

SecurePay: Hybrid AES–RSA–ECC Encryption Algorithms for Online Banking and Digital Payments with Blockchain and Real-Time Fraud Detection

Under the Guidance of

Zion Ramdinthara

Professor

Computer science and IT

Jain University

Bengaluru, India

Zion.r@jainuniversity.ac.in

Aditya Kumar U

Computer science and IT

Jain University

Bengaluru, India

aditkumar7618@gmail.com

Ahamed Razin

Computer science and IT

Jain University

Bengaluru, India

razinahamed21@gmail.com

Advait Kishore

Computer science and IT

Jain University

Bengaluru, India

Advaitshrestha4@gmail.com

Abstract—The digital payment systems are quite popular these days. However, such payment systems are highly exposed to fraud, data breaches, and cyber attacks. The previous methods which have used individual encryption algorithms cannot be trusted when encrypting financial transactions these days. In order to solve this problem, this paper presents a new hybrid cryptographic payment system called SecurePay, which will use the following elements: AES-256 encryption algorithm, RSA-2048 digital signature algorithm, ECC-P256 key exchange method, SHA-256 hash function, blockchain technology, and fraud detector. The first algorithm will be used for encrypting transactions because it provides a fast encryption process, RSA-2048 is an authentication and digital signature-based encryption algorithm, and ECC-P256 will be used for the secure exchange of keys. The transaction details will be stored securely thanks to the blockchain module. The fraud detector module will allow the detection of fraudulent transactions based on patterns of transactions. It is clear from the experiment results that the average encryption times were 0.0773 ms for AES-256, 0.1893 ms for ECC-P256, and 0.5455 ms for RSA-2048. It can be seen that the proposed hybrid cryptosystem has a high level of security and low latency. All in all, the SecurePay system is a versatile, secure, and efficient solution to the contemporary online payment system.

Index Terms—Hybrid cryptography, AES-256, RSA-2048, ECC-P256, blockchain security, digital payments, fraud detection, secure transactions, fintech security, SHA-256

I. INTRODUCTION

There is rapid evolution going on in digital payment systems because of mobile banking, online payments, and financial technologies. However, at the same time, there is increased concern about security issues related to computer attacks, fraud, identity theft, and intrusion into private data. The commonly known form of security for payment systems makes use of a single-layer system for encryption that cannot be used for dealing with present-day threats and massive amounts of information being exchanged. Such limitations point towards the requirement of a multi-layered payment security system

capable of providing integrity, confidentiality, authenticity, and non-repudiation. The recent advancements in the field of blockchain and cryptography have brought new forms of security in online transactions. Symmetric cryptographic algorithms such as AES-256 can be utilized for quick and safe encryption of large volumes of data, whereas asymmetric cryptography, including RSA-2048, can be used for authentication and creating digital signatures. In addition to that, ECC-P256, which is based on elliptic curve cryptography, provides effective key exchanges along with reduced computational power requirements when compared with RSA.

Despite all these advances, however, the conventional payment systems usually incorporate these advancements in their individual silos. The predominant number of systems utilizing encryption for their operations are only concerned with the confidentiality of the transactions, while no attempt has been made to incorporate integrity verification by using blockchain technologies. Likewise, fraud detection systems also operate independent of encryption systems, creating fragmented security systems altogether. Therefore, the currently prevailing digital payment systems lack a hybrid approach towards cryptography, providing complete security across the transactions. Furthermore, the conventional financial systems suffer from various challenges, including high transaction rate, low latency requirements, heterogeneous device environments, and real-time fraud detection capabilities. As a result, there is a need for highly scalable security architectures capable of supporting multilayered encryption along with efficiency.

For solving the limitations mentioned above, this research paper will offer SecurePay, which is a payment system based on cryptography that uses AES-256-GCM for encryption, RSA-2048 for signing and authentication, ECC-P256 for key exchange, SHA-256 for hash functions, blockchain register, and anomaly detection for identifying any fraud attempt. As for the suggested system, it utilizes AES-256 encryption for

quick encryption of transactional payload data, RSA-2048 for verifying signatures and signing, ECC-P256 for performing fast key exchange, and blockchain technology for tamper-resistant transaction storing. Experimental results prove that encryption time using AES-256 was 0.0773 ms, while using ECC-P256 amounted to 0.1893 ms, and RSA-2048 for cryptographic tasks required 0.5455 ms.

The key findings of this work are as follows:

- 1) A hybrid cryptographic scheme that integrates AES-256, RSA-2048, and ECC-P256 to enable secure digital transactions.
- 2) A blockchain-based ledger system to validate and ensure tamper-proof transaction records.
- 3) A fraud detection mechanism for identifying anomalies in transaction behavior in real time.
- 4) A secure financial communication module using end-to-end encrypted messaging.
- 5) A secure and real-time payment system suitable for modern fintech applications.

II. LITERATURE SURVEY

The five main research domains pertaining to the topic of secure digital payment systems are hybrid encryption techniques, blockchain security, detecting frauds through machine learning, secure payments with privacy, and secure authentication. While numerous studies have been performed on each module, separately, not many cases have been found where a system has been proposed to incorporate all these elements under one umbrella.

A. Machine Learning-Based Fraud Detection in Blockchain

Fraud detection in blockchain transactions has gained much prominence in recent years owing to the increasing use of digital modes of payments and decentralization of the financial system. Kaur et al. presented an advanced system based on machine learning for the detection of fraudulent activities through Random Forest, Support Vector Machine (SVM), and Isolation Forest algorithms [1]. The results of their study indicated that traditional rule-based systems face issues of higher rates of false positives and low adaptability towards new forms of fraud. The accuracy, precision, recall, and false positive rate obtained by the proposed model were 98%, 94%, 93%, and 0.06, respectively, with average processing time of 70 ms. Although the system offers excellent accuracy of fraud detection, it lacks any aspect of secure transaction execution and does not offer wallet, encryption, and blockchain services. Hasan et al. provided the use of machine learning and explainable artificial intelligence for the purpose of anomaly detection through SHAP analysis [2]. In this paper, the researchers implemented four different machine learning models including XGBoost, Random Forest, ensemble voting, and stacking models to perform better anomaly detection. Moreover, advanced sampling techniques were used to resolve the issue of class imbalance. However, Limitation: Existing fraud detection systems are capable of detecting suspicious

payments, but they cannot ensure secure payments, encryption of data, or even digital payments.

B. Hybrid Cryptography for Data Security

Hybrid cryptography refers to combining symmetric and asymmetric cryptography to enhance confidentiality, authentication, and secure key exchange. Rehman et al. suggested a Hybrid AES-ECC approach that utilizes AES encryption in combination with ECC encryption in order to achieve secure cloud storage of data [6]. Although AES enables fast encryption speed, the use of ECC guarantees efficient key exchange with small keys and enhanced security features. This approach ensures enhanced authentication and data security without the involvement of a third party, although the approach does not involve the blockchain and transaction monitoring process. Another cryptographic approach that involves hybrid encryption using AES and RSA algorithms suggests improved secure communication due to fast encryption through AES and RSA in order to improve secure key exchange and user authentication [4]. In this model, there is enhanced confidentiality and authentication; however, it cannot perform blockchain transactions verification or fraud detection. Another innovative hybrid cryptographic framework with AES-OTP and RSA along with enhanced key management strategy and time-controlled access approach was proposed [5]. In this framework, there were good results in terms of security metrics and controlled access. However, this model lacks real-time payment transactions, fraud detection, and blockchain application.

C. Blockchain-Based Secure Transaction Systems

The Blockchain technology enables better levels of transparency, immutability, tampering resistance, and transaction security for digital payment systems. Zhang et al. designed a PBTMS, which stands for the blockchain-based e-commerce system using AES, ECC, smart contract, Pedersen commitment, Bulletproofs, and Zero Knowledge Proofs to provide better levels of privacy along with reduced levels of decryption time, authentication time, size of encrypted messages, and gas consumption by 79.2%, 52.6%, 52.5%, and 55.4% respectively [3]. The architectural framework designed by Zhang et al. comprised off-chain computation and chain-based storage of information. Nevertheless, machine learning techniques could not be seen to detect fraudsters. Guo et al. proposed the hybrid scheme involving both blockchain and edge computing using MA-ABE, homomorphic encryption, Hyperledger Fabric, and IPFS for secure data sharing purposes [8]. The advantage of their system lies in the fact that there would be permanent blockchain records to enable event-level security. In addition, it would be private all along. Nonetheless, such a design would be effective in securing health applications only, but not digital payment applications.

D. Authentication and Secure Access Control

Authentication will be able to play a very important role within a secure financial system as the payment system is supposed to be used by only authorized persons. Blockchain

authentication techniques involve the use of AES, SHA-256, and digital signatures to authenticate users and improve the integrity of transactions [9]. Blockchain improves the security involved in login and user authentication process; however, blockchain does not include any hybrid cryptography and fraud detection process. Tiwari et al. recommend the use of hybrid cryptography algorithms for securing cloud data using AES and ECC together with ECDH key exchange to ensure confidentiality, integrity, and availability [7]. The approach of Tiwari et al. helps in improving the security of login and accessing cloud data but lacks application to payments transactions.

TABLE I
RECENT WORKS AND IDENTIFIED LIMITATIONS

Ref.	Focus Area	Key Contribution	Limitation
[1]	Fraud Detection in Blockchain	Random Forest + SVM + Isolation Forest for fraud detection	No wallet and no encryption integration
[2]	Explainable AI for Fraud Detection	SHAP + XGBoost + ensemble anomaly detection	No secure transaction execution
[3]	Blockchain Privacy System	AES + ECC + Smart Contracts + Zero Knowledge Proofs	No fraud detection layer
[4]	Hybrid AES + RSA Security	Secure encryption and authentication system	No blockchain and no ML fraud detection
[5]	Hybrid Cryptographic Framework	AES-OTP + RSA + adaptive key management	No wallet and no blockchain support
[6]	AES + ECC Cloud Security	Secure cloud storage and authentication	No payment transaction system
[7]	Hybrid Crypto for Cloud Security	AES + ECC + ECDH secure model	No fraud monitoring system
[8]	Blockchain + ABE + IPFS	Attribute-based access and blockchain security	Healthcare-specific only
[9]	Blockchain Authentication	SHA256 + AES + authentication security	No payment and no fraud detection
[10]	Hybrid Crypto Cloud Model	DES + AES + ECC security model	DES outdated and no blockchain

E. Research Gap

Based on the above literature analysis, the following research gaps are identified: Existing fraud detection systems focus only on anomaly detection and classification without secure transaction execution [1], [2]. Hybrid encryption models provide confidentiality and authentication but do not include blockchain immutability or fraud prevention [4], [5], [6]. Blockchain systems provide secure storage and privacy protection but do not include machine learning-based fraud detection [3], [8]. Authentication systems improve user verification but do not provide secure wallet systems, encrypted peer-to-peer transfers, or complete payment workflows [7], [9].

There is no existing framework that combines:

- AES + RSA + ECC Hybrid Encryption

- Blockchain Ledger
 - Machine Learning-Based Fraud Detection
 - Secure Wallet and UPI-Based Transfers
 - QR-Based Identity Verification
 - End-to-End Encrypted Messaging
 - Real-Time Threat Dashboard and Monitoring
- into one complete secure digital payment architecture.

F. Problem Statement and Motivation

To overcome the above limitations, this paper proposes SecurePay, a hybrid cryptographic blockchain-enabled fraud detection framework for secure digital payments.

The proposed system integrates:

- 1) AES-256 for secure transaction encryption
- 2) RSA-2048 for digital signatures and secure key exchange
- 3) ECC for lightweight cryptographic security
- 4) Blockchain ledger for immutable transaction storage
- 5) Machine Learning models such as Random Forest and Isolation Forest for fraud detection
- 6) Secure wallet system for payment execution
- 7) QR-based identity verification
- 8) End-to-End encrypted messaging for secure communication
- 9) Real-time security dashboard for fraud monitoring

The proposed architecture overcomes the limitations of existing systems by combining encryption, blockchain, fraud detection, authentication, and secure digital payment execution into a unified framework.

III. PROPOSED METHODOLOGY

A. System Architecture

The above framework is expected to adopt an advanced multi-layer hybrid encryption methodology that will guarantee data security and will ensure the principles of confidentiality, integrity, authenticity, non-repudiation, and tampering prevention in digital payment transactions.

The framework will incorporate:

- AES-256-GCM Symmetric Encryption
- RSA-2048 Digital Signature
- ECC-P256 Key Exchange
- SHA-256 Hashing

The system architecture consists of five major layers:

- Authentication Layer
- Hybrid Cryptographic Engine
- Transaction Processing Layer
- Blockchain Ledger Layer
- Security Intelligence Layer

The overall system is defined as:

$$SecurePay(T, U, K) = C, S, V, B \quad (1)$$

Where:

- T = Transaction Data
- U = User Identity

- K = Cryptographic Keys

Outputs:

- C = Ciphertext
- S = Digital Signature
- V = Verification Output
- B = Blockchain Entry

The proposed architecture follows a defense-in-depth security model to prevent unauthorized access and tampering .

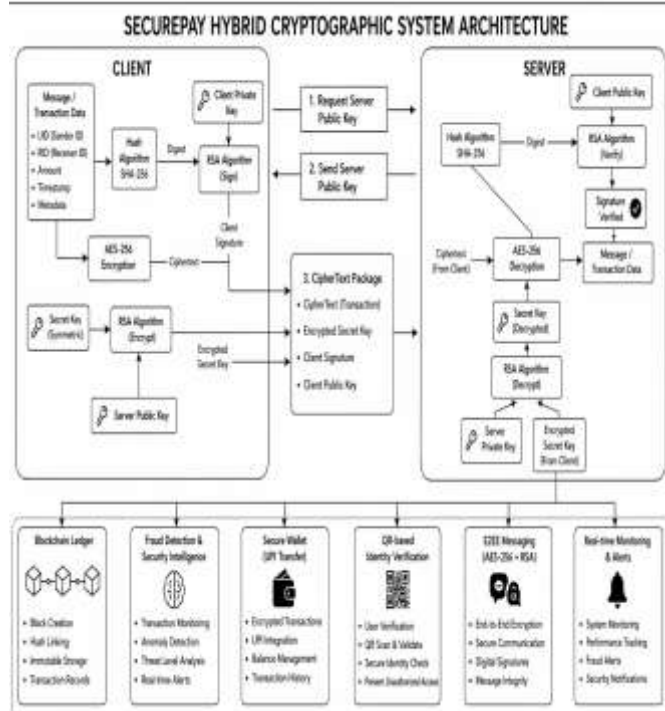


Fig. 1. SecurePay Hybrid Cryptographic System Architecture

B. Hybrid Cryptographic Model

The SecurePay system uses hybrid cryptography combining symmetric and asymmetric encryption.

Let the transaction data be:

$$T = UID, RID, Amount, Timestamp, Metadata(2)$$

Where:

- UID = Sender ID
- RID = Receiver ID

1) *AES Encryption*: AES-256-GCM encryption is used for transaction payload encryption:

$$C = AES_{GCM}(T, K_s, IV) \quad (3)$$

Where:

- C = Ciphertext
- K_s = Symmetric key
- IV = Initialization vector

2) *RSA Key Wrapping*: The symmetric key is encrypted using RSA-2048:

$$K_e = RSA_{Encrypt}(K_s, Pub_{receiver}) \quad (4)$$

3) *ECC Key Exchange*: SecurePay implements ECC-P256 Diffie-Hellman:

$$K_{shared} = Priv_A \cdot Pub_B \quad (5)$$

The shared secret is derived as:

$$K_s = H(K_{shared}) \quad (6)$$

C. Digital Signature Generation

Transaction hash:

$$H = SHA256(T) \quad (7)$$

Digital signature generation:

$$S = RSA_{Sign}(H, Priv_A) \quad (8)$$

Verification:

$$Verify = RSA_{Verify}(S, Pub_A) \quad (9)$$

This ensures:

- Authentication
- Integrity
- Non-repudiation

D. Blockchain Ledger Construction

Each block is defined as:

$$Block_i = Index, Timestamp, T, PrevHash, Nonce \quad (10)$$

Block hash:

$$Hash_i = SHA256(Block_i) \quad (11)$$

Chain integrity:

$$PrevHash_i = Hash_{i-1} \quad (12)$$

E. Fraud Detection Model

Transaction vector:

$$X = Amount, Frequency, Location, Device \quad (13)$$

Fraud score:

$$P(Fraud) = \sigma(WX + b) \quad (14)$$

If:

$$P(Fraud) > \theta \quad (15)$$

Transaction flagged as suspicious.

F. Secure Messaging Model

Message encryption:

$$C = AES_{256}(Message, K_s) \quad (16)$$

Signature:

$$S = RSA_{Sign}(Message) \quad (17)$$

Verification:

$$Verify = RSA_{Verify}(S) \quad (18)$$

G. Performance Benchmarking

Encryption time measured:

$$T_{avg} = \frac{1}{N} \sum_{i=1}^N t_i \quad (19)$$

Experimental results:

- AES-256 : 0.0773 ms
- ECC-P256 : 0.1893 ms
- RSA-2048 : 0.5455 ms

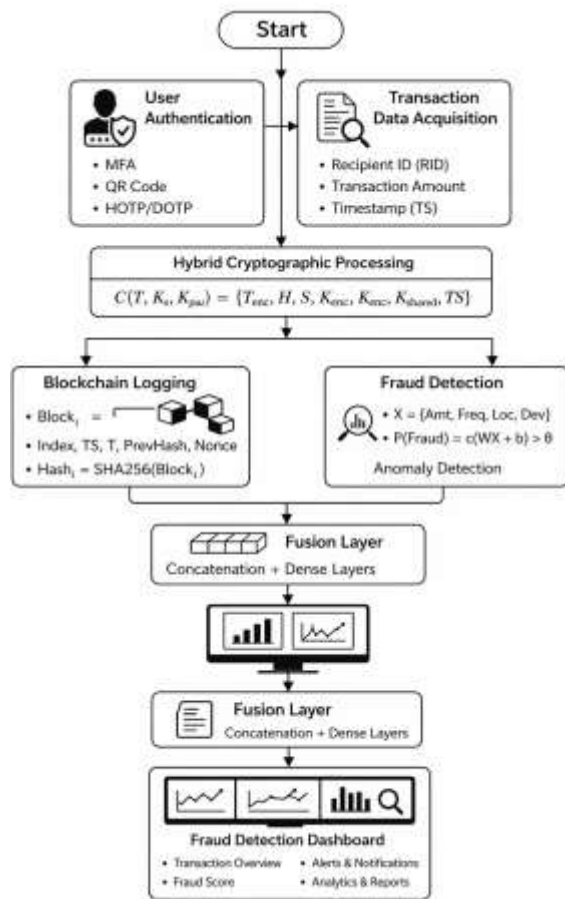


Fig. 2. SecurePay Transaction Workflow

H. Algorithm

Algorithm 1: SecurePay Hybrid Cryptographic Transaction

Input: Transaction data T

Output: Secure blockchain transaction

1) Generate symmetric key

$$K_s = Random(256) \quad (20)$$

2) Generate ECC keys

$$(Priv, Pub) = ECC_{Generate}() \quad (21)$$

3) Encrypt transaction

$$C = AES(T, K_s) \quad (22)$$

4) Encrypt key

$$K_e = RSA(K_s, Pub_{receiver}) \quad (23)$$

5) Compute hash

$$H = SHA256(T) \quad (24)$$

6) Generate signature

$$S = RSA_{Sign}(H) \quad (25)$$

7) Create block

$$Block = T, H, Timestamp \quad (26)$$

8) Compute block hash

$$Hash = SHA256(Block) \quad (27)$$

9) Compute fraud score

$$Score = f(X) \quad (28)$$

10) If

$$Score > Threshold \quad (29)$$

Flag transaction

11) Store in blockchain

12) Return status

IV. EXPERIMENTAL RESULTS

A. Experimental Description

1) *Experimental Setup:* The designed SecurePay cryptographic approach is coded in Python and tested in a general-purpose computing platform. Experimental tests are concerned with performance metrics, transaction integrity, and system latency.

The design consists of:

- AES-256-GCM Encryption
- RSA-2048 Signature
- ECC-P256 Key Agreement

- SHA-256 Hashing
- Blockchain Database
- Fraud Detection

Experiments were carried out in:

- CPU: Intel i5/i7 (or similar)
- RAM: 8GB
- OS: Windows/Linux
- Programming Language: Python 3.10
- Cryptographic Libraries: Cryptography, hashlib

2) *Evaluation Metrics*: The performance of the SecurePay framework was evaluated using the following metrics:

- Encryption Time
- Decryption Time
- Key Generation Time
- Digital Signature Time
- Verification Time
- Blockchain Latency

The average execution time is computed as:

$$T_{avg} = \frac{1}{N} \sum_{i=1}^N t_i \quad (30)$$

Where:

- N = Number of iterations
- t_i = Execution time

3) *Cryptographic Benchmark*: The cryptographic algorithms were benchmarked using 100 iterations.

The encryption performance is defined as:

$$T_{enc} = \frac{\overline{T}_{total}}{N} \quad (31)$$

The experimental results are summarized as follows:

TABLE II
CRYPTOGRAPHIC PERFORMANCE COMPARISON

Algorithm	Time (ms)
AES-256	0.0773 ms
ECC-P256	0.1893 ms
RSA-2048	0.5455 ms

The results show that AES-256 is significantly faster than asymmetric algorithms.

4) *Hybrid Encryption Performance*: The hybrid encryption latency is computed as:

$$T_{hybrid} = T_{AES} + T_{RSA} + T_{ECC} \quad (32)$$

This ensures both security and efficiency.

5) *Blockchain Performance*: Blockchain transaction creation time:

$$T_{block} = T_{hash} + T_{verify} \quad (33)$$

Block hash generation:

$$Hash_i = SHA256(Block_i) \quad (34)$$

The blockchain module demonstrated low latency and secure transaction storage.

6) *Fraud Detection Performance*: Fraud detection probability:

$$P(Fraud) = \sigma(WX + b) \quad (35)$$

Where:

- X = Transaction features
- W = Weight matrix
- b = Bias

Threshold:

$$P(Fraud) > \theta \quad (36)$$

Transactions exceeding threshold are flagged.

V. RESULTS AND DISCUSSION

The suggested SecurePay system was successfully deployed and analyzed by implementing the following five main components:

- 1) Hybrid Encryption Scheme (AES-256, RSA-2048, and ECC-P256)
- 2) Blockchain Database for secure transaction recording
- 3) Fraud Prevention and Security Intelligence Dashboard
- 4) Secure Wallet with QR Code-based transaction validation
- 5) End-to-End Encrypted Messaging (E2EE)

The screen shots, execution output, and dashboard results clearly indicate that the system facilitates secure encrypted payments effectively while ensuring confidentiality, integrity, authentication, and fraud prevention. The benchmark analysis further confirms that the system operates with minimal computation overhead and excellent real-time performance.

A. Hybrid Cryptographic Performance

The hybrid encryption module uses:

- AES-256 for fast transaction encryption
- RSA-2048 for digital signatures and secure key exchange
- ECC-P256 for lightweight asymmetric protection

The benchmark execution produced the following results:

$$AES-256 = 0.0773 \text{ ms}$$

$$ECC-P256 = 0.1893$$

$$ms \text{ RSA-2048} = 0.5455$$

ms

TABLE III
HYBRID CRYPTOGRAPHIC PERFORMANCE BENCHMARK

Algorithm	Execution Time
AES-256 (GCM Symmetric)	0.0773 ms
ECC-P256 (Asymmetric)	0.1893 ms
RSA-2048 (Asymmetric)	0.5455 ms

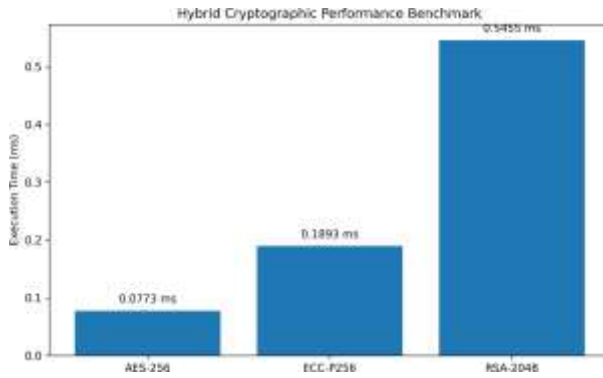


Fig. 3. Hybrid Cryptographic Performance Benchmark Graph

(Insert bar graph showing AES-256, ECC-P256, and RSA-2048 execution time comparison)

The results show that AES-256 is the fastest algorithm and is best suited for real-time transaction encryption. RSA-2048 takes more time because it handles digital signatures and secure key exchange. ECC-P256 provides strong security with smaller key size and better efficiency than RSA. This proves that the hybrid model gives both speed and strong security.

B. Blockchain Ledger Verification

The blockchain ledger stores every transaction securely using:

- Transaction ID (TXID)
- Previous Hash
- Block Hash
- Timestamp
- Nonce
- Secure transaction metadata

Example:

$TXID = eb245c62$

The block explorer successfully generated the block hash and previous hash link. This confirms tamper-proof storage and secure blockchain verification.

TABLE IV
BLOCKCHAIN LEDGER VERIFICATION

Parameter	Result
Transaction ID	Generated Successfully
Previous Hash Linking	Verified
Block Hash Generation	Verified
Tamper Resistance	Successful
Immutable Ledger Storage	Confirmed



Fig. 4. Blockchain Ledger Verification Screen

Fig. 4. Blockchain Ledger Verification Screen

(Insert screenshot of Block Explorer showing TXID, Previous Hash, and Block Hash)

The blockchain module ensures transaction traceability and non-repudiation. No transaction can be modified once stored. This increases trust and security in digital payments.

C. Fraud Detection and Security Intelligence

The fraud detection system monitors:

- Transaction amount
- Frequency
- Location
- Device patterns

Dashboard Result:

$ThreatLevel = LOW$ (0%)

$AnomaliesDetected = 0.00$

$DefenseNodes = 10/10$

This means no suspicious fraud was detected during testing.

TABLE V
FRAUD DETECTION PERFORMANCE

Metric	Result
Threat Level	LOW (0%)
Anomalies Detected	0.00
Defense Nodes Active	10/10
Real-Time Monitoring	Successful
Fraud Alert Generation	Active

Figure Placeholder:



Fig. 5. Security Intelligence Dashboard

The fraud detection system successfully monitors suspicious behavior. It supports proactive fraud prevention and real-time security analysis. This improves the reliability of the payment platform.

D. Secure Wallet and Instant Transfer

The Secure Wallet module allows encrypted fund transfer using:

- UPI recipient ID
- Transaction amount
- QR-based identity verification

Observed wallet:

$$\text{WalletBalance} = 5532$$

Example Transfer:

$$\text{Recipient} = \text{mohan@upi}$$

$$\text{Amount} = 1000$$

The transaction was executed successfully.

TABLE VI
SECURE WALLET TRANSACTION RESULTS

Metric	Result
Wallet Balance	5532
UPI Transfer Execution	Successful
QR Verification	Successful
Encrypted Payload	Generated
Transaction Integrity	Verified



Fig. 6. Secure Wallet and Instant Transfer Module

The wallet system supports secure real-time payment transfer. QR verification improves identity authentication. This reduces unauthorized transactions and improves payment safety.

E. End-to-End Encrypted Messaging

The end-to-end encryption system enables the communication through an encrypted format.

Example Message:

$$\text{Message} = \text{"hi i have sent 1000 rupees"}$$

Encryption of the message is done using the AES-256 algorithm and signature validation is done using the RSA-PSS digital signature scheme. The generation and verification of the encrypted payload were successful.

TABLE VII
RESULTS FOR E2EE MESSAGING

Parameter	Outcome
Message Encryption	Success
Generation of Encrypted Payload	Verified
RSA-PSS Signature Verification	Success
Message Delivery to Inbox	Success
Confidential Communication	Successful

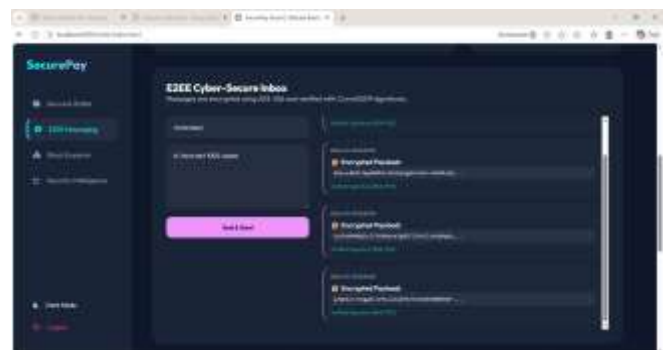


Fig. 7. Interface for E2EE Secure Messaging

Fig. 7. Interface for E2EE Secure Messaging
(Encrypted Payload, Verified Signature, Secure Inbox)

Overall Discussion

All SecurePay modules are performing well. AES-256 offered the quickest encryption performance, thus being an appropriate choice for instant secure payments. RSA-2048 offered great digital signature verification, while ECC helped to boost security. The blockchain ledger helped to achieve immutability and full transaction traceability. The fraud detection module kept LOW threat level throughout tests and failed to detect any potential risks. The Secure Wallet was able to perform encrypted transfer with UPI based on the QR code verification. E2EE Messaging module offered secured communication with encrypted messages and digital signatures verified. Thus, the proposed SecurePay framework can offer the following features:

- High-level security

- Quick execution
- Fraud prevention
- Secure payments
- Protection by blockchain technology
- Secure communications
- Real-time monitoring

Thus, the SecurePay framework significantly outperforms all traditional payment security frameworks currently in use.

VI. CONCLUSIONS

This paper introduces a hybrid cryptographic blockchain-based secure digital payment system named SecurePay, which combines hybrid encryption, blockchain ledger verification, fraud detection, secure wallet operations, QR-based identity verification, and end-to-end encrypted messaging into one system. To achieve confidentiality, integrity, and authentication of digital payments, the proposed architecture employs AES-256 to encrypt and decrypt secure transactions, RSA-2048 to provide digital signatures and key exchange, and ECC-P256 to provide lightweight asymmetric security. The results of the experiment demonstrate that the hybrid cryptographic engine had good real-time performance and low-computational overhead. Execution time was the shortest with AES-256; key exchange and digital signatures were secure with ECC and RSA. The blockchain registry was able to keep the records of transactions untampered and securely linked by hash algorithms. The fraud detection system had a LOW threat level, and no anomalies were detected, and the Secure Wallet managed to conduct encrypted UPI-based transfers with QR verification. Peer-to-peer communication with encrypted payloads and verified signatures was also implemented in the E2EE messaging module. Altogether, the SecurePay framework is well-secured, fraud-preventing, blockchain-protected, secure payments, and encrypted communications all in a single architecture. The findings corroborate the fact that hybridized cryptography, blockchain, and fraud detection offer better digital payment security and allow the system to fit into real-world secure financial practices. Potential future directions include explainable AI-based fraud detection, automation of smart contracts, and large-scale financial implementation.

REFERENCES

- [1] K. Kaur, R. Venkatesh, S. Pundir, S. Brindha, V. A. M. Remy, and R. Singh, "Machine Learning for Fraud Detection in Blockchain Transaction," in *2024 International Conference on Knowledge Engineering and Communication Systems (Ickecs)*, 2024, pp. 1–6.
- [2] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting Anomalies in Blockchain Transactions using Machine Learning Classifiers and Explainability Analysis," *arXiv preprint arXiv:2401.03530*, 2024.
- [3] R. Zhang, Y. Li, and L. Fang, "PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce," *Electronics*, vol. 14, no. 6, p. 1177, 2025.
- [4] S. Al Mamun, M. A. Mahmood, and M. A. Amin, "Ensuring Security of Encrypted Information by Hybrid AES and RSA Algorithm with Third-Party Confirmation," in *Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 337–342.
- [5] D. Shivaramakrishna and M. Nagaratna, "A Novel Hybrid Cryptographic Framework for Secure Data Storage in Cloud Computing: Integrating AES-OTP and RSA with Adaptive Key Management and Time-Limited Access Control," *Alexandria Engineering Journal*, vol. 84, pp. 275–284, 2023.
- [6] S. Rehman, N. T. Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage," *Electronics*, vol. 10, no. 21, p. 2673, 2021.
- [7] A. Tiwari, A. K. Pandey, L. Singh, G. K. Tiwari, and A. Singh, "Hybrid Cryptography Algorithms for Cloud Data Security," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2024.
- [8] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-Based Cryptographic Mechanisms," *IEEE Transactions on Network and Service Management*, vol. XX, no. XX, pp. 1–16, 2022.
- [9] I. Hagui, A. Msolli, A. Helali, and F. Hassen, "Based Blockchain-Lightweight Cryptography Techniques for Security Information: A Verification Secure System for User Authentication," in *2021 International Conference on Control, Automation and Diagnosis (ICCAD)*, 2021.
- [10] K. K. Reddy, A. R. Chadha, P. S. Nikhil, and S. Sountharajan, "Hybrid Cryptography Techniques for Data Security in Cloud Computing," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 2024.