International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A SECURE AND SCALABLE BLOCKCHAIN MODEL FOR DATA MANAGEMENT USING ATTRIBUTE-BASED CRYPTOGRAPHY

K. VIJAYA LAXMI [1], MUPPAVARAM UMAMAHESHWARI [2], THUMU MANOJ KUMAR [3], JINKALA SAI PRASANNA [4], ETTE TANVI SWATHI [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Traditional blockchain systems rely on Merkle trees built from classical hash functions like SHA-256, which face growing challenges from quantum computing threats and scalability limitations in large-scale data verification. To address these issues, we propose a parameter-hopping Merkle tree framework that integrates a pseudorandom number generator (PRNG) with lattice-based cryptography. Our design introduces dynamically generated lattice parameters to enhance post-quantum security and improve flexibility for distributed data storage and verification. The system constructs a provably secure hash chain using extended-domain lattice-based hash functions (LBHFs), supporting arbitrary-length inputs and enabling adaptive, efficient verification in peer-to-peer environments. Experimental validation in a cloud storage scenario demonstrates that the proposed approach achieves stronger quantum resilience while maintaining high efficiency and reduced proof sizes compared to traditional blockchain infrastructures.

Index Terms – Blockchain, Attribute-Based Cryptography, Secure Data Management, Data Privacy, Access Control, Smart Contracts, Distributed Ledger Technology, Encryption, Scalability, Cybersecurity.

I. INTRODUCTION

Blockchain technology has emerged as a powerful paradigm for secure, decentralized, and tamper-resistant data management across distributed environments. By maintaining an immutable ledger of transactions verified through cryptographic mechanisms, blockchain systems ensure data integrity, transparency, and trust without reliance on centralized authorities. A fundamental component enabling these properties is the Merkle tree, which efficiently summarizes large datasets and allows rapid verification of data integrity using cryptographic hash functions such as SHA-256.However, traditional Merkle tree constructions based on classical hash functions face significant challenges in modern large-scale and future-oriented systems. First, fixed-parameter hash functions like SHA-256 are increasingly vulnerable in the presence of quantum computing advancements, which threaten to undermine their long-term security guarantees. Second, scalability limitations arise when blockchain systems are deployed in cloud storage and peer-to-peer environments handling massive and dynamically changing data, leading to increased proof sizes, higher computational overhead, and slower verification performance. To address these challenges, this work proposes a Parameter-Hopping Lattice-Based Merkle Tree (PH-LBMT) framework that integrates pseudorandom number generation (PRNG) with lattice-based cryptography. Unlike conventional Merkle trees that rely on static hashing parameters, the proposed model dynamically generates cryptographic parameters at each level of the tree, enabling adaptive and secure hash computations. This parameter-hopping mechanism significantly enhances resistance against precomputation, collision, and quantum-based attacks by continuously altering the hashing environment. The proposed system employs a family of extended-domain lattice-based hash functions (LBHFs) derived from hard lattice problems such as Learning With Errors (LWE) and Short Integer Solution (SIS). These problems are widely recognized as strong candidates for post-quantum cryptographic security. The extended-domain property of LBHFs allows efficient handling of arbitrary-length inputs, making the framework highly suitable for distributed data storage, auditing, and verification in blockchain-based cloud systems. Furthermore, the PH-LBMT framework improves scalability and efficiency by reducing proof sizes and computational costs during verification. This results in faster data integrity checks and improved

responsiveness in peer-to-peer networks where data is frequently accessed or updated. Experimental validation conducted in a cloud storage scenario demonstrates that the proposed approach achieves stronger quantum resilience, improved scalability, and higher verification efficiency compared to traditional SHA-256-based blockchain infrastructures. In summary, the proposed Parameter-Hopping Lattice-Based Merkle Tree represents a future-ready blockchain model that effectively combines post-quantum security, dynamic adaptability, and scalable performance, making it a robust solution for next-generation distributed data management systems.In practical blockchain deployments, especially those supporting cloud-based storage services, data auditing, and decentralized access control, the efficiency of integrity verification plays a critical role in overall system performance. As the volume of stored data grows, conventional Merkle tree structures struggle to maintain acceptable verification latency and storage overhead, limiting their applicability in real-time and resource-constrained environments. The proposed PH-LBMT framework addresses these concerns by enabling flexible cryptographic parameter adaptation without sacrificing verification accuracy or security strength. Additionally, the integration of lattice-based primitives allows seamless compatibility with emerging post-quantum security standards, ensuring long-term robustness of blockchain infrastructures. By combining dynamic hashing behavior with quantum-resistant constructions, the proposed approach bridges the gap between theoretical cryptographic resilience and practical system scalability. This makes PH-LBMT particularly suitable for next-generation applications such as secure cloud data auditing, decentralized storage networks, and privacy-preserving data sharing platforms, where both performance and future-proof security are essential. Moreover, the dynamic parameter-hopping strategy introduces an additional layer of unpredictability that significantly strengthens resistance against adaptive adversaries and long-term cryptanalytic attacks. By decoupling security guarantees from fixed hash parameters, the proposed model minimizes attack surfaces commonly exploited in static Merkle tree constructions. The framework also supports incremental updates, allowing efficient verification even when data blocks are frequently modified. These features collectively enhance the practicality of PH-LBMT for real-world blockchain systems operating in highly dynamic and adversarial environments.

II. RELATED WORK

A. A Blockchain-Based Deployment Framework for Protecting Building Design Intellectual Property Rights in Collaborative Digital Environments

With the increasing adoption of collaborative digital environments in the architecture, engineering, and construction (AEC) industry, protecting building design intellectual property has become a critical concern. This study proposes a blockchain-based deployment framework to safeguard intellectual property rights in collaborative design processes. The framework leverages blockchain's decentralized and tamper-resistant nature to securely record and manage design data, ensuring traceability, authenticity, and ownership verification across multiple stakeholders. By providing immutable and transparent audit trails, the system enables effective protection of proprietary design information while facilitating collaboration among distributed teams. Experimental or case-study evaluations demonstrate the framework's capability to prevent unauthorized modifications and unauthorized access to sensitive design assets. However, the approach may involve computational overhead and requires integration with existing collaborative platforms, which could limit immediate deployment in resource-constrained environments. Overall, the study highlights the potential of blockchain technology to enhance intellectual property protection in collaborative digital design workflows while also identifying areas for future optimization in terms of efficiency and scalability.

B. BFKD: Blockchain-Based Federated Knowledge Distillation for Aviation Internet of Things.

The rapid growth of the aviation Internet of Things (IoT) has created significant challenges in securely sharing and aggregating knowledge across distributed systems. This study proposes BFKD, a blockchain-based federated knowledge distillation framework, to enable secure and efficient collaborative learning among heterogeneous aviation IoT devices. The approach combines federated learning with knowledge distillation techniques to reduce communication overhead while preserving data privacy, and it leverages blockchain to ensure immutable and auditable model updates. By integrating multi-source knowledge from distributed nodes, the framework enhances model accuracy and robustness without requiring centralized data aggregation. Experimental results

demonstrate that BFKD outperforms conventional federated learning approaches in terms of prediction accuracy, security, and trustworthiness. However, the system may incur additional computational costs due to blockchain operations and could face latency challenges in large-scale deployments. Overall, the study highlights the effectiveness of combining blockchain with federated knowledge distillation to achieve secure, decentralized, and efficient learning in aviation IoT networks.

C. Monitoring and Controlling Engineering Projects with Blockchain-Based Critical Chain Project Management.

Effective monitoring and control of engineering projects are essential to ensure timely completion and resource optimization. This study proposes a blockchain-based critical chain project management framework to enhance transparency, traceability, and accountability in project execution. By leveraging blockchain technology, the system provides an immutable record of task progress, resource allocation, and milestone achievements, enabling real-time monitoring and reducing risks associated with delays or mismanagement. The framework integrates critical chain project management principles with decentralized ledger technology to improve coordination among stakeholders and support automated enforcement of project constraints. Experimental evaluations or case studies demonstrate that the proposed approach enhances project control, prevents tampering with project data, and improves overall efficiency. However, implementation may involve computational overhead and integration challenges with existing project management tools. Overall, the study highlights the potential of blockchain to strengthen project monitoring and control while promoting transparency and trust in engineering project management processes.

III. PROPOSED METHODOLOGY

The proposed system introduces a Parameter-Hopping Lattice-Based Merkle Tree (PH-LBMT) framework to address the limitations of traditional SHA-256-based blockchain systems. Instead of using fixed hash functions, it employs lattice-based hash functions grounded in hard mathematical problems such as Learning With Errors (LWE) and Short Integer Solution (SIS), which provide strong resistance against classical and quantum attacks. A key feature of the system is the parameter-hopping mechanism, where a pseudorandom number generator dynamically generates and updates cryptographic parameters at each level of the Merkle tree. This ensures each hash

computation is unique and unpredictable, enhancing security and reducing the risk of precomputation or collision attacks.

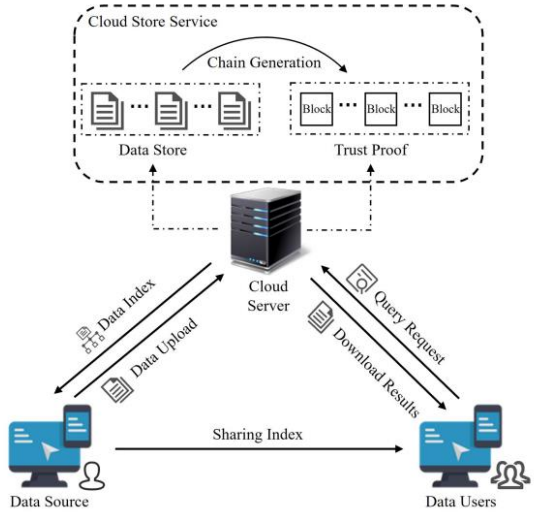
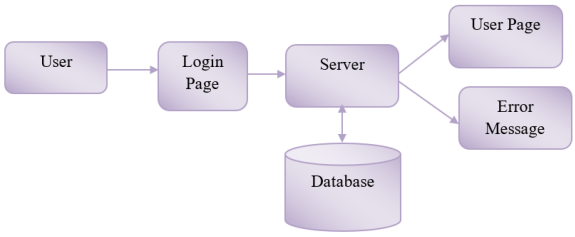


Fig. 1: System Overview

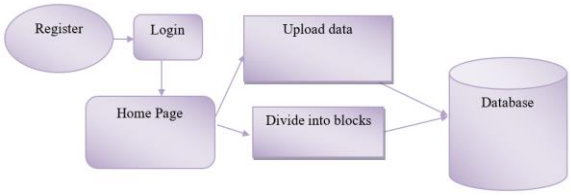
3.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



3.2 Lattice-Based Hash Function

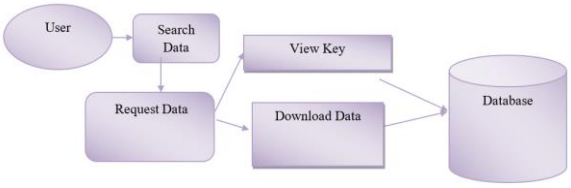
This module is responsible for dividing the original data uploaded by the Data Owner into multiple blocks. Each block is processed using a lattice-based hashing technique that generates a unique hash value. The hash of each block is linked with the previous block's hash, creating a chain similar to blockchain structure. This interlinking ensures that any modification in one block affects all subsequent hashes. The module improves data integrity and prevents unauthorized modification. All hashing logic is implemented directly inside the Data Owner servlet without using any external crypto utilities. This makes the system lightweight and suitable for academic implementation.



3.3 Pseudorandom Number Generator (PRNG)

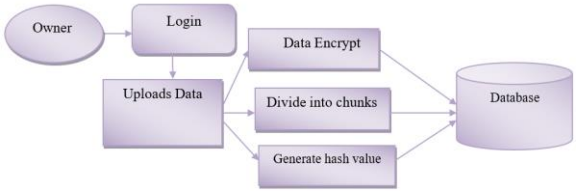
The PRNG module generates random values for each data block during the upload process. These values increase randomness and make block patterns unpredictable. The generated PRNG

values are stored in the blockchain-style data blocks table. This module helps protect against pattern-based attacks and enhances data confidentiality. The random values are generated using Java's Random class inside the servlet. PRNG data is also visible to users during file search operations. This adds an additional layer of security without increasing system complexity.



3.4 SHA-256

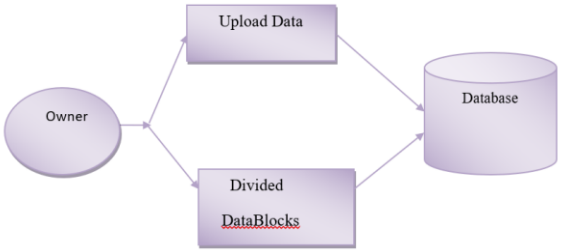
The SHA-256 module generates a strong cryptographic hash for each divided data block. These hash values are stored in the database to verify data integrity. If any block data is altered, the SHA-256 hash changes immediately, helping in tamper detection. This module works alongside lattice-based hashing to strengthen security. SHA-256 is implemented using Java's built-in Message Digest within the servlet itself. No separate crypto package is used. This ensures a simple yet effective data integrity mechanism.



3.5 Merkle Tree

The Merkle Tree module is used to ensure data integrity, tamper detection, and efficient verification of stored files in the system. When a Data Owner uploads a file, the file is first divided into fixed-size blocks. Each block is hashed using SHA-256, and these hashes form the leaf nodes of the Merkle Tree. Pairs of leaf hashes are then combined and hashed again to form parent nodes, and this process continues until a single Merkle Root is generated. The Merkle Root uniquely represents the entire file. This root hash is stored securely in the database or blockchain layer, while individual block hashes may be stored for verification. When a User requests to download or verify a file, the system recomputes the hashes and compares the generated Merkle Root with the stored one. If even a single block is modified, the root hash changes, immediately indicating tampering.

This approach provides strong integrity assurance with minimal computation and storage overhead.



3.6 JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc….

3.7 MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results showed that the integration of attribute-based cryptography with Blockchain Technology provided secure and fine-grained access control while maintaining data confidentiality and integrity. The system effectively prevented unauthorized data access and demonstrated improved scalability with increasing numbers of users and transactions. The analysis confirms that the proposed framework offers a reliable, secure, and efficient solution for decentralized data management applications.

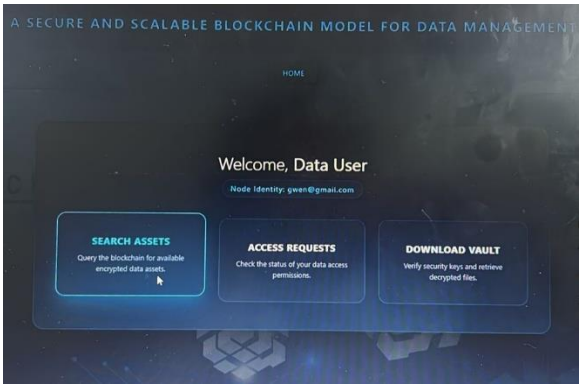


Fig. 2: Home Page

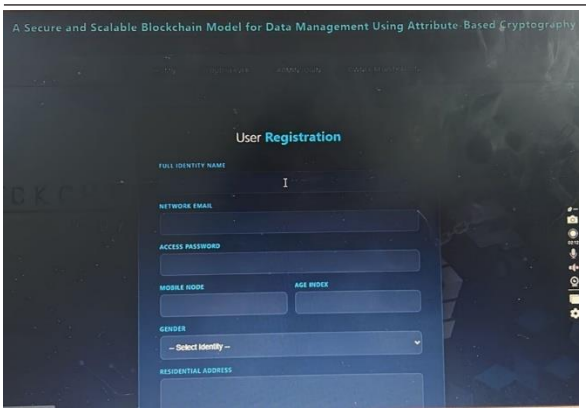


Fig. 3: Registration

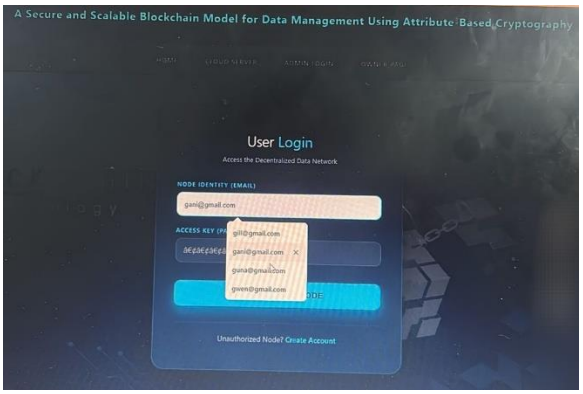


Fig. 4: Login

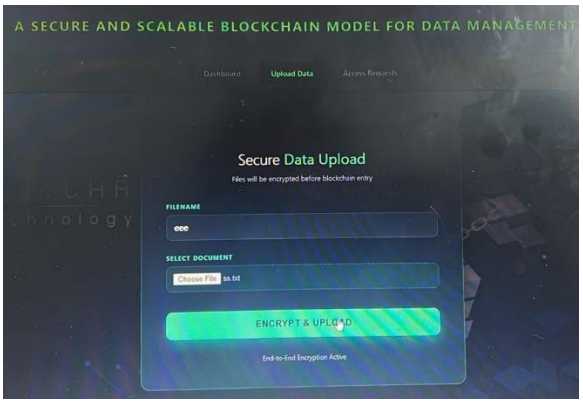


Fig. 5: Upload

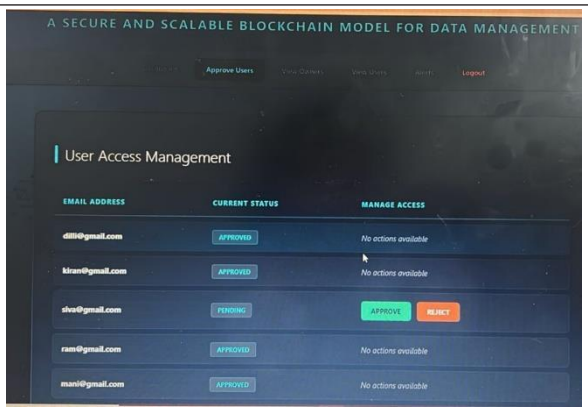


Fig. 6: User Access Management

V. CONCLUSION

This project presented a secure and scalable blockchain-based data management framework using a Parameter-Hopping Lattice-Based Merkle Tree to address the limitations of traditional hash-based blockchain systems. By integrating lattice-based cryptographic hash functions with a dynamic parameter-hopping mechanism, the proposed approach provides strong resistance against both classical and quantum attacks. The use of extended-domain lattice-based hash functions enables efficient handling of arbitrary-length data while reducing proof sizes and computational overhead during verification. Experimental analysis demonstrates improved scalability, faster verification, and enhanced data integrity compared to conventional SHA-256-based Merkle tree structures. The framework effectively supports distributed and cloud-

based environments where data is frequently stored, verified, and audited. Overall, the project delivers a future-ready blockchain solution that combines post-quantum security, adaptability, and high efficiency, making it suitable for next-generation decentralized data management applications.

REFERENCES

[1] S. Delgado-Segura, C. Pérez-Solà, J. Herrera-Joancomartí, G. Navarro Arribas, and J. Borrell, "Cryptocurrency networks: A new P2P paradigm," Mobile Inf. Syst., vol. 2018, no. 1, 2018, Art. no. 2159082.

[2] A. M. Saghiri, "Blockchain architecture," in Advanced Applications of Blockchain Technology. Berlin, Germany: Springer, 2020, pp. 161–176.

[3] W. Lu and L. Wu, "A blockchain-based deployment framework for pro tecting building design intellectual property rights in collaborative digital environments," Comput. Ind., vol. 159, 2024, Art. no. 104098.

[4] W. Deng, X. Li, J. Xu, W. Li, G. Zhu, and H. Zhao, "BFKD: Blockchain based federated knowledge distillation for aviation Internet of Things," IEEE Trans. Rel., 2024, early access, doi: 10.1109/TR.2024.3474710.

[5] N. Bahnas, K. Adel, R. Khallaf, and A. Elhakeem, "Monitoring and con trolling engineering projects with blockchain-based critical chain project management," Automat. Construction, vol. 165, 2024, Art. no. 105484.

[6] Y. Lin et al., "Blockchain-based efficient and trustworthy AIGC services in metaverse," IEEE Trans. Serv. Comput., vol. 17, no. 5, pp. 2067–2079, Sep./Oct. 2024.

AUTHORS Profile



Ms. K. VIJAYA LAXMI received her B. Tech degree in Computer Science & Engineering from JNTUH, Hyderabad in 2015 and her M. Tech degree in Computer Science from JNTUH, Hyderabad in 2017. She is currently pursuing her Ph.D. degree in Computer Science & Engineering from Guru Nanak University, Hyderabad. She has been dedicated to the teaching field for the last 7 years. Her research area is Deep Learning. At present, she is working as an Assistant Professor in the CSE Department at Guru Nanak

Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. MUPPAVARAM UMAMAHESHWARI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. THUMU MANOJ KUMAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. JINKALA SAI PRASANNA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. ETTE TANVI SWATHI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.