption time compared to the existing Intelligent Framework for Healthcare Data Security (IFHDS) method. Alabdulatif, et al. [13] provided a comprehensive review of the security and privacy of medical big data, including countermeasures. Secondly, they propose a novel cloud-enabled hybrid access control framework for securing the medical big data in healthcare organizations, and the result of this research indicates that the proposed access control model can withstand most cyber-attacks, and it is also proven that the proposed framework can be utilized as a primary base to build secure and safe medical big data solutions.

Zhou, et al. [14] proposed a strategy to fragment and distribute space–time big data while enabling both encryption and nonencryption operations based on different data types. The sharing of sensitive data is enabled via smart contract technology. Second, CSSoB's single-node storage performance was assessed under local and local area network (LAN) conditions, and results indicate that the read performance of CSSoB surpasses its write performance. Mishra, et al. [15] proposed approach aims to enhance both the flexibility and efficiency of data protection in cloud environments. The findings of this study are anticipated to have significant implications, contributing to the advancement of existing techniques and inspiring the development of innovative research-driven solutions. Continuous research efforts are required to validate the effectiveness of the proposed framework across diverse contexts and assess its performance against evolving privacy vulnerabilities in cloud computing.

3. PROPOSED SYSTEM

The system architecture integrates secure authentication, encrypted data management, and role-based access within a unified Flask-based application. It begins with user interaction through login or signup, followed by multi-level authentication involving biometric verification and OTP validation to ensure strong identity confirmation. As illustrated in Figure 2, encryption mechanisms are applied across multiple layers, including secure storage, data sharing, and document protection using ChaCha20-Poly1305 and RSA–AES hybrid techniques. Once authenticated, the system establishes a session and

dynamically routes users based on their roles to either user or admin dashboards. The backend manages encryption, decryption, and secure key handling while interacting with TinyDB for persistent storage. Sensitive data such as vault entries, shared messages, and documents are always stored in encrypted form and decrypted only when accessed by authorized users. The architecture also includes logging, monitoring, and encryption comparison modules to evaluate performance.

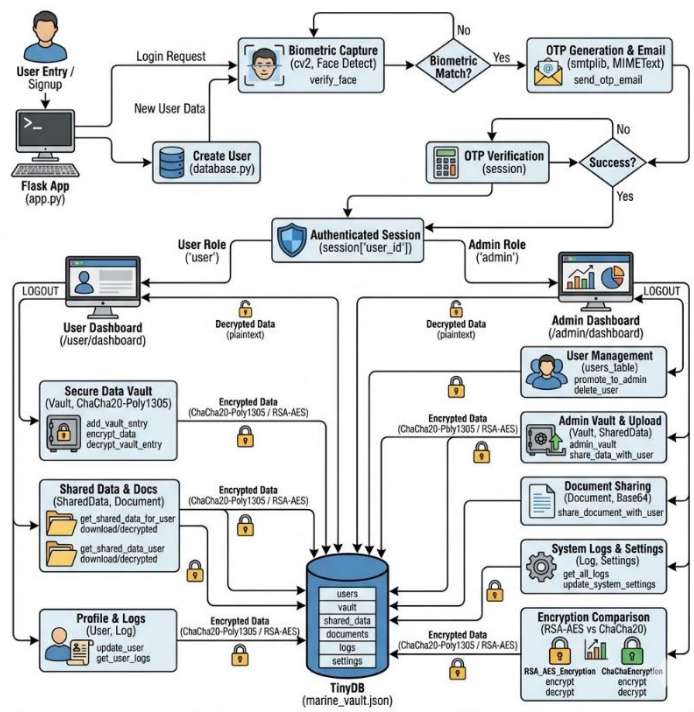

Figure 2: Proposed System Architecture

User Entry and Authentication Initialization: The system begins when a user performs login or signup through the interface. User credentials are collected and validated, while new users are registered with securely stored details and generated encryption keys. This step ensures that each user is uniquely identified and prepared for secure interaction within the system.

Biometric and OTP-Based Verification: After credential verification, the system performs biometric authentication using face detection and comparison techniques. If the biometric match is successful, an OTP is generated and sent to the user's email for additional verification. This multi-factor authentication strengthens security by combining multiple identity validation methods.

Session Creation and Role-Based Routing: Once authentication is successful, a secure session is established using session variables to maintain user state. The system determines the user role and redirects accordingly to either user or admin dashboard. This ensures controlled access to features and secure handling of encrypted data based on authorization levels.

Encryption-Based Data Storage: All sensitive data such as vault entries, user information, and shared content are encrypted before being stored in the database. The system uses ChaCha20-Poly1305 for primary encryption and RSA–AES hybrid techniques for secure key handling. This ensures that stored data remains protected from unauthorized access.

Secure Data Sharing and Document Protection: When data or documents are shared, the system encrypts the content separately for both sender and receiver using their respective keys. Documents are encoded and encrypted before being transmitted or stored. This ensures confidentiality and prevents data exposure during sharing operations.

Decryption, Access, and Logging: Authorized users can request access to stored or shared data, which is decrypted using their respective keys. All operations such as access, sharing, and downloads are logged in the database for monitoring and auditing. This maintains transparency, accountability, and system integrity.

4. RESULTS ANALYSIS

The results demonstrate that the system successfully achieves strong data security through the integration of multi-factor authentication and hybrid encryption techniques. The implementation of password, biometric, and OTP-based authentication significantly reduces unauthorized access. Encryption mechanisms such as ChaCha20-Poly1305 and RSA–AES ensure efficient and secure data storage and sharing. The system also maintains data integrity using SHA-256 hashing, preventing tampering. Performance analysis shows that the system handles encryption and decryption efficiently across different file sizes.

Figure 3: Security Protocol Comparison with Encryption and Decryption time

Figure 3 depicts the security protocol comparison, presenting a detailed analytical evaluation of encryption and decryption performance between RSA-AES (legacy) and ChaCha20-Poly1305 (proposed) using quantitative metrics. The figure shows that the key generation time is approximately 0.0442 s for RSA-AES, while it is nearly 0.00000 s for ChaCha20-Poly1305, indicating a significant improvement. It also illustrates that the encryption time for a 1 MB file is around 6.32 ms in the legacy system compared to 5.54 ms in the proposed approach, achieving about 12.33% faster performance. Similarly, the decryption time is reduced from approximately 6.00 ms to 4.99 ms, resulting in nearly 16.81% improvement.

Figure 4 depicts the secure data management module for users, showcasing how individuals can create, store, and manage their confidential information within the encrypted vault. The figure emphasizes the process of adding new entries, categorizing data, and ensuring secure storage through encryption techniques. It reflects the system's structured approach to handling personal and sensitive data.

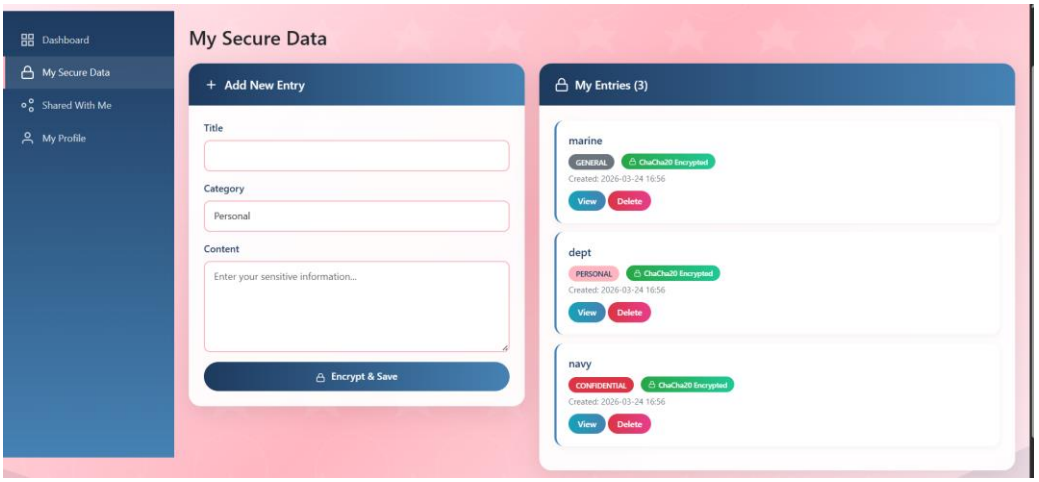

Figure 4: Secure Data

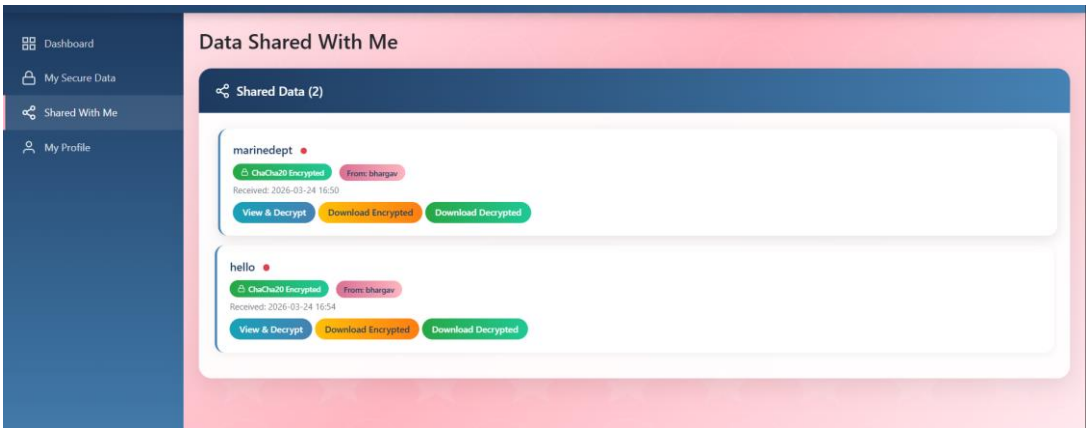

Figure 5: Shared Data

Figure 5 illustrates the shared data module, demonstrating how users can access and manage data that has been securely shared with them by other authorized users. The figure highlights the ability to view, download, and decrypt shared information while maintaining security constraints. It reflects the system's capability to ensure controlled access to shared resources. The depiction also indicates the presence of secure data exchange workflows within the platform.

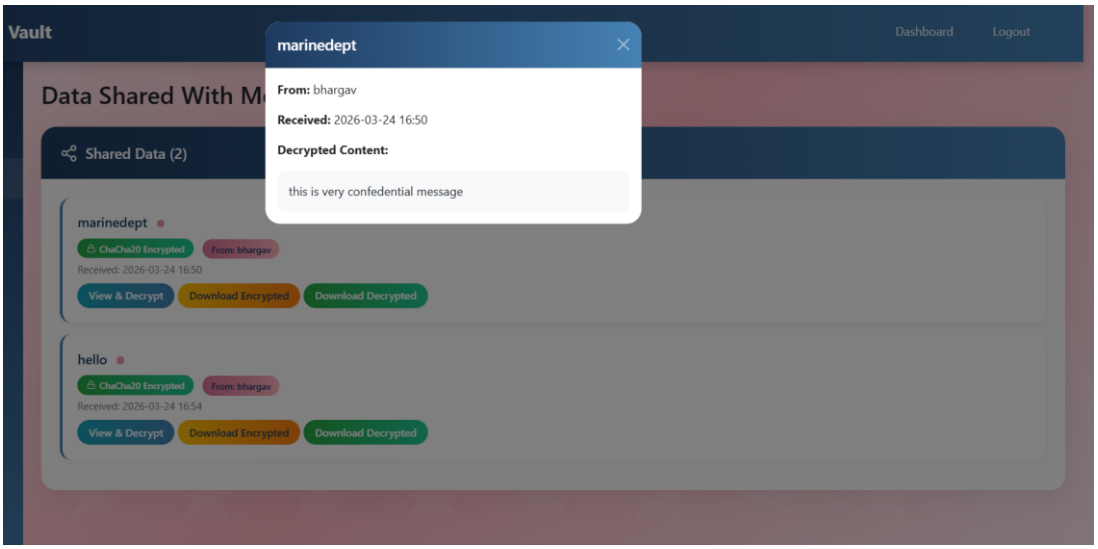

Figure 6: Decrypting and Viewing Messages

Figure 6 depicts the decryption and message viewing process, illustrating how users can securely access the original content of encrypted data after successful authentication. The figure highlights the transformation of encrypted information into readable format while maintaining security protocols. It reflects the system's ability to preserve confidentiality during storage and ensure secure retrieval during access. The illustration also indicates controlled visibility of sensitive information only to authorized users.

5. CONCLUSION

The developed system successfully addresses the growing need for secure data storage and sharing by integrating multiple layers of security into a unified platform. It combines strong authentication mechanisms with advanced encryption techniques to ensure confidentiality, integrity, and controlled access to sensitive information. The implementation of multi-factor authentication significantly enhances user verification, reducing the risk of unauthorized access. The use of hybrid encryption improves both security and performance by balancing speed and strength in data protection. Efficient handling of encryption and decryption operations ensures minimal delay even with increasing data sizes. The system demonstrates reliable performance during data storage, retrieval, and sharing processes. Integrity verification mechanisms effectively detect any unauthorized modifications to data. Role-based access control ensures that users can only perform permitted actions, enhancing overall system security. Activity logging improves transparency and accountability by tracking user operations. The architecture is lightweight and scalable, making it suitable for real-time applications. Performance evaluations indicate that the system maintains stability under moderate workloads. Optimization of cryptographic processes contributes to faster execution times compared to traditional methods. The integration of biometric authentication adds an extra layer of robustness without significantly affecting system speed. The system design also ensures efficient resource utilization, making it practical for deployment on standard hardware.

REFERENCE

[1] Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. J. Parallel Distrib. Comput. 2021, 153, 150–160.

[2] Mante, R.V.; Bajad, N.R. A study of searchable and auditable attribute-based encryption in cloud. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; IEEE: Piscataway, NJ, USA, 2021; pp. 1411–1415.

[3] Vennala, A.; Radha, M.; Rohini, M.; Anees Fathima, M.; Lakshmi, P.D. Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage. J. Eng. Sci. 2022, 13, 532–541.

[4] Li, R.; Yang, H.; Wang, X.A.; Yi, Z.; Niu, K. Improved Public Auditing System of Cloud Storage Based on BLS Signature. Secur. Commun. Netw. 2022, 2022, 6800216.

[5] He, J.; Zhang, Z.; Li, M.; Zhu, L.; Hu, J. Provable data integrity of cloud storage service with enhanced security in the internet of things. IEEE Access 2018, 7, 6226–6239.

[6] A R, Kautish S, Juneja S, Mohiuddin K, Karim FK, Elmannai H, Ghorashi S, Hamid Y. Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments. *Electronics*. 2023; 12(3):714. https://doi.org/10.3390/electronics12030714

[7] Chen Y, Dong G, Xu C, Hao Y, Zhao Y. EStore: A User-Friendly Encrypted Storage Scheme for Distributed File Systems. *Sensors*. 2023; 23(20):8526. https://doi.org/10.3390/s23208526

[8] Al Lail M, Moncivais M, Benton R, Perez AJ. Cloud-Based Access Control Including Time and Location. *Electronics*. 2024; 13(14):2812. https://doi.org/10.3390/electronics13142812

[9] Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219

[10] Zhang J, Chen A, Zhang P. Provably Secure Data Access Control Protocol for Cloud Computing. *Symmetry*. 2023; 15(12):2111. https://doi.org/10.3390/sym15122111

[11] Li S, Zhou T, Yang H, Wang P. Blockchain-Based Secure Storage and Access Control Scheme for Supply Chain Ecological Business Data: A Case Study of the Automotive Industry. *Sensors*. 2023; 23(16):7036. https://doi.org/10.3390/s23167036

[12] Ramachandra MN, Srinivasa Rao M, Lai WC, Parameshachari BD, Ananda Babu J, Hemalatha KL. An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard. *Big Data and Cognitive Computing*. 2022; 6(4):101. https://doi.org/10.3390/bdcc6040101

[13] Alabdulatif A, Thilakarathne NN, Kalinaki K. A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data. *Electronics*. 2023; 12(12):2646. https://doi.org/10.3390/electronics12122646

[14] Zhou B, Zhao J, Chen G, Yin Y. Research on Secure Storage Technology of Spatiotemporal Big Data Based on Blockchain. *Applied Sciences*. 2023; 13(13):7911. https://doi.org/10.3390/app13137911

[15] Mishra KN, Lal RK, Barwal PN, Mishra A. Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework. *Applied Sciences*. 2025; 15(13):7485. https://doi.org/10.3390/app15137485