International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 3238-3254
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secure data transmission and authentication scheme using advanced blockchain cryptography approach for protecting financial assets in decentralized third party intranet communication

S. Mohamed Iliyas[1]*, M. Mohamed Surputheen[2]

[1*]Research Scholar, PG & Research Department of Computer Science, Jamal Mohamed College (Autonomous), Trichy, Tamilnadu, India.
* **Corresponding Author Email:** iliyasjmc@gmail.com - **ORCID:** 0000-0001-9585-4209

[2]Associate Professor, PG & Research Department of Computer Science, Jamal Mohamed College (Autonomous), Trichy, Tamilnadu, India.
Email: msurfudeen@yahoo.com - **ORCID:** 0000-0003-1491-2740

Article Info:

DOI: 10.22399/ijcesen.2062
Received : 22 January 2025
Accepted : 01 May 2025

Keywords :

security mechanisms
authentication
data transmission
financial assets
blockchain

Abstract:

As the digital landscape advances, the need for robust security mechanisms in the transmission and authentication of data, particularly in financial sectors, becomes increasingly critical. This progressive data transmission and authentication scheme leveraging advanced blockchain cryptography for the protection of financial assets across decentralized third-party intranet communications. Traditional security methods, widely employed in contemporary systems, have exhibited numerous vulnerabilities leading to security breaches, token mismanagement, and susceptibility to packet injections, culminating in compromised security keys. To resolve this. This paper presents an innovative approach leveraging advanced blockchain cryptography to protect financial assets during inter-party communication. The proposed method begins with the generation of a data block based on a Hash Index Policy (HIP) that systematically enhances data integrity. Then create of Proof Of Key Stack (PoKS) for chain link shuffle status and Private keys are generated with role of access rights. Finally, the Peer End Master Node Authentication (PEMNA) verifies the key authenticity to handover the data to ensure the safety to the access right person. The final authentication process is governed by a peer-end master node, which rigorously verifies key authenticity prior to data handover, ensuring that only authorized individuals can access sensitive information. The proposed system demonstrates superior security performance metrics compared to conventional methods, evidenced by enhancements in cryptographic policy compliance, authentication validity, and key verification processes. The proposed system proves higher security performance as well in Crypto-policy enrich standard, proof of authentication, key validation, verification and higher secured true positives rates to allow permissions to improve the security compared to the tradition methods.

1. Introduction

Blockchain technology has developed as a groundbreaking financial security instrument through its distributed system, which produces non-alterable and transparent transaction processes. The distributed ledger method supports blockchain operation through network node verifications without intermediaries and implements security against fraudulent activities [1]. The technology now finds widespread use within financial services, including banking insurance and digital asset management, since it improves data integrity and cybersecurity measures [2]. Financial transactions with blockchain encryption eliminate data modifications while providing full tracking capabilities toward a decentralized, secure platform [3]. The implementation of blockchain technology exists with several significant constraints that limit financial asset protection specifically for decentralized third-party intranets. The present blockchain authentication systems with data transmission protocols face scalability limitations, high computational overheads, and extended transaction delays [4]. Most cryptographic methods operating on blockchain

networks become prone to quantum attack threats and sophisticated hacking attempts [5]. Financial transactions lack a secure authentication system; thus, they become vulnerable to unauthorized access and double-spending attacks. Financial institutions using permissioned blockchain networks face trust issues in secure multi-party transactions because they need an improved cryptographic strategy to protect business transactions.

A Peer End Master Node Authentication (PEMNA) method using advanced blockchain cryptography would resolve these issues through secure data transmission and authentication in decentralized financial systems. PEMNA builds an authentication structure with trusted master nodes who control approved peer participation in financial transactions. The authentication process in PEMNA operates differently from public-private key encryption since it combines multi-factor authentication approaches and zero-knowledge proof technology for improved security. Crypto-hashing with advanced features and fluctuating key generation protects financial operations from damage while preempting potential cyber threats. The proposed scheme uses intranet communication-enabled distributed ledger consensus protocols to minimize transaction speed and maintain data security bounds. Financial institutions using PEMNA as their cybersecurity framework can achieve better protection against fraud attempts along with secure decentralized transactions in digital financial systems.

1.1 Contribution of the paper

- This study proposes an innovative blockchain-based cryptographic system that ensures the secure transmission, authentication, and protection of sensitive data in decentralized third-party intranet communications.
- It proposes using a HIP to systematically enhance data integrity by structuring financial data blocks as tamper-resistant.
- For security at the block level, a new BL-OPMSES is introduced that uses SHA-256 for block encryption.
- Implementing RSPSA allows for the dynamic shuffling of block order, enhancing security from sequential data exposure.
- A PoKS is created to monitor the chain link shuffle's status and ensure robust key management without modification access.
- By implementing the PEMNA mechanism, users are prevented from retrieving sensitive financial data without proper key verification to ensure the authenticity of the user.
- The proposed framework has higher throughput, lower authentication validation, encryption decryption time, transaction latency, storage overhead, and communication overhead, improving overall security compared to existing systems.

2. Literature Survey

According to a data trading platform [6], there are more issues in the financial threat; the problem is required to focus on blockchain technology to be used in the secure and enhanced reliability of the dataset. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a method used to improve data privacy, and healthcare and e-commerce departments are used for more datasets to be maintained securely. However, the process is in a high-cost range because the process is more power-consuming.

Blockchain technology means that all data sets are secure and reliable. Still, more data integrity issues are required to solve the method, which uses a Merkel Hash Tree (MHT) process in the data exchange [7]. The process enhances the data-driven and mismatching data-solving process. The method uses encryption algorithms to secure the data. However, the technique has a s ow performance because of the step-by-step process.

Supply Chain Network is a more significant threat to financial data is an issue; the process is focused on blockchain technology to enhance data privacy and ensure that all kinds of data a reliability [8]. The Proxy Encryption Model (PEM) is used for all datasets that are encrypted in the process and have a high level of performance. The method has high accuracy in the result; however, the technique has a limited capacity range due to not being occupied by a larger dataset.

Data privacy is not adequately maintained in the financial system due to the threat in datasets; the processes used in blockchain technology are secret and reliable of the central concept but sometimes mismatch the data [9]. The required issue used in the Zero Knowledge Proof (ZKP) is used all data is properly maintained, testing the process and measuring in the real-time data analysis. However, the process is average accurate

and results low level of efficiency.Cryptography is required in the financial data threat process but has low accuracy and average scalability [10]. The process is based on blockchain technology and is focused on the structure of the datasets due to its use in the Peet-to-Peer Network (PPN), which is more scalable and structured for all datasets. The process involves direct communication in the network. However, because of the complex network structure, it is a storage problem.Table 1 demonstrates the data secured based on blockchain technology using encryption and decryption algorithms and the author's previous structure's method, limitation, and used dataset, achieved result.

Table 1. *Data Secure Based on The Blockchain Technology Using Encryption and decryption algorithm*

Author/year	Method	Used dataset	Achieved result	Limitation
Chen, Y et al.,2020	Hyperledger Fabric	Chain channel code	95%	More Memory space is occupied.
Banupriya, S et al.,2021	Lattice-based hierarchical deterministic key generation (LB-HDKG)	Structure Data	98%	Blockchain has been one factor that hinders its practical application
Volodymyr et al 2021	Distributed Ledger (DLT) Technology	Digital Data	93%	Blockchain technology based on encryption has more potential errors
Masood, I et al 2024	Blockchain-Based Access Control Model (BBACM)	Binary data	91%	The data is secure proof and maintained at a high cost.
Yunsen Wang et al 2019	(ZKP)	Encrypted data	98%	The stake is a level of limited capacity.
Kangning Zheng et al 2021	Proof of Stake (POS)	Structure data	92%	More memory space is occupied
Z. Su et al.,2020	Proxy re-encryption technology	Encrypted Data	95%	The method is more steps included and slow performance
KM Deepika et al.,2022	Crypto-Proof of Stake (CPoS)	Numerical data	89%	Low reliability of the process
W Zhao et al.,2023	Merkel-tree	sensing data	90%	Data secure verification of the process is slow.
G Manoharan et al.,2022	Blockchain assisted secure data sharing model (BSDS)	Correlation data	82%	More power is consumed

Table 2. *Survey of the Various methods for Financial Security*

Author/Year	Used Method	Dataset	Performance Analysis	Drawback
Jiang L et al., (2024)	Blockchain-based Financial Sharing Algorithm (BFSA)	Financial accounting data	data tampering rate = 8%,	Existing obstacles include regulatory uncertainties, scalability, and technical issues that could impede widespread acceptance.
Almadadha, R et al., (2024)	Blockchain Technology	ESG reports	data accuracy = 25%	This approach has a particular stake in financial ESG reporting due to the expensive implementation costs alongside standardization requirements across distinct domains_ industries.
Chen et al., (2023)	Novel thinking exploration method	Case studies of financial institutions	transaction processing time = 40%, operational costs = 50%	It poses the problems of reluctance to adopt new innovations and the fusion of blockchain technology with current systems in finance being overly complicated.
Mhlanga, D et al., (2023)	Blockchain Technology	Case studies on blockchain applications	transaction fees = 35%	Illiteracy coupled with low internet penetration in remote locations was emphasized as a barrier preventing the realization of blockchain's full

				potential for decoupled financial inclusion.
Wu, H et al., (2024)	Proof-of-Work (POW), Proof-of-Stake (POS)	multiple financial institutions	transaction transparency = 45%,	These were asserted as serious limitations to blockchain technology, knowledge transfer, and even undergo documented identity verification and regulatory compliance.
Zhang, L et al., (2020)	Blockchain Technology	financial institutions	data security = 50%	The proposed method has limited access caused by regulatory restrictions, significant scaling challenges, and lacking solid technology networks.
S. Singh et al., (2016)	Exploration of blockchain	financial institutions	security breaches = 70%, data integrity = 60%	These methods serve to demonstrate the viability of tackling the issue of energy inefficient power usage associated to certain mechanisms of blockchain consensus.
Binghui Wu et al., (2019)	R3CEV, Hyperledger and Qiwi	financial markets	transaction settlement times = 50%, market transparency = 45%	Blockchain implementation in financial markets will have to deal with scalability issues and resistance from legacy systems due to the transformation of business models.
Onteddu eta l., (2020)	Blockchain Technology	FinTech Database	security = 65%, system efficiency = 50%	The drawback that is noted in this method is an issue of scaling, as performance latency may prevent these systems from managing large quantities of transactions smoothly.
Amponsah et al., (2022)	Cloud-based blockchain framework	health insurance claim data	security = 89%	The difficulty of incorporating blockchain into current health insurance systems and skepticisms of existing users who don't understand blockchain technology.

A Blockchain-Based Accounting Information Sharing System (BBAISS) was developed to improve enterprise-level financial data exchange [31]. The smart contracts used for automated validation and the Distributed Ledger Technology (DLT) employed for transaction integrity guarantees make the assurance of security and immutability achievable. Nevertheless, the system shows some computational overheads which cause higher processing time and limits scalability for high volume financial data transactions. To improve financial risk forecasting, an Optimized BP Neural Network (OBPNN) model has been proposed [32], which individually selects features and performs weight optimization to achieve better accuracy. This approach for more advanced risk assessment in financial management is based on the adoption of past financial trends, which is beneficial. However, the heavy reliance on historical financial data makes it inflexible to unexpected changes in the economies or external financial shocks, which limits effectiveness in volatile markets.To strengthen trust between stakeholders in the supply chain while mitigating scam strategies, a Multi-Layered Smart Contract Model (MSCM) was developed [34] on top of blockchain SCF to automate financial transactions. While this model helps reduce fraud attempts by automating the execution of contracts under set parameters, the legislation and regulations surrounding the model's widely use is capped due to inconsistency of compliance standards across regions. In Supply Chain Finance (SCF), a Consortium Blockchain for Credit Sharing (CBCS) has been proposed [33] for enabling secure and transparent exchange of credit information between businesses and financial institutions. The system augments trust and minimizes the chances of fraudulent activities through the use of automated validation processes, nevertheless, some areas still require improvement. The employed consensus mechanism comes with severe latency problems which causes delays in the transaction confirmations thus affecting the real time assessment and decisioning of credits.

To enhance the use of blockchain in supply chain finance (SCF), a Permissioned Blockchain Based SCF System (PBSCFS) framework built on Hyperledger Fabric has been proposed [35]. This approach improves the security, traceability, and prevention of transactional frauds through the usage

of permissioned access control systems. In spite of its advantages, the PBSCFS system suffers from lack of adoption due to its expensive infrastructural requirements and difficulties with interfacing with older financial systems.

3. Proposed Method

In this section, we briefly describe the performance of the proposed method for protecting financial assets in decentralized third-party intranet communication. To run the proposed method with security, we used the Finance Data dataset taken from the Kaggle website. In this proposed method, we perform five phases: generation of the data block, data encryption at the block level, altering the block order, chain link shuffle, and key authentication. For the first phase, a HIP is deployed next; in the second phase, a BL-OPMSES method is deployed, then to alter the block order, we use RSPSA; in the fourth phase PoKS method was proposed, finally the PEMNA method was proposed for key authentication. In below figure 1 we illustrate the architecture diagram of the proposed method.

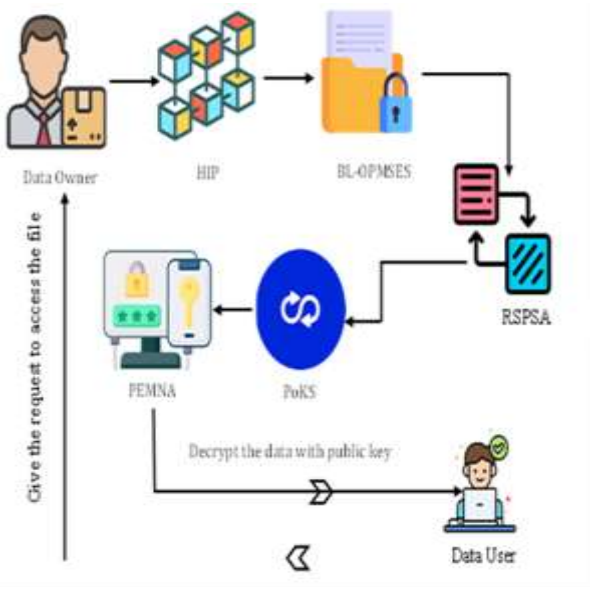

Figure 1. *Architecture diagram of the proposed method*

In the first phase, a HIP generates the data blocks to enhance financial asset data integrity systematically. In this method, each data block receives a unique tamper-resistant index value through cryptographic hash functions that enable verification. The system guarantees strong data security, financial regulation compliance, and defense against fraudulent activities. By following in the second phase, the BL-OPMSES is used to segment the communication data into packets and is stored into generated blocks with more security. The SHA-256 hashing verifies data integrity through SHA-256 hashing, yet the poly matrix shuffle technique adds encryption strength by preventing cryptographic attacks during transmission. Then, we use the RSPSA method to enhance the security, which dynamically alters the block order within the blockchain. Through integrating RSPSA with the BL-OPMSES, financial asset data maintains structural obfuscation and encryption to ensure complete confidentiality. Then, create PoKS for chain link shuffle status, and Private keys are generated with the role of access rights. This innovative layer of security is complemented by creating a proof of key stack to manage the chain link shuffle status effectively. Finally, we use the PEMNA method to verify the key authenticity to hand over the data to ensure the safety of the access right person. PEMNA protects financial operations with digital asset exchanges and secures investment records by preventing fraud and cyber threats.

3.1 Hash Index Policy (HIP)

The Hash Index Policy (HIP) method creates data blocks through this section to enhance financial asset data integrity. Each data block in HIP receives a unique tamper-resistant index value through cryptographic hash functions that enable verification. The policy's hashing mechanisms, the solution stops unauthorized changes to data and enables safe data deduplication to decrease storage expenses while sustaining authenticity. Protecting transactional records, financial fraud risk reduction, and regulatory compliance requirements depends on HIP to function effectively in financial systems. Through HIP integration with blockchain distribution technologies, financial data becomes more unalterable and traceable, thus producing more substantial asset management transparency and improved trust. Each B_i data block obtains its distinct hash index using the $H(x)$ cryptographic hash function.

$$H_i = H(B_i) \qquad (1)$$

A cryptographic hash function generates unique hash indexes during the first step of equation 1, which gets applied to financial data blocks. The system generates $H_i = H(B_i)$ as the hash value once a new data block B_i appears. The cryptographic hash operation creates an unalterable fingerprint to recognize each data block independently and guarantees new data hash values when any modification occurs. The system stores financial record data with these hash indexes to validate document integrity throughout its lifespan. Before releasing retrieved data block B_i', its hash

value $H(B_i')$ undergoes a comparison test with H_i stored in the index to confirm data integrity.

$$H(B_i') = H_i \quad (2)$$

The verification process uses Equation 2 to retrieve data block B_i', which must match the previous hash index H_i. The authenticity of the data remains unchanged whenever $H(B_i')$ is obtained. Any data alteration or corruption would be identified through a hash mismatch condition ($H(B_i') \neq H_i$). The system detects unauthorized modifications in real time for financial records through this capability, which keeps all data trustworthy and unchanging. A Merkle tree allows HIP to prove large data set integrity through hash storage at leaf nodes with recursive parent computations for each node.

$$H_{parent} = H(H_{left} || H_{right}) \quad (3)$$

A leaf node within this equation stores hash data from each data block, but recursion through $H_{parent} = H(H_{left} || H_{right})$ calculates the parent nodes. To verify a specific data block, users must inspect minimal hash subsets rather than scan through the complete dataset. The established data protocol ensures high performance and security when tracking financial assets, enabling blockchain applications with distributed ledger technologies.

$$H(B_{new}) \neq H(B_{existing}) \Rightarrow Store\ B_{new} \quad (4)$$

Every instance of financial data storage is reduced by HIP, thus maximizing storage efficiency. The system compares $H(B_{new})$ to available hash values during the introduction of new data block B_{new}. A new data block receives individual storage status when the hash value between $H(B_{new})$ and $H(B_{existing})$ fails to match. New data blocks that match previously stored hashes in the system do not need storage since they are recognized as duplicates and will reference the existing blocks. Through its deduplication system, data storage expenses decrease without harming information accuracy.

$$H(K_{user}) = H_i \Rightarrow Access \quad (5)$$

User access rights verification happens through key-based hashing, as described in Equation 5. Users receive individual access keys denoted as K_{user} that undergo hashing before checking against hash indices that store financial data blocks. When $H(K_{user}) = H_i$, the system enables permission A for the user to access or modify the requested data. Access is denied when the access key comparison fails to match the stored hashes thus initiating authorization procedures for database administrators who can approve or reject delayed access procedures. The system guarantees strong data security, financial regulation compliance, and defense against fraudulent activities in the system.

3.2 Optimal Advances Poly Matrix Shuffle Encryption Standard (BL-OPMSES)

The security measures of the platform are strengthened through the implementation of the SHA-256 Optimal Advances Poly Matrix Shuffle Encryption Standard (BL-OPMSES) algorithm for block-level encryption efforts. The SHA-256 hashing verifies data integrity through SHA-256 hashing, yet the poly matrix shuffle technique adds encryption strength by preventing cryptographic attacks during transmission. Through a programmed encryption process of separate blocks, BL-OPMSES establishes secure data protection, which remains unreadable to unauthorized parties who lack proper decryption keys. The encryption methods create secure data transmission while protecting monetary operations and reaching data protection requirements.

$$D = \bigcup_{i=1}^{n} P_i, : P_i \subset D \quad (6)$$

The first step in managing financial asset data involves dividing D into smaller fragments P_i to optimize security enforcement and efficient handling. The formula delivers improved methods for data processing, along with encryption and storage management, to prevent any unauthorized party from accessing the complete data set. Financial records are converted to packets P_i to enable structured data security deployment alongside high availability and contain transaction logs, asset ownership details, and compliance reports.

$$H_i = H_{SHA-256}(P_i) \quad (7)$$

The SHA-256 hashing algorithm protects data from changes by operating on each packet P_i, which produces the unique fingerprint H_i. Financial records can detect unauthorized modifications and detect illegal changes to transactions, unlawful fund movements, and deceptive record updates through the implementation of Equation 7. Financial regulatory requirements depend on the hashing methodology to maintain solid traces of all financial transaction records independently from tampering attempts.

$$C_i = E_O(P_i, K) \quad (8)$$

The data packet processing includes block-level encryption by applying the SHA-256 BL-OPMSES E_O function following the hash operation. Secure encryption key K allows the encryption function E_B to convert plaintext packets into ciphertext C_i. Financial assets protected by this equation stay secure and unalterable even when communications are intercepted between processing servers. Financial organizations and authorized entities can access original financial data through the correct decryption procedure.

$$S(C) = \pi(C_1, C_2, \dots, C_n) \qquad (9)$$

The security measures include poly matrix shuffling, which applies secure permutation function π to encrypted packets $S(C)$ to perform randomized block reordering. The randomized order creates such a complex structure that no matter how much cryptographically protected data an attacker can access, it is virtually impossible to extract useful information. Conducting this security measure is essential for protecting high-stakes financial operations while defending against pattern detection attacks during digital banking and asset management platform anti-fraud systems.

$$P_i = D_O(C_i, K) \qquad (10)$$

The protected financial record packets need to be reversed through shuffling to return their initial arrangement before users authorized for them can access them. The BL-OPMSES decryption function D applies to decrypt the data. Financial data can be secured for auditing and regulatory reporting purposes through the K decryption key application, which enables the system to restore plaintext packets P_i.

$$H_i' = H_{SHA-256}(P_i'), \Leftrightarrow H_i' = H_i \qquad (11)$$

Once the system decrypts the packets it verifies their validity by comparing their renewed hash value H_i' to the original hash value H_i. The system maintains data authenticity when it calculates H_i' equal to H_i. The system identifies data corruption and unauthorized modification or security vulnerabilities when H_i' does not equal H_i. The tested data verification method protects financial institutions from fraudulent activities and ensures authorized modifications remain unaltered while preventing non-compliance with regulations. In figure 2, we illustrate the workflow process of the BL-OPMSES method. The work begins with converting financial data into P_i to enable

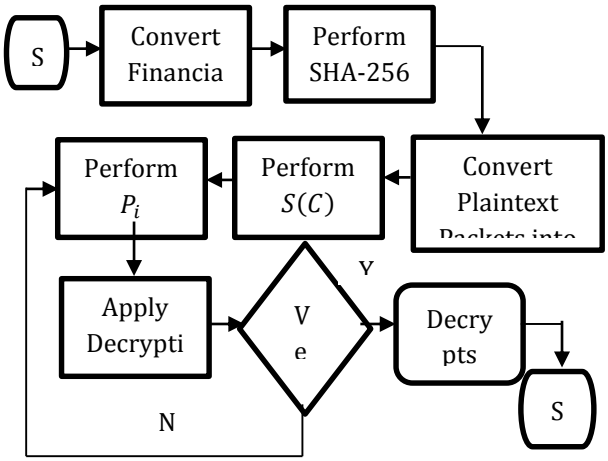

Figure 2. *Flowchart Diagram of the BL-OPMSES method*

structured data security deployment alongside high availability and containing transaction logs, asset ownership details, and compliance reports. We perform SHA-256 H_i to protect data from changes by operating on each packet P_i, which produces the unique H_i. After that, convert plaintext packets into C_i to stay secure and unalterable even when communications are intercepted between processing servers. Then, performing $S(C)$ to create such a complex structure makes it virtually impossible to extract valid financial data when an attacker can access it. Then apply D function to decrypt the data for auditing and regulatory reporting purposes. Then verify the H_i' to verify the validity. If it is true, decrypt the packets else return to the perform P_i to check the validity.

3.3 Random Shuffle Padding Block Level Shifting Algorithm (RSPSA)

The Random Shuffle Padding Block Level Shifting Algorithm (RSPSA) establishes dynamic encryption block ordering within the blockchain to enhance its security measures. The method intentionally scrambles the natural arrangement of stored data to make attacks based on pattern recognition and unauthorized reconstruction more challenging to achieve. Through integrating RSPSA with the BL-OPMSES, financial asset data maintains structural obfuscation and encryption to ensure complete confidentiality. Partially exposed blockchain information does not enable adversaries to trace transaction patterns because the algorithm deploys randomized padding and shuffling implementations. The adaptive security layer provides better protection for financial data through its ability to reduce transaction correlation risks and strengthen resistance against cryptographic attacks in decentralized ledger systems.

$$H_i = H_{SHA-256}(B_i)$$
$$C_i = E_O(B_i, K) \quad (12)$$

The system utilizes SHA-256 to hash B_i, so H_i becomes unique fingerprints that detect unauthorized modifications. The BL-OPMSES acts to encrypt the block into ciphertext known as C_i. The encryption system guarantees that financial records stay secure because it protects asset transfers, transaction histories, and investment data from unauthorized access while keeping them tamper-proof.

$$C_i' = C_i || P(C_i) \quad (13)$$

Before storage, each padlock-protected block receives added security by receiving random sequence P padding C_i'. The padding operation $P(C_i)$ produces unique encrypted versions of identical financial data to stop adversaries from detecting such patterns. The security priority of this technique protects financial records from statistical attacks because it renders unauthorized extraction of valuable data impossible regardless of multiple encrypted block inspections.

$$S(C') = \pi(C_1', C_2', \dots, C_n') \quad (14)$$

RSPSA adopts encryption and padding methods before performing a block order shuffling process through the random permeation function π. RSPSA shuffles the equation in the blockchain sequence, making it impossible for attackers to connect financial records or rebuild transaction timelines. RSPSA achieves improved financial transaction confidentiality through its method of block position randomization because attackers cannot decipher intercepted data when the correct decryption and reshuffling process is absent.

$$(C_1', C_2', \dots, C_n') = \pi^{-1}\big(S(C')\big)$$
$$C_i = R\left(P(C_i')\right) \quad (15)$$
$$B_i = D_O(C_i, K)$$

The authorized entity can access financial data by implementing the inverse permutation function π^{-1} to unshuffled block orderings before removing padding and running BL-OPMSES decryption with key K. The decryption mechanism applies BL-OPMSES decryption function to financial asset data after padding removal using the valid key K. The controlled access enables only authorized users holding decryption privileges to restore transaction records.

$$H_i' = H_{SHA-256}(B_i') \Leftrightarrow H_i' = H_i \quad (16)$$

When data retrieval concludes, the system rehashes all obtained financial data blocks with SHA-256 before confirming that the hash values match their initial H_i values. Data authenticity is proven when the recorded and original hash values synchronize. The system detects unauthorized modifications and potential breaches by comparing original hashes against calculated values but reports such incidents in real time. Verification is vital in creating unmodified financial registers that demonstrate auditing preparedness, regulatory adherence, and digital asset protection needs.

3.4 Proof of Key Stack (PoKS)

Proof of Key Stack (PoKS) generates chain link shuffle status in this section, while private keys use access rights during generation. The key stack-proof system establishes an advanced security layer which helps manage chain link shuffle status reliably. The assignment of private keys through defined access rights allows users to create a protected framework for data protection when making transactions. PoKS integration makes each transaction subject to cryptographic validation procedures that authenticate user access and ensure blockchain data remains shuffled. The implemented security approach defends financial assets through secure access controls that protect confidential transactions and guard against unauthorized modifications in financial systems.

Algorithm 1: PoKS for chain link shuffle status

Start

Phase 1: Key Stack setup

State the R system roles {Admin, User, Validator}

For system wide encryption:

Create the master Key pair

$$\left(K_{pub}^{root}, K_{priv}^{root}\right)$$

Set $K_{stack} = \emptyset$

End for

Phase 2: Create the private key based on access of role-based

For every role $r \in R$:

Create the unique pair for the private and public key

$$\left(K_{pub}^{T}, K_{priv}^{T}\right) = KeyGen()$$

According to access rights A allocate the permission of K

$$A\left(K_{priv}^{T}\right) = \{Read, Write, Validate\} \forall R$$

Deploy K_{priv}^{T} in PoKS

$$K_{stack} \leftarrow K_{priv}^{T}$$

End for

Phase 3: Status Verification of Chain Link Shuffle

Recover encrypted blocks

$$C = \{C_1, C_2, \dots, C_n\}$$

After recovered C verify block integrity through Proof of Shuffle

First evaluate the H hash of shuffle sequence

$$H_{shu} = H_{SHA-256}\left(\pi(C_1, C_2, \dots, C_n)\right)$$

Then the stored shuffle proof H_{st} with H_{shu}

If

$$H_{shu} \neq H_{st}$$

flag inconsistency

else

save $H_{shu} = H_{st}$

valid in PoKS

end if

Phase 4: Verify transaction authorization and validation of access

For T_i every request transaction from U user:

Recover r user role and K_{priv}^{T}

Then perform key legitimacy Verification V through digital signature authentication

$$V\left(K_{priv}^{T}, PoKS\right)$$

If (V=True):

Proceed with T_i transaction

Else

Access Denied

End if

End for

Phase 5: T_i execution of secure data

Encrypt T_i by utilizing key structure of PoKS

$$C_{T_i} = E\left(T_i, K_{priv}^{T}\right)$$

Add on C_{T_i} to blockchain

Phase 6: Constant Monitoring of PoKS Integrity

Verify the PoKS structure integrity through periodically

Update role-based assignments while scanning for keys that have expired or been invalidated.

Verify again H_{shu} and H_{st}

Stop

The algorithm 1 provides safe management of encryption keys, distribution control, and blockchain link validation for financial transactions based on blockchain systems. The system uses a method to produce private keys that comply with authorized access rights automatically; thus, it protects confidential transactions and secures processed blockchain data distributions. The Protocol for Key Management and Access Control provides financial asset transactions with security through its role-governed system and protection from unauthorized access. It also upholds blockchain ledger shuffle integrity.

3.5 Peer End Master Node Authentication (PEMNA)

The Peer End Master Node Authentication (PEMNA) operates as the financial asset transaction framework's termination point to verify authentic access to sensitive data by authorized personnel. A peer-end master node executes PEMNA by verifying private key authenticity

before allowing data access. PEMNA protects financial operations with digital asset exchanges and secures investment records by preventing fraud and cyber threats. The data handover process in PEMNA can only be completed following successful key verification to maintain data security through multiple layers of protection for financial asset management platforms.

$$A_{req} = \left(U_i, K_{priv}^{U_i}\right) \quad (17)$$

To verify identity, the requesting user sends their private key $K_{priv}^{U_i}$ from their account. During this step, verification guarantees authorized personnel exclusive access to financial records, asset ownership information, and transaction documentation. After submitting the authentication request A_{req} the PEMNA system becomes responsible for verification tasks. The procedures set up by PEMNA protect valuable financial data from unauthorized persons, which maintains its availability only for authorized individuals.

$$V\left(K_{priv}^{U_i}, PoKS\right) = \begin{cases} 1, & if\ K_{priv}^{U_i} \in PoKS \\ 0, & otherwise \end{cases} \quad (18)$$

The PEMNA system validates the received private key by verifying it against the PoKS to check its validity and any current revocation or non-existence behavior. The system grants authentication when the key appears in PoKS, confirming the authorized user status for financial record access. Any attempt to access the system leads to denial when security breaches or policy changes have invalidated the provided key or left it undiscovered in the system. The access control system implements this step to provide strong protection against unauthorized modifications of digital assets, investment portfolios, and transaction records.

$$M_{status} = H_{SHA-256}\left(ID_{U_i} || T_{OTP}\right) \quad (19)$$

The system implements multi-factor authentication (M) to strengthen security through an additional requirement of user identity verification. The system creates One-Time Passwords (OTPs), which connect to specific user individuality, making it impossible for identity thieves to access accounts even if they capture the private keys. Using SHA-256, the system conducts safe verification of authentication requests through a hash process of user IDs and OTPs. The system authentication system accepts input when the generated hash value matches what is stored as M hash.

$$M_{valid} = \begin{cases} 1, & if\ M_{status} = M_{std} \\ 0, & otherwise \end{cases} \quad (20)$$

The described equation strengthens financial security by defending against phishing attacks, credential theft, and fraud attempts.

$$Access_{decision} = \begin{cases} 1, & if\ V\left(K_{priv}^{U_i}, PoKS\right) = 1\ and\ M_{valid} = 1 \\ 0, & otherwise \end{cases} \quad (21)$$

PEMNA completes the access decision analysis only after verifying the private key and confirming the M status. When M validation and key verification procedures are successful, users can access requested financial records. After this verification, the system triggers access denial and a corresponding security alert to block unauthorized attempts. The decision grants access only to verified stakeholders, such as investors, financial managers, and auditors, who possess the required keys for accessing confidential financial transactions, thus minimizing potential fraud risks.

$$D_{encrypted} = E\left(D_{financial}, K_{pub}^{U_i}\right)$$
$$D_{decrypted} = D\left(D_{encrypted}, K_{priv}^{U_i}\right) \quad (22)$$

After successful authentication, the system encrypts $D_{financial}$ financial data using the recipient's public key before sending it. The encryption is so strong that intercepted data cannot be read. After successful delivery, the user completes the decryption of financial records using their verified private key. The encryption-decryption process safeguards financial transactions by maintaining data confidentiality in ways that meet the industry's regulatory standards. As illustrated in figure 3 we input $K_{priv}^{U_i}$ to perform A_{req} to validate $K_{priv}^{U_i}$, if $K_{priv}^{U_i}$ is true perform M_{status} else return to check $K_{priv}^{U_i}$. We generated the hash value by perform M_{status}, after generated the value perform the M_{valid}, if True perform

Table 3. *Simulation parameters*

Parameters	**Values processed**
Name of the Dataset	Finance Data
Used Tool	Visual studio .net frame wrok
Used Language	C#.Net
Number of data/users	4567/ 200
No of attributes	24
Testing/training	7:3 ratio

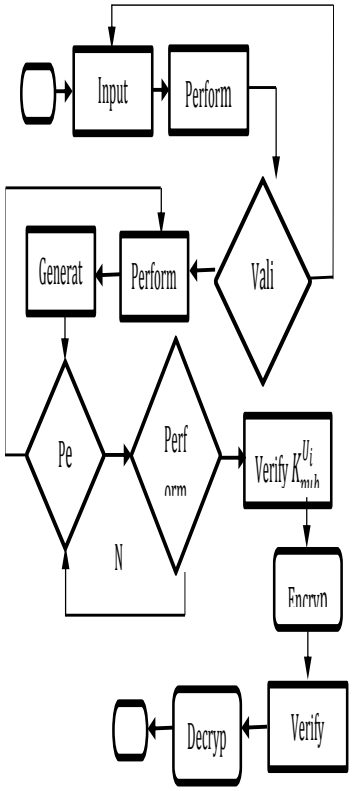

Figure 3. *Flowchart Diagram of the PEMNA*

$Access_{decision}$, else recheck the M_{status}. Then perform $Access_{decision}$ function to authenticate the private key and public key. If private key and public key are True it goes to verification process, else return to the M_{valid}. In verification process there two steps were involved like first verify the $K_{pub}^{U_i}$ its true the $D_{financial}$ data encrypted by the data owner, after encrypted the data, then verify the $K_{priv}^{U_i}$ its true decrypt the $D_{financial}$ data to the user.

4. Result and Discussion

This section examines how the proposed PEMNA scheme performs through the Finance Data dataset analysis. A performance comparison of PEMNA occurred versus CP-ABE, MHT, PrivySharing, and Hyperledger Fabric methods. The performance evaluation consisted of significant metrics, including authentication validity rate, encryption & decryption time, transaction latency, throughput and storage overhead, and communication overhead. The authentication validity rate demonstrates how correctly authorized users receive their permissioned access. The evaluation method measured encryption and decryption duration to determine computational method speed. Blockchain verification and the addition of transactions to the network depend on transaction latency, representing the verification period. The system efficiency can be measured through Transactions Per Second (TPS,) which indicates throughput data. The system network consumes and authenticates peers optimally, enabling improved transaction capacity because key verification processes run faster. The storage overhead describes how much additional space cryptographic operations and data handling operations require. The analysis evaluated the communication overhead which appears as network protocol usage needed for authentication alongside encryption processes.

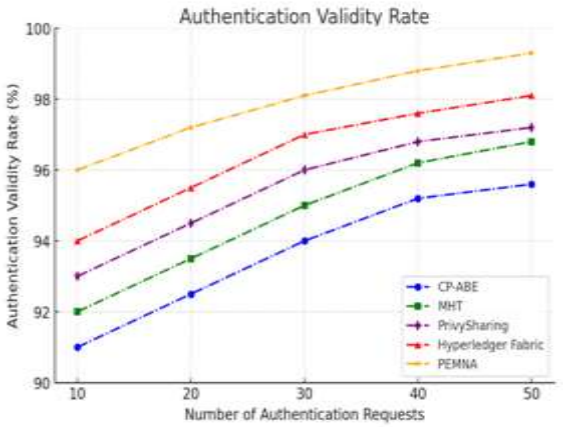

Figure 4. *Performance Analysis of Authentication Validity Rate*

Table 4. *Performance Analysis of Authentication Validity Rate*

Authentication Requests	CP-ABE (%)	MHT (%)	PrivySharing (%)	Hyperledger Fabric (%)	PEMNA (%)
10	91.5	92.5	93.5	94.5	96.0
20	92.8	94.0	94.8	96.0	97.2
30	94.0	95.3	95.8	97.0	98.0
40	95.0	96.5	96.8	97.8	98.8
50	95.5	97.2	97.4	98.5	99.2

An authentication mechanism establishes its value through the authentication validity rate, indicating how well it verifies legitimate users while stopping unauthorized access attempts. The security of a system improves as its authentication validity rate increases, thereby reducing both false authorization and incorrectly denied access attempts. The authentication validity rates for CP-ABE, MHT, PrivySharing, Hyperledger Fabric, and PEMNA are

compared in Figure 4 and Table 4 regarding Finance Data. PEMNA delivers the highest authentication validity rate among the methods, guaranteeing reliable security in decentralized financial operations.

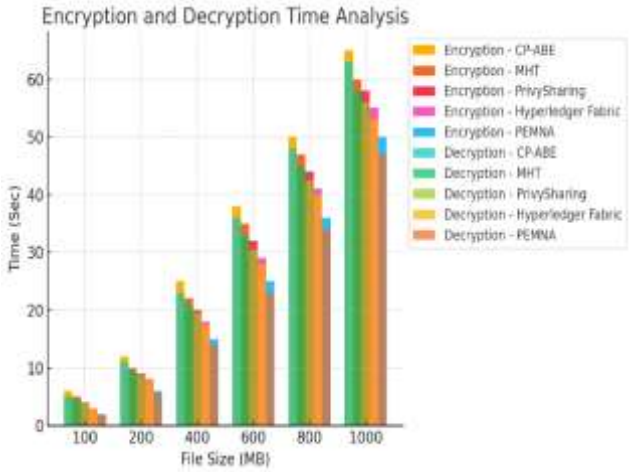

Figure 5. *Performance Analysis of Encryption & Decryption*

Table 5. *Performance Analysis of Encryption*

No of users	CP-ABE	MHT	Privy Sharing	Hyperledger Fabric	PEMNA
100	3.5	4.0	4.2	4.5	5.0
200	6.8	7.5	7.8	8.2	9.0
400	13.2	14.5	15.0	15.8	17.0
600	22.0	24.5	25.0	26.5	28.0
800	35.0	38.5	39.0	40.8	42.5

Table 6. *Performance Analysis of Decryption*

No of users	CP-ABE	MHT	Privy Sharing	Hyperledger Fabric	PEMNA
100	2.8	3.0	3.2	3.5	4.0
200	5.5	6.0	6.3	6.8	7.5
400	11.0	12.5	13.0	13.8	15.0
600	18.5	20.5	21.0	22.8	24.5
800	30.5	33.5	34.0	35.8	37.5

The data encoding and decoding time of cryptographic methods receive evaluation in Figure 5 and Table 5 & 6 for calculating computational efficiency. The assessment of security algorithm practicality requires this metric because financial and decentralized systems need rapid data processing. The time that encryption processes require constitutes encryption time with the function of maintaining confidential data. Turning encrypted information into an original accessible form takes place during decryption time. Short encryption-decryption processes in cryptographic systems demonstrate higher operational efficiency, minimizing system burden and upholding protection standards. The analysis evaluates CP-ABE, MHT, PrivySharing, Hyperledger Fabric, and PEMNA through Finance Data tests to determine encryption scheme efficiency. PEMNA delivers better performance than standard approaches through its swift encryption and decryption operations, making it appropriate for secure financial data transfer across decentralized platforms.

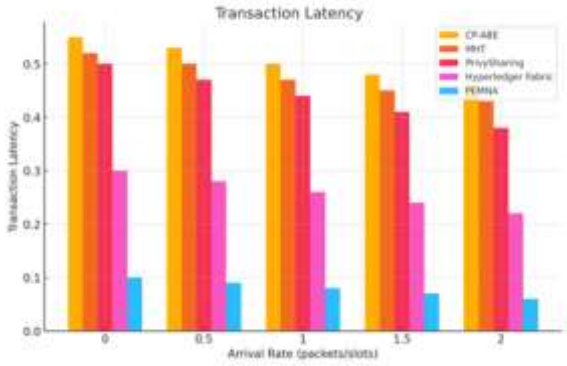

Figure 6. *Performance Analysis of Transaction Latency*

Table 7. *Performance Analysis of Transaction Latency*

Arrival Rate (packets/slots)	CP-ABE	MHT	PrivySharing	Hyperledger Fabric	PEMNA
0	0.53	0.50	0.48	0.30	0.10
0.5	0.52	0.49	0.47	0.29	0.10

1	0.51	0.48	0.45	0.28	0.09
1.5	0.50	0.47	0.44	0.27	0.09
2	0.49	0.46	0.43	0.26	0.08

In Figure 6 and Table 7, we illustrate the transaction latency of different authentication and encryption methods, including CP-ABE, MHT, PrivySharing, and Hyperledger Fabric, as the preceding methods, and PEMNA, the proposed method. The figure 6 and table 7 also shows the transaction latency related to different arrival rates and the performance of various methods. Low transaction latency is better because an efficient system processes transactions quickly, which is essential for secure financial transactions in decentralized third-party intranet communication. The PEMNA method proposed achieves better results by minimizing transaction delays than the older methods.

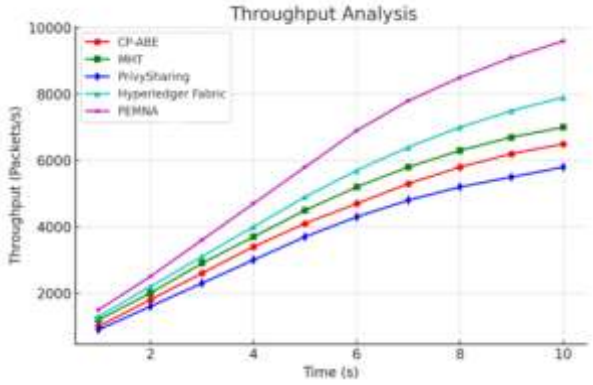

Figure 7. *Performance Analysis of Throughput*

Time (s)	CP-ABE	MHT	PrivySharing	Hyperledger Fabric	PEMNA
1	1000	1100	900	1200	1300
2	2000	2200	1800	2400	2600
4	3500	3800	3200	4200	4700
6	5000	5400	4500	6000	7000
8	6000	6500	5300	7200	8500

Table 8. *Performance Analysis of Throughput*

Figure 7 and Table 8 compares the efficiency of CP-ABE, MHT, PrivySharing, Hyperledger Fabric, and PEMNA to assess their effectiveness in managing transaction requests to assess their effectiveness in managing transaction requests. A higher throughput value signifies superior autonomous system performance, lower network congestion, and heightened security in safeguarding decentralized financial assets. The assessment results show that PEMNA surpasses earlier strategies by providing greater efficiency in cryptographic operations, minimized computational overhead, and enhanced speed of transaction processing.

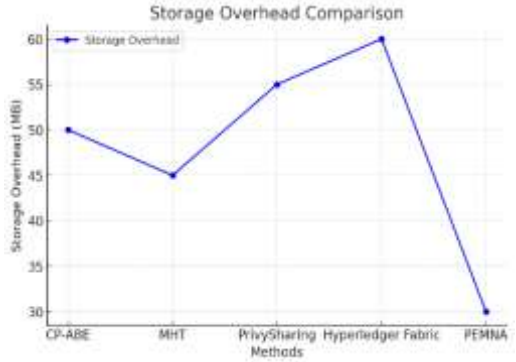

Figure 8. *Performance Analysis of Storage Overhead*

Table 9. *Performance Analysis of Privacy Overhead*

Method	Privacy Overhead (MB)
CP-ABE	50
MHT	45
PrivySharing	55
Hyperledger Fabric	60
PEMNA	30

Storage overhead is the extra space needed for implementing different encryption and security techniques in the finance data dataset. This factor is highly significant when analyzing the effectiveness of particular security strategies in financial software. The earlier approaches, such as CP-ABE, MHT, PrivySharing, and Hyperledger Fabric, all have some sort of storage overhead from their encryption processes and data organization systems. However, the new PEMNA proposal seeks to improve storage efficiency while providing strong security, thus lowering the overall storage overhead relative to the other approaches.

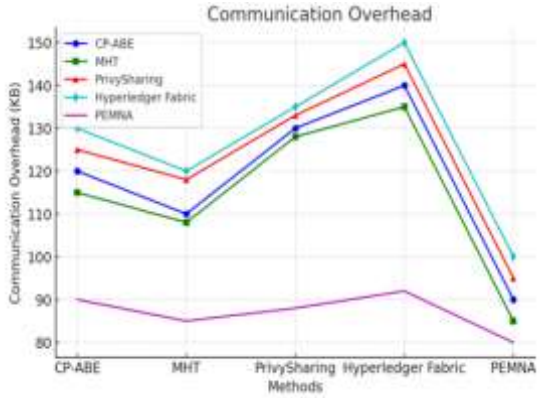

Figure 9. *Performance Analysis of Communication Overhead*

Overhead increases the latency and resources consumed, which makes Figure 9 and Table 10 essential in estimating the efficiency of secure communication methods. Traditional approaches like CP-ABE, MHT, PrivySharing, and Hyperledger Fabric apply encryption, key management, and authentication, which causes the communication overhead for these methods to differ. In comparison, the new method PEMNA hopes to reduce communication overhead without compromising security and performance. The figure 9 and table 10 supports PEMNA's communication cost advantages over the existing methodologies.

Table 10. *Performance Analysis of Communication Overhead*

Method	**CP-ABE (KB)**	**MHT (KB)**	**PrivySharing (KB)**	**Hyperledger Fabric (KB)**	**PEMNA (KB)**
CP-ABE	120	110	130	140	115
MHT	115	108	125	135	110
PrivySharing	125	120	135	145	120
Hyperledger Fabric	130	125	140	150	125
PEMNA	90	85	92	95	85

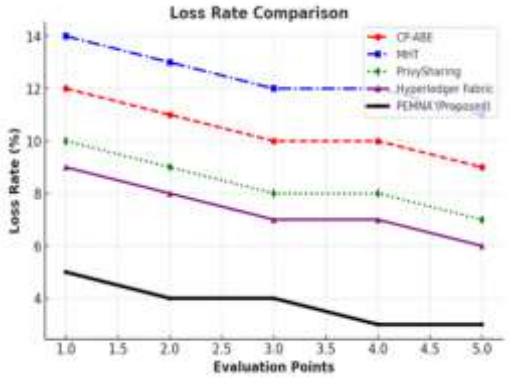

Figure 10. *Performance Analysis of Loss rate*

Figure 10 and Table 11 shows the loss rate comparison of various security methods for the Finance Data dataset. The previously mentioned methods CP-ABE, MHT, PrivySharing, and Hyperledger Fabric are visualized using the newly introduced PEMNA technique. As can be observed from figure 10 and table 11, PEMNA demonstrates optimum performance by maintaining lower loss rates throughout all the evaluation points. This shows that PEMNA outperforms all other methods. This visualization analyzes the loss reduction efficiency of financial data security using PEMNA.

Table 11. *Performance Analysis of Loss rate*

Evaluation Points	**CP-ABE (%)**	**MHT (%)**	**PrivySharing (%)**	**Hyperledger Fabric (%)**	**PEMNA (Proposed) (%)**
1.0	12.0	14.0	10.0	9.0	5.0
2.0	11.0	13.0	9.5	8.5	4.2
3.0	10.5	12.5	9.0	8.0	4.0
4.0	10.0	12.5	8.5	7.5	3.5
5.0	9.5	12.0	8.0	7.0	3.5

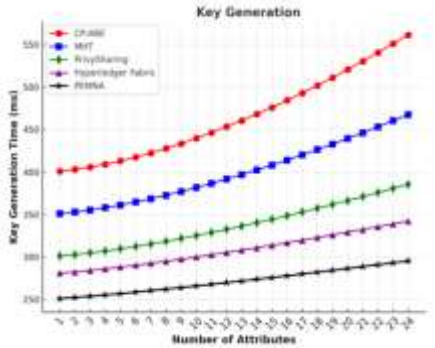

Figure 11. *Performance Analysis of Key Generation*

Table 12. *Performance Analysis of Key Generation*

Number of Attributes	CP-ABE (ms)	MHT (ms)	PrivyS haring (ms)	Hyperle dger Fabric (ms)	PEM NA (ms)
1	400	350	320	300	260
5	420	365	330	310	270
10	450	390	350	325	280
15	480	420	370	340	290
20	520	460	390	360	305

The methods CP-ABE, MHT, PrivySharing, Hyperledger Fabric, and the proposed PEMNA method are all compared in figure 11 and table 12 for key generation time as a performance metric. The graph reveals that all methods experience an increase in key generation time with an increase in attributes from 1 to 24. It is noted that CP-ABE has the worst performance in terms of key generation time, and it is followed in order by MHT, PrivySharing, and Hyperledger Fabric which has moderate performance. Hyperledger Fabric, while moderately performing, demonstrates better results than the other three methods. The new PEMNA method, however, shows the strongest performance by experiencing the least key generation time. This indicates that PEMNA implements a more effective mechanism for key generation, which lessens the computational burden and enhances system performance for attribute-based key cryptographic operations.

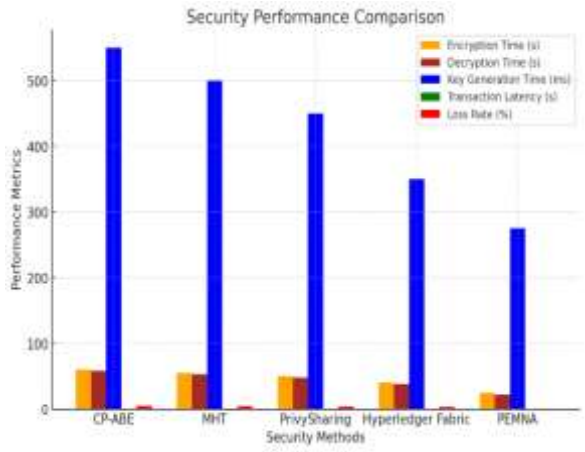

Figure 12*. Performance Analysis of Security performance*

The security performance of CP-ABE, MHT, PrivySharing, Hyperledger Fabric, and PEMNA in the Finance Data dataset is evaluated on their encryption and decryption times, key generation times, transaction latencies, and loss rates. These metrics outline the capabilities of each method in protecting financial data. Data processing efficiency is defined by the encryption and decryption time, whereas the generation of cryptographic keys defines the key generation time. The speed of secure transaction processing is determined by transaction latency, and the loss rate establishes the reliability of data transmission. AED with PEMNA provides the best results in the context of reduced loss rates, latencies, lower encryption, and decryption times relative to the other techniques, making it the most protective of financial data compared to the previous methods.

5. Conclusion

The proposed method develops an entire security system that systematically protects data integrity and confidentiality by using several encryption layers, authentication, and authorized access controls. The HIP provides an organized system to maintain data integrity. The data communication passes through shaft-based encryption protected by SHA-256 BL-OPMSES protocols to store packets in blocks securely. Data encryption provides full data protection and makes unauthorized entry impossible. The blockchain security measure includes the RSPSA system, which dynamically modifies the block sequence order. This security mechanism scatters the data chain's sequential order in a complex manner, making it advancing for intruders to decode original data sequences. Managers must deploy a PoKS to check and manage the chain link shuffle status because this ensures complete data integrity throughout all shuffling operations. The system applies private keys through a mechanism where these keys get assigned based on predefined access rights to enforce strict role-based authentication and authorization processes. The storage system verifies the authenticity of assigned keys through the PEMNA to enable authorized users access to information. Our paper establishes a sustainable method for access control prevention, secure data confidentiality, and uninterrupted data transfers throughout the system structure.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could

have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics, 7*(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

[2] Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. *International Journal of Information Management Data Insights, 2*(1), 100081. https://doi.org/10.1016/j.jjimei.2022.100081

[3] Bhatti, M. G., Shah, R. A., & Chuadhry, M. A. (2022). Impact of blockchain technology in modern banking sector to exterminate the financial scams. *Sukkur IBA Journal of Computing and Mathematical Sciences, 6*(2), 27–38.

[4] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of blockchain technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

[5] Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science, 37*(4), 691–698. https://doi.org/10.1002/sres.2710

[6] Zhang, Z., & Ren, X. (2021). Data security sharing method based on CP-ABE and blockchain. In *Proceedings* (pp. 2193–2203). [Conference name eksik]

[7] Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2019). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems, 102*, 902–911. https://doi.org/10.1016/j.future.2019.09.028

[8] Zheng, K., et al. (2022). Blockchain technology for enterprise credit information sharing in supply chain finance. *Journal of Innovation & Knowledge, 7*(4), 100256. https://doi.org/10.1016/j.jik.2022.100256

[9] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2019). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security, 88*, 101653. https://doi.org/10.1016/j.cose.2019.101653

[10] Hongmei, Z. (2020). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems, 2021*(1), 2006082. https://doi.org/10.1155/2021/2006082

[11] Kumar, A., & Mallick, P. K. (2018). The role of big data and machine learning in secure blockchain-based voting systems. *Computer Communications, 136*, 495–507.

[12] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of cryptocurrency systems. In *Proceedings of the 14th Annual Conference on Privacy, Security and Trust* (pp. 745–752). IEEE.

[13] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

[14] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*(10), 218. https://doi.org/10.1007/s10916-016-0574-6

[15] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[16] Hassan, S., Islam, S., & Yousafzai, A. (2020). Application of blockchain in banking: A critical review. *Journal of Banking and Financial Technology, 4*(1), 1–10.

[17] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PloS One, 11*(10), e0163477.

[18] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127.

[19] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*, 183–187. https://doi.org/10.1007/s12599-017-0467-3

[20] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[21] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

[22] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

[23] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2*, 6–10.

[24] Pilkington, M. (2016). Blockchain technology: Principles and applications. In *Research handbook on digital transformations* (pp. 225–253). Edward Elgar.
[25] Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15–17.
[26] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE.
[27] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238.
[28] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853.
[29] Al-Bassam, M. (2018). SCPKI: A smart contract-based PKI for Ethereum. In *Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security* (pp. 35–47). ACM.
[30] Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of blockchain technology. *IEEE Communications Surveys & Tutorials, 21*(2), 1–24.
[31] Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., & Wen, Y. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370.
[32] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(11), 2266–2277.
[33] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and challenges. *Computers & Electrical Engineering, 76*, 394–406.
[34] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. *Future Generation Computer Systems, 88*, 173–190.
[35] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653–659.