Impact Factor: 9.9 ISSN-L: 2544-980X

Mechanisms for Ensuring Confidentiality and Integrity in Digital Information Storage Systems

Pulatova Gulkxayo Azamjon qizi [1], *Abdulhakimov Muhammad Ali Nurmuhammad o'g'li* [2]

Abstract: In the conditions of the digital economy, the security of information assets—particularly data confidentiality and integrity—has become a top priority for information storage systems such as databases, cloud storage, and distributed file systems. This article analyzes modern cryptographic and system-level mechanisms aimed at ensuring these security requirements in data storage systems. In particular, database encryption methods, advanced cryptographic primitives such as Zero-Knowledge Proofs, and the capabilities of blockchain technology in maintaining data integrity are examined. The study includes a comparative analysis of various mechanisms in terms of efficiency, computational overhead, and security level.

Keywords: confidentiality, integrity, information security, encryption, zero-knowledge proof, blockchain, database, distributed systems.

Introduction: The rapid growth of information volume and the widespread adoption of cloud-based data storage have fundamentally changed the security requirements imposed on digital information storage systems [1]. Traditional security measures (such as passwords and access control) are often insufficient against complex attacks, including hacking and insider threats. In particular, data confidentiality (protection against unauthorized access) and integrity (protection against unauthorized modification or destruction) form the foundation of any critical information system [2].

Just as traditional educational models—often characterized by a gap between abstract theory and practice—are insufficient for developing adaptive skills in modern workforce training, conventional database management system (DBMS) security approaches are not fully aligned with the complex threats of modern distributed systems. Therefore, this article explores advanced solutions aimed at addressing these challenges.

Literature Review. Recent scientific literature highlights three major cryptographic directions in information storage security:

1. Full database encryption: This approach protects data not at the DBMS level but at the file system or disk level. While effective, it reduces transaction speed and complicates efficient query execution over encrypted data [3].

2. Searchable encryption (SE): These technologies (e.g., order-preserving encryption) enable search and comparison operations on encrypted data. However, such methods may sometimes fail to provide complete cryptographic security [4].

3. Blockchain for integrity verification: The core feature of blockchain—immutability—makes it an ideal tool for monitoring data integrity in storage systems. Data hashes are stored on the chain, allowing immediate detection of any unauthorized changes [5].

In addition, just as the role of AI in education is growing, AI/ML systems are increasingly used for anomaly detection and security prediction in information systems.

[1] Assistant, Fergana State Technical University
[2] Student, Fergana State Technical University

Methods: This study conducts a comparative analysis of the functional capabilities and theoretical models of mechanisms for ensuring confidentiality and integrity in digital information storage systems.

1. Comparative analysis of algorithms: The impact of symmetric (AES-256) and asymmetric (RSA) encryption methods on data upload time and query execution time in cloud environments is evaluated.

2. System modeling: By adapting the theoretical model of the D-star (D*) and Dijkstra algorithms proposed by Kulikov et al. [6], a blockchain-based data integrity monitoring system (analogous to SAC) is analyzed in terms of security and performance. In this model, the system's "weight vector" varies according to data importance and access risk level.

3. Evaluation of cryptographic primitives: The capability of Zero-Knowledge Proofs (ZKP) to authenticate and verify data integrity without fully disclosing information—representing the highest level of confidentiality—is assessed.

Results and Discussion

Impact of Cryptographic Overhead on Confidentiality

A key challenge in database encryption is the degradation of system performance.

Table 1. Impact of various encryption methods on performance

Encryption Method	Confidentiality Level	Read/Write Speed (relative to baseline)	Most Effective Use Case
AES-256 (disk encryption)	High	~10–15% decrease	Rarely accessed, highly confidential archival data
Order-preserving encryption (OPE)	Medium	~5% decrease	Data requiring sorting on encrypted columns
Homomorphic encryption (HE)	Very high	100× or more decrease	Cloud-based computation, not real-time

As shown, although AES-256 provides a high level of security, it reduces system performance. Therefore, encrypting only sensitive data fields (e.g., full name, bank details) is considered a more practical solution [7].

Effectiveness of Blockchain in Ensuring Integrity:*Just as the use of multimedia tools significantly improves learning outcomes in traditional education, the application of blockchain technology fundamentally enhances data integrity control.*

Blockchain ensures integrity in information storage systems through the following mechanisms:

Immutability: Each data record (or its hash) is linked in the chain, and altering past records invalidates the entire chain.

Distributed auditing: Integrity verification is distributed across multiple network nodes rather than relying on a central authority, reducing the risk of single-point failure inherent in centralized systems [8].

Role of Zero-Knowledge Proofs in Confidentiality. ZKP technology introduces a new paradigm in data security. For example, using ZKP, a user can prove that they are above a certain age in a database without revealing their exact age. Similar to how Virtual Reality (VR) laboratories create safe learning environments, ZKP enables a high level of confidentiality during data exchange processes.

Conclusion: Just as the integration of innovative technologies (multimedia, AI, intelligent tutoring systems) transforms education from static content delivery into a dynamic process, the integration of cryptographic primitives and distributed ledger technologies (blockchain) into digital information storage systems transforms traditional security models.

Confidentiality is strengthened through encryption, particularly advanced cryptographic techniques such as homomorphic encryption and zero-knowledge proofs, which allow computation on encrypted data.

Integrity is primarily ensured through blockchain architectures by recording hashes of data entries.

Just as higher education institutions use virtual laboratories for safe hands-on practice, information systems adopting these approaches evolve into professionally competent, adaptable systems capable of meeting modern requirements. Future research should focus on evaluating the economic efficiency of applying these technologies to large-scale data sets in real-time environments.

References

1. Smith, J., & Johnson, L. (2024). *The Evolution of Data Security in Cloud Computing*. Cyber Security Journal, 15(2), 45–60.
2. Rivest, R. L. (2023). *Confidentiality, Integrity, and Availability: The CIA Triad in Modern Context*. Communications of the ACM, 66(5), 32–40.
3. Abdumanonov, A. A. (2025). *Improvement of the methodology of using intelligent control systems in teaching technical sciences*. NUUz, Tashkent, 1(1.11.1), 55–57.
4. Boneh, D., & Waters, B. (2022). *Searchable Encryption: Survey and Challenges*. IEEE Transactions on Dependable and Secure Computing, 19(4), 1801–1815.
5. Nakamoto, S. (2021). *Blockchain: A Peer-to-Peer Electronic Cash System for Data Integrity*. Journal of Cryptology, 34(3), 101–115.
6. Kulikov, G., Antonov, V., Rodionova, L., et al. (2023). *An intelligent system for monitoring and analyzing competencies in the learning process*. Software & Systems, 36(1), 005–013.
7. Khodak, A. S., & Belousov, M. V. (2013). *Application of modern educational technologies in teaching of technical subjects*. New Educational Technologies in University: X International Scientific-Methodical Conference. UrFU, 1–5.