Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

BlockSecure :A Decentralized Framework for Secure Digital Information Storage

Abhishek Lal
dept. of Computer Science
Dr.D.Y.Patil ACS College, Pimpri
Pune, India

Lavanya Shankarnarayanan
dept. of Computer Science
Dr.D.Y.Patil ACS College, Pimpri
Pune, India

Abstract - The rapid development of digital services has increased reliance on centralized systems for storing delicate information such as medical records, legal documents, academic certificates, and digital identities. Although centralized storage offers operational convenience, it introduces critical challenges including single-point failures, vulnerability to cyberattacks, limited user confidentiality, and delayed threat detection. To address these limitations, this paper proposes BlockSecure, a fully software-based decentralized framework that integrates blockchain technology, distributed storage, advanced cryptography, and artificial intelligence-driven security mechanisms for secure digital data management. In the anticipated approach, data files are encrypted using post-quantum cryptographic techniques to ensure long-term resilience against emerging quantum threats. The encrypted data is fragmented and distributed across the InterPlanetary File System (IPFS), thereby eliminating dependence on centralized storage infrastructures. Only cryptographic hashes, access policies, and ownership metadata are recorded on the Polygon blockchain through smart contracts, ensuring data integrity, transparency, and tamper resistance. User privacy is further enhanced through Zero-Knowledge Proof-based access control, enabling authorization verification without revelation of sensitive identity data. In addition, an AI-driven anomaly detection module continuously monitors access patterns and transaction behavior to recognize unauthorized activities or abnormal usage trends, allowing proactive and automated response mechanisms. The proposed BlockSecure framework improves data confidentiality, integrity, availability, and instantaneous threat detection while maintaining scalability and cost efficiency, making it apt for high-trust applications such as healthcare systems, legal services, and digital identity management.

Keywords - Blockchain, Cybersecurity, Decentralized Storage, Zero-Knowledge Proofs, Post-Quantum Cryptography

I. INTRODUCTION

In the modern digital era, sensitive information such as medical records, legal documents, academic certificates, and digital identities are increasingly stored and managed through online platforms. Centralized storage systems remain extensively implemented due to their scalability and operational convenience; they propose substantial security and privacy vulnerabilities. Reports indicate that more than 60% of major data breaches originate from centralized architectures, chiefly due to single-point failures, insider threats, and large-scale cyberattacks **[1]**. Such systems are often deprived of transparent data ownership, strong privacy assurances, and real-time threat detection, making them unsuitable for high-trust applications.

Additionally, several existing security frameworks rely on orthodox cryptographic techniques that may become vulnerable with the development of quantum computing capabilities **[2]**. The combined limitations of centralization, long-term cryptographic ambiguity, and reactive security monitoring highlight the necessity for a more robust and future-ready approach.

To address these shortcomings, this paper proposes BlockSecure, a decentralized framework that integrates blockchain technology, distributed storage, post-quantum cryptography, Zero-Knowledge Proof–based access control, and AI-driven anomaly detection. The framework aims to deliver secure, privacy-preserving, and scalable digital data management for contemporary applications. **[3]**

II. PROBLEM STATEMENT

Centralized data storage architectures remain to aid as the foundation for most virtual record management systems across healthcare, education, finance, and government sectors. While these systems support administrative control and operational simplicity, they also accompany structural security weaknesses. A centralized structure creates a single point of failure, meaning that a successful breach, outage, or administrative compromise can expose the entire dataset. Significant breaches over the past decade demonstrate that centralized databases prevail to be primary targets for attackers due to their high-value data concentration **[4]**.

Another critical limitation is scarce user-level data ownership and verification transparency. In many applications, users cannot independently authenticate how their data is accessed, modified, or shared. Excessive administrative privileges and weak audit mechanisms increase exposure to insider threats and unauthorized access **[5]**. Orthodox perimeter-based security models no longer suffice against current distributed attack strategies.

Cryptographic resilience is also an emerging concern. Many deployed systems depend on RSA and ECC-based encryption, which are supposedly vulnerable to future quantum computing attacks**[6].** Security agencies and standards bodies have already emphasized the need to transition toward quantum-resistant algorithms for long-term data protection **[7]**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Furthermore, current monitoring systems are largely reactive, relying on predefined signatures and rule-based alerts. Such methods struggle to detect previously unseen or evolving attack behaviors. Research shows that AI-based anomaly detection significantly improves early threat identification compared to static rule systems **[8]**.

These limitations collectively create the need for a decentralized, privacy-preserving, quantum-resilient, and intelligently monitored data security framework forming the basis for the proposed BlockSecure architecture.

III. OBJECTIVES OF THE STUDY

The primary objective of this research is to design and define a decentralized, privacy-preserving, and future-resilient data security framework capable of addressing the cryptographic limitations of centralized storage systems. The proposed BlockSecure architecture aims to improve data integrity, access control, threat detection, and long-term confidentiality through the integration of multiple advanced security technologies within a unified model.

The specific objectives of this study are as follows:

1. To analyze the security, privacy, and reliability weaknesses of traditional centralized data storage architectures.
2. To design a blockchain-based integrity layer that ensures tamper-evident logging and decentralized trust establishment.
3. To incorporate distributed storage mechanisms which can eliminate single-point failure risks and improve data availability.
4. To integrate post-quantum cryptographic techniques to strengthen long-term encryption resilience against evolving computational threats.
5. To implement Zero-Knowledge Proof (ZKP)–based access verification to enable authentication without data disclosure.
6. To include AI-driven anomaly detection mechanisms for proactive identification of suspicious access patterns or system misuse.
7. To develop a scalable and interoperable framework suitable for deployment across multiple high-trust domains such as healthcare, education, and governance.

These objectives collectively guide the architectural design and evaluation approach of the BlockSecure framework.

IV. LITERATURE REVIEW

Existing research in digital data security considers blockchain technology as a strong base for unalterable record management and decentralized trust establishment. Blockchain-based systems distribute verification across various nodes, reducing dependence on centralized authorities and improving inspection transparency.**[9]** Studies and technical literature validate that distributed ledger mechanisms significantly improve integrity assurance and traceability in high-value data environments **[10]**.

Research in standard network and database security further underlines that centralized architectures remain vulnerable to misuse, aggregation risk, and single-point compromise. Traditional cryptographic protection methods and perimeter-based defenses provide limited protection but rely heavily on correct administrative controls and key management practices **[11]**.

With the expected growth of quantum computing capabilities, researchers and organizations have anticipated post-quantum cryptographic algorithms intended to resist quantum-based attacks. NIST's post-quantum standardization initiative highlights the importance of transitioning toward quantum-resistant encryption models for long-term data confidentiality **[12]**.

Privacy-preserving authentication has also advanced through Zero-Knowledge Proof protocols, which allows one to prove validity without revealing underlying confidential data. **[13]**.

Parallelly, anomaly detection study shows that AI-driven behavioral models outperform static rule-based monitoring in detecting previously unknown threats and irregular access patterns.

However, most prior work considers blockchain integrity, distributed storage, post-quantum cryptography, privacy-preserving verification, and AI monitoring as separate solutions.[**14**] There is inadequate research describing an integrated architecture combining all these components into an incorporated security framework. The proposed BlockSecure model addresses this integration gap.

V. PROPOSED SYSTEM BLOCKSECURE ARCHITECTURE

BlockSecure is aimed to be a layered decentralized security framework designed to offer integrity, confidentiality, privacy-preserving verification, and intelligent threat detection within a unified architecture. The system eliminates single-point dependency by distributing trust, storage, and verification functions across numerous cooperating nodes. Instead of relying on a central authority, BlockSecure combines blockchain logging, distributed storage, quantum-resistant encryption, Zero-Knowledge verification, and AI-based monitoring to produce defense-in-depth protection for sensitive digital data.

The system is organized into five functional layers: integrity layer, storage layer, cryptographic layer, privacy verification layer, and intelligent monitoring layer. Each layer performs a dedicated security role while interoperating through distinct secure interfaces

A. Blockchain Integrity Layer

The blockchain layer maintains tamper-evident logs of all data operations, access requests, and authorization events. Each transaction is cryptographically chained and distributed across partaking nodes, preventing undetected alteration. This layer ensures transparency, auditability, and non-repudiation of actions. Blockchain-based integrity models have been widely

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

recognized for their resistance to record tampering and centralized manipulation **[15]**.

B. Distributed Storage Layer

Instead of storing whole records in a single repository, BlockSecure divides encrypted data into shards and distributes them across multiple storage nodes. Redundant encoding and controlled replication improve availability while restricting breach impact **[16]**. Even if a node is compromised, attackers cannot reconstruct meaningful data without sufficient fragments and keys. This approach reduces aggregation risk and improves resilience compared to centralized databases.

C. Post-Quantum Cryptographic Layer

To ensure long-term confidentiality, the framework uses post-quantum cryptographic algorithms recommended by current standardization efforts **[17]**. These algorithms are designed to resist attacks from both classical and quantum computers. Encryption is applied before storage and during transmission, ensuring end-to-end protection of data fragments and access credentials.

D. Zero-Knowledge Access Verification Layer

Access control is implemented using Zero-Knowledge Proof (ZKP) protocols, enabling users to verify authorization without revealing sensitive credentials or underlying data. This lessens information exposure during authentication and supports privacy-preserving verification workflows **[18]**.

E. AI-Based Anomaly Detection Layer

An AI-driven monitoring module continuously analyzes access patterns, transaction behavior, and node activity to detect anomalies and emerging threats.

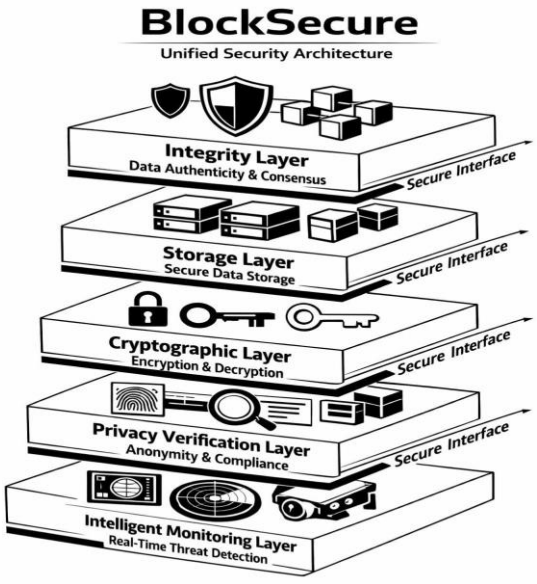

Figure 1. Layered view of BlockSecure structure

VI. METHODOLOGY

This research introduces a conceptual, analytical, and architecture-driven methodology to design and assess the proposed BlockSecure foundation. The study begins with a comparative breakdown of centralized and decentralized data security models to recognize structural vulnerabilities, threat patterns, and flexible mechanisms. Documented infringement reports, security standards, and cryptographic constraints are examined to construct baseline risk factors and protection prerequisites.

A layered system approach is then executed to map security functions uprightness, storage resilience, encryption strength, privacy-conserving verification, and anomaly detection into discrete but compatible architectural components. Each layer is defined in terms of inputs, outputs, reliable boundaries, and attack surfaces. Technology selections such as blockchain logging, distributed storage fragmentation, post-quantum cryptography, and Zero-Knowledge Proof verification are estimated based on published research and standardization recommendations.

Threat scenario modelling is used to examine system behavior under replicate attack conditions, including node compromise, credential abuse, illegitimate access attempts, and partial storage collapse. Instead of physical deployment, first scenario-based architectural substantiation is performed to assess durability, confidentiality conservation, and appraise integrity.

For smart supervision, AI-based anomaly detection models are mapped to the system using behavioral analysis principles derived from anomaly detection research. Assessment criteria include breach containment capability, privacy preservation, decentralization strength, and long-term cryptographic resilience. This structured approach ensures that the proposed framework is assessed through systematic design reasoning and security-focused evaluation

VII. APPLICATIONS AND ADVANTAGES

A. Applications

The BlockSecure framework is fit for deployment across multiple high-trust digital environments where data integrity, privacy, and long-term confidentiality are essential requirements. In healthcare systems, it can be used to protect electronic medical records through decentralized storage and privacy-preserving verification, reducing breach impact while maintaining auditability. In academic and professional management, the framework enables tamper-resistant certificate verification without exposing full records. Legal and governmental document repositories can use BlockSecure to ensure non-repudiable record storage and transparent access logging.

Since the model integrates quantum-resistant cryptography and distributed trust mechanisms, it is particularly suitable for long-retention data scenarios requiring future-proof security guarantees.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

B. Advantages

The proposed architecture offers several advantages over traditional centralized security architectures. By eliminating single-point storage dependency, it significantly diminishes catastrophic breach risk. Blockchain-based integrity logging ensures tamper-evident audit trails, improving accountability and traceability. Distributed storage fragmentation limits data compromise even when individual nodes are compromised. Post-quantum cryptographic protection strengthens confidentiality against emerging quantum-computational threats **[19]**.

Zero-Knowledge Proof–based verification enables validation without data disclosure, enhancing user privacy. Additionally, AI-driven anomaly detection supports proactive threat identification rather than reacting purely defensively **[20].** The layered design also supports modular scalability and domain-specific customization. Collectively, these advantages improve resilience, privacy protection, transparency, and operational trust.

VIII. CONCLUSION

This paper presented BlockSecure, a decentralized security framework designed to address key weaknesses of centralized data storage systems, including single-point failure, limited transparency, and long-term cryptographic risk. The proposed system integrates blockchain-based integrity logging, distributed storage, post-quantum cryptography, Zero-Knowledge Proof–based access control, and AI-driven anomaly detection within a layered framework.

The architecture demonstrates how decentralization, privacy-preserving verification, and smart AI- monitoring can jointly improve data confidentiality, integrity, and auditability. Its modular and scalable design offers functionality across high-trust digital environments.

IX. FUTURE SCOPE

Future work on the BlockSecure framework can focus on prototype implementation and performance testing under real-world workloads. Experimental deployment across distributed nodes would enable measurement of latency, scalability, storage overhead, and fault tolerance. Smart contract automation for access governance and inspection of workflows can be further developed and tested.

Additional research may further include integration with standardized post-quantum cryptographic libraries, federated AI monitoring models, and cross-platform interoperability with existing identity and record systems.

X. REFERENCES

[1] [1] IBM Security, “Cost of a Data Breach Report,” IBM, 2023.
[2] [2] W. Stallings, “Cryptography and Network Security: Principles and Practice”, 7th ed. Pearson, 2017.
[3] [3] J. Benet, “IPFS – Content Addressed, Versioned, Peer-to-Peer File System,” Protocol Labs, 2014.
[4] [4] Jon L. Mills and Kelsey Harclerode, Privacy, “Mass Intrusion and the Modern Data Breach”, 69 Fla. L. Rev. 771 (2017).
[5] [5] IBM Security, “Cost of a Data Breach Report 2023,” IBM, 2023.
[6] [6] Amjad Nsour, “Quantum-Resilient Secure Onboard Communication (QRSecOC): Integrating Post-Quantum Cryptography for Robust Automotive Network Security”, Volume 12, Issue 1, January – February (2025).
[7] [7] Arit Kumar Bishwas, Mousumi Sen, “Strategic Roadmap for Quantum- Resistant Security: A Framework for Preparing Industries for the Quantum Threat”, 2024.
[8] [8] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Computing Surveys, vol. 41, no. 3, 2009.
[9] [9] Saad Ahmed, “Enhancing Data Security and Transparency: The Role of Blockchain in Decentralized Systems”, Feb 2025.
[10] [10] Raymond Farouq, “Implications of Quantum Computing for Health Data Security and Privacy Regulation”, 25 December, 2025.
[11] [11] Dave Micheal, “Resilient Cyber Defense: A Multilayer Approach to Preventing Intrusions in Distributed Environments Using Encryption and Deep Learning”, June, 2025.
[12] [12] National Institute of Standards and Technology (NIST), “Post-Quantum Cryptography Standardization,” 2023.
[13] [13] Yue Zhou, “Efficient Zero-Knowledge Range Arguments and Privacy-Preserving Applications,” July 2024.
[14] [14] Seun Adeoye, “Blockchain-Enabled, Post-Quantum Cryptographic Framework for Securing Electronic Health Records: A Next-Generation Approach to Healthcare Data Protection”, April 2025.
[15] [15] Shreya Khetani, “Data integrity and security: Blockchain vs. traditional databases”, 2025.
[16] [16] Charlotte Taylor, Muhammadu Sathik Raja, “Building Robust Backup Systems: The Role of Data Redundancy, Encryption, and RBAC for Secure Data Recovery”, 2024.
[17] [17] Nehal Narendra Singh, “Post-Quantum Cryptography-Safe Network Architectures: Design Frameworks and Implementation Strategies for Enterprise Zero-Trust Environments”,2025.
[18] [18] Sandeep Gupta, “Zero-Knowledge Proofs for Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond”, Volume 10 Issue 07 July-2025.
[19] [19] Fakhar Rehman, Anwar Abbas, “Quantum-Safe Blockchain Solutions: Protecting Information Security in a Post-Quantum World”, December, 2024.
[20] [20] Subhash Bondhala, “Cybersecurity in AI-Driven Data Centers: Reinventing Threat Detection”, Volume 5, Issue 7, March 2025