International Journal of Engineering Research and Science & Technology

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

Research Paper

SECURE MULTI-SIGNATURE PROTOCOL TO COUNTER TRANSACTION MALLEABILITY IN DEFI

K. MAMATHA[1], SAMPATHI ARCHANA REDDY[2], KALLEM AKSHITHA[3], GOPU PAARTHIVA[4], ALLALA SADHVIN RAO[5]

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

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

ABSTRACT— In blockchain-based Decentralised Finance (DeFi) protocols, signatures play a vital role in ensuring the security and integrity of transactions and smart contracts. However, weaknesses in existing signature schemes make them vulnerable to malleability attacks (MA), where an attacker can alter the transaction ID (TxId) without changing the transaction's content or validity. To address this, we propose an advanced multi-signature scheme (MSS) that integrates unmalleable transaction implementations as a supplementary signature mechanism. In MSS, both owners and block producers collaboratively generate joint signatures, enhancing efficiency while ensuring stronger protection against malleability. Although the method is complex and time-intensive, it has been adapted to blockchain environments with additional optimisations, such as hash-based execution of intermediate transactions, to guarantee complete resistance to malleability attacks. Experimental results from testbed simulations highlight that MSS offers improved scalability and achieves a 15% higher resistance rate against attack success compared to baseline approaches.

Index Terms – Blockchain, decentralized finance (DeFi), multi-signature scheme (MSS), transaction malleability, malleability attacks, transaction security, smart contracts, blockchain security, cryptographic signatures, transaction integrity, hash-based verification, secure blockchain transactions.

I. INTRODUCTION

In recent years, Decentralised Finance (DeFi) has emerged as a transformative innovation in blockchain technology, enabling secure and transparent financial transactions without the need for centralized intermediaries such as banks or financial institutions. Blockchain-based financial systems rely heavily on digital signatures to authenticate transactions and verify asset ownership across distributed networks. However, existing cryptographic signature mechanisms used in many blockchain platforms are vulnerable to transaction malleability attacks, where an attacker can alter the transaction identifier (TxId) without modifying the actual transaction content. This creates significant security risks, including transaction duplication, smart contract exploitation, and disruption of transaction processing within DeFi environments.

To overcome these challenges, this project introduces a Secure Multi-Signature Protocol designed to protect blockchain transactions from malleability attacks by enhancing signature integrity and verification processes. The proposed system enables multiple participants, such as transaction owners and block validators, to collaboratively generate a unified digital signature that ensures authenticity and immutability of transactions. By incorporating advanced cryptographic techniques and hash-based execution mechanisms, the system strengthens resistance against signature manipulation and unauthorized transaction modifications.

II. RELATED WORK

A. Dynamic fine grained SLA management for 6G eMBB-plus slice using mDNN & smart contracts

The project titled Dynamic Fine-Grained SLA Management for 6G eMBB-Plus Slice using mDNN and Smart Contracts focuses on developing an intelligent and automated Service Level Agreement (SLA) management framework for next-generation 6G mobile networks. As 6G networks are expected to support enhanced Mobile Broadband Plus (eMBB-Plus) services such as ultra-high-definition streaming, virtual reality, and real-time communication, maintaining consistent Quality of Service (QoS) becomes a critical challenge. Traditional SLA management approaches are static in nature and lack the flexibility to adapt to dynamic network conditions such as fluctuating traffic loads, latency variations, and bandwidth requirements. This project aims to overcome these limitations by introducing a dynamic and fine-grained SLA monitoring and enforcement mechanism. The proposed system integrates a modified Deep

Neural Network (mDNN) model to predict network performance parameters and intelligently manage resource allocation for eMBB-Plus network slices. The mDNN continuously monitors key performance indicators such as latency, throughput, packet loss, and bandwidth usage to ensure SLA compliance in real time. Additionally, blockchain-based smart contracts are utilized to automate the enforcement of SLA policies between network service providers and users. These smart contracts enable transparent, tamper-proof, and decentralized agreement execution, ensuring that SLA terms are automatically validated and enforced without the need for manual intervention.

B. *SecureVision: Advanced cybersecurity deepfake detection with big data analytics*

SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics is a security-focused project that aims to detect and prevent the misuse of deepfake technology using advanced data analysis and machine learning techniques. With the rapid advancement of Artificial Intelligence, deepfake content such as manipulated videos, audio clips, and images has become increasingly sophisticated, posing serious threats to cybersecurity, digital identity, privacy, and public trust. These fabricated media files can be used for malicious purposes including identity theft, misinformation, financial fraud, and cyberattacks. Traditional detection methods often fail to identify such manipulated content due to the realistic nature of AI-generated media. This project introduces a robust deepfake detection framework that leverages big data analytics and deep learning algorithms to analyze large volumes of multimedia content in real time. The system extracts key visual and audio features such as facial expressions, lip synchronization patterns, pixel-level inconsistencies, and voice modulation anomalies to identify forged media. By processing massive datasets through distributed computing environments, the proposed solution enhances detection accuracy and improves the ability to identify subtle manipulations that are not visible to the human eye.

C. *Areliable zero-trust network for task offloading in vehicular systems using an asynchronous federated learning approach in 6G*

The project titled A Reliable Zero-Trust Network for Task Offloading in Vehicular Systems using an Asynchronous Federated Learning Approach in 6G aims to develop a secure and intelligent framework for

managing computational task offloading in next-generation vehicular networks. With the rapid growth of autonomous vehicles, smart transportation systems, and real-time vehicular applications, there is a growing demand for efficient processing of large volumes of data generated by vehicles. These applications often require high computational resources that cannot be handled solely by onboard vehicle systems. Task offloading to edge or cloud servers is therefore necessary; however, traditional network architectures are vulnerable to security threats such as unauthorized access, data breaches, and malicious nodes. To address these challenges, this project introduces a Zero-Trust Network (ZTN) model that ensures continuous authentication and strict access control for all entities involved in the vehicular communication environment. The system assumes that no device, user, or network component is inherently trustworthy, thereby enforcing security verification at every stage of communication and task execution. Additionally, the project incorporates an asynchronous federated learning approach that allows vehicles to collaboratively train machine learning models without sharing raw data, preserving privacy and reducing communication overhead. This decentralized learning mechanism enables efficient decision-making for task offloading based on network conditions, resource availability, and latency requirements.

D. Understanding failures in security proofs of multi-factor authentication for mobile devices

The project titled Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices focuses on analysing and identifying potential weaknesses in the design and implementation of multi-factor authentication (MFA) systems used in modern mobile environments. As mobile devices increasingly serve as primary platforms for accessing sensitive applications such as online banking, healthcare systems, cloud storage, and enterprise services, ensuring strong authentication mechanisms has become a critical requirement. MFA schemes typically combine multiple verification factors such as passwords, biometrics, one-time passwords (OTP), and device-based authentication to enhance user security. However, despite their widespread adoption, many MFA protocols still suffer from hidden vulnerabilities due to incorrect or incomplete security proofs. This project investigates how flaws in theoretical security assumptions, cryptographic implementations, and protocol

design can lead to authentication failures even when MFA appears robust in practice. In many cases, mobile-based authentication schemes rely on insecure communication channels, weak key management strategies, or improperly validated cryptographic operations, making them susceptible to attacks such as impersonation, replay attacks, man-in-the-middle attacks, and session hijacking. The study evaluates existing MFA models and highlights the gaps between formal security proofs and real-world deployment scenarios, especially in resource-constrained mobile environments.

III. PROPOSED METHODOLOGY

The proposed system introduces an advanced Multi-Signature Scheme (MSS) designed to enhance transaction security in blockchain-based DeFi protocols by addressing the vulnerabilities of traditional signature schemes. In this system, multiple signers, including transaction owners and block producers, collaboratively generate a joint signature that is resistant to malleability attacks, ensuring that the transaction ID (TxId) cannot be altered without affecting the transaction's validity. MSS is integrated with additional optimisations, such as executing intermediate transactions through hash functions, to further strengthen security while maintaining efficiency. Although the scheme is more complex and time-consuming than conventional methods, it provides complete protection against transaction malleability, improves scalability, and achieves higher resilience—demonstrated by a 15% increase in resistance against malleability attacks compared to baseline approaches. The Advanced Multi-Signature Scheme (MSS) in our project is designed to enhance the security and integrity of blockchain-based DeFi transactions by addressing the limitations of traditional signature algorithms like ECDSA. By integrating unmalleable transaction implementations and optimisations such as hash-based execution of intermediate transactions, MSS ensures that transaction IDs (TxIds) cannot be altered without affecting the underlying transaction, thereby preventing double-spending or replay issues. Although more complex and computationally intensive, MSS improves transaction efficiency through multi-party coordination and demonstrates enhanced scalability, providing a 15% higher resistance to malleability attacks compared to standard approaches.

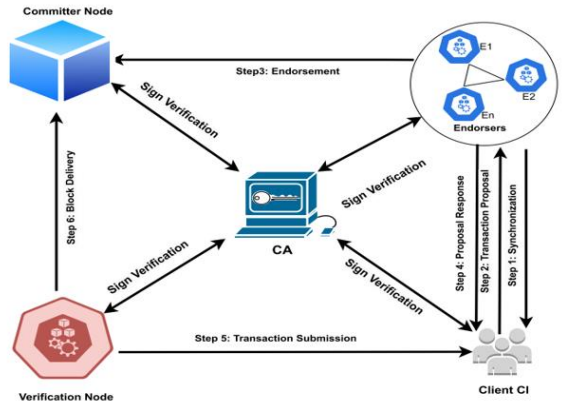
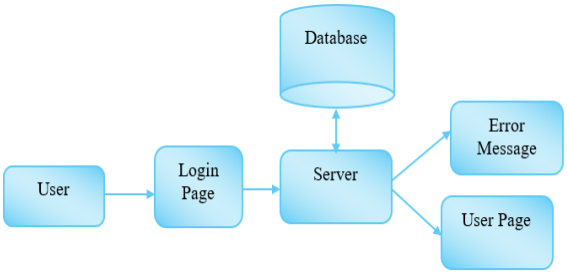


Fig. 1: System Overview

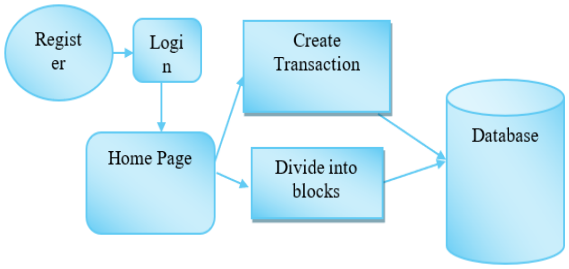
1. User Interface Design

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



2. Block Chain

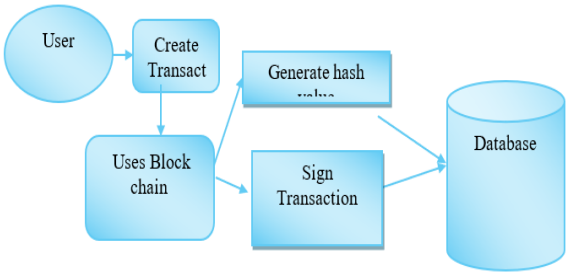
This module is responsible for securely grouping verified transactions into blocks. After producer verification, the system calculates the Merkle Root of included transactions. Then it generates a block hash using SHA-256 based on previous hash and Merkle root. This ensures cryptographic linkage between blocks. Each block stores block id, tx id, block hash, previous hash, and created time. The chaining mechanism prevents alteration of historical data. If a block is modified, all subsequent hashes become invalid. This ensures immutability. The module prevents transaction malleability at the blockchain level. It ensures decentralized ledger consistency.



3. Advanced Multi-Signature Scheme (MSS)

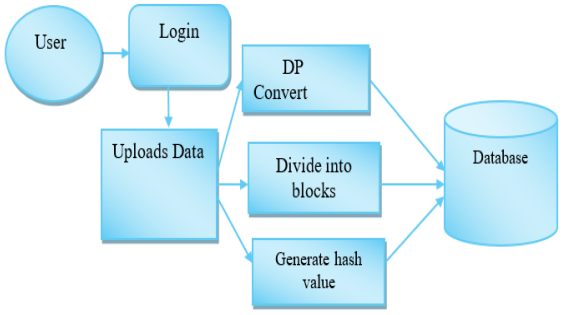
The Advanced Multi-Signature Scheme (MSS) implemented in our project, Secure Multi-Signature Protocol to Counter Transaction Malleability in DeFi, is a cryptographic security mechanism that requires multiple independent digital signatures before a transaction is considered

valid. In our system, a transaction is first created by the user (transaction owner), and a SHA-256 hash is generated to uniquely represent the transaction data. This hash acts as a digital fingerprint and prevents any unnoticed modification. The owner then signs this hash using their RSA private key, ensuring authentication and non-repudiation. This two-level signing process ensures that no single party can manipulate or finalize a transaction independently.



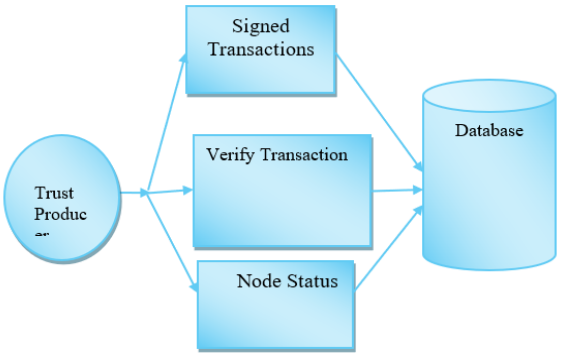
4. Cryptographic Signature Generation

This module implements RSA-based digital signature generation to ensure transaction authenticity. Once a transaction hash is generated, the owner signs the hash using their private key. The system reconstructs the private key securely from stored Base64 format. The SHA256withRSA algorithm is used to generate a digital signature. This ensures that the transaction cannot be altered without invalidating the signature. The signature is stored in the owner signatures table for verification. This module prevents transaction malleability by binding the transaction hash to the owner's identity.



5. SHA-256

In our project, Secure Multi-Signature Protocol to Counter Transaction Malleability in DeFi, SHA-256 plays a critical role in ensuring data integrity and immutability across all modules. SHA-256 is a cryptographic hash function that converts input data into a fixed 256-bit unique hash value, which acts as a digital fingerprint of the transaction. This hash uniquely represents the transaction and ensures that even a small change in data results in a completely different hash value. In the Cryptographic Signature Module, the owner signs this SHA-256 hash instead of the raw transaction data, which strengthens security and prevents tampering.



6. JSP Dashboard

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

7. MySQL Database

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

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed multi-signature scheme (MSS) effectively protects blockchain transactions against transaction malleability attacks. By combining joint signatures from owners and block producers with hash-based transaction execution, the scheme enhances transaction integrity and security. Testbed simulations demonstrate improved scalability and approximately 15% higher resistance to attack success compared to baseline methods. Overall, the proposed protocol provides a secure and reliable solution for DeFi transaction protection.

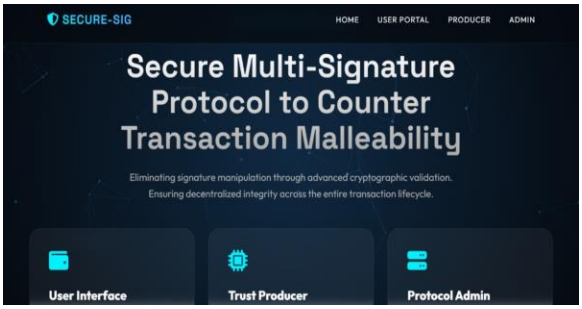


Fig. 2: Home Page

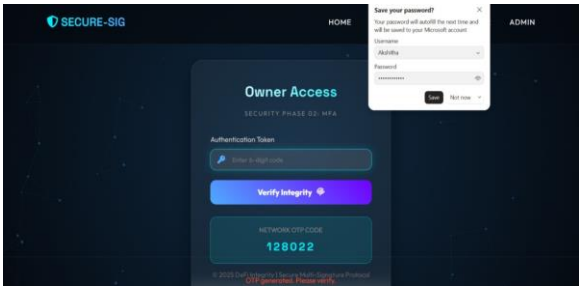


Fig. 3: Owner Access

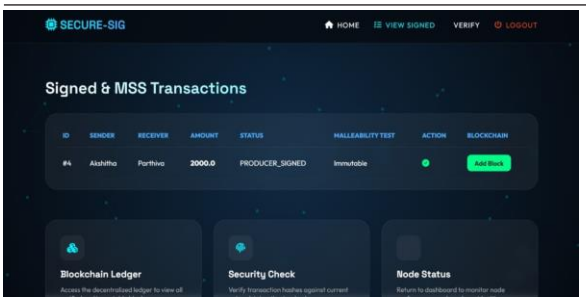


Fig. 4: Transactions

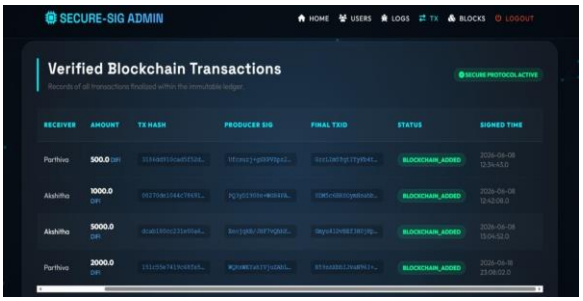


Fig. 5: Verified Transactions

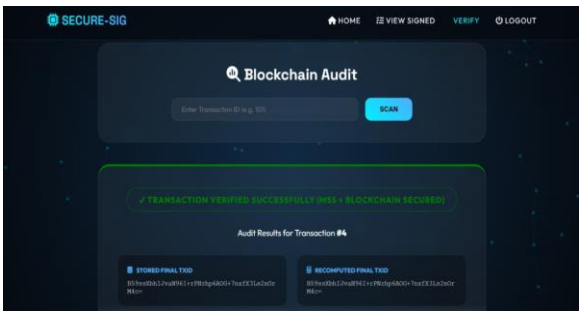


Fig. 6: Enter Transactions

V. CONCLUSION

The conclusion of our project Secure Multi-Signature Protocol to Counter Transaction Malleability in DeFi demonstrates how multi-layer cryptographic validation can effectively secure decentralized financial transactions. Through the integration of User, Trust Producer, and Protocol Admin modules, the system ensures that no transaction is confirmed without multiple levels of authorization. The implementation of SHA-256 hashing guarantees transaction integrity by preventing data tampering. The RSA-based digital signature mechanism authenticates both the owner and the assigned producer, eliminating forgery risks. The producer assignment model strengthens accountability and prevents unauthorized validation. The blockchain component, including Merkle root and block hash generation, ensures immutability of transaction records. Role-based access control enhances system security and prevents misuse. The structured transaction flow—from creation to owner signing, producer verification, and block generation—ensures transparency and traceability. The database design maintains consistency and secure storage of cryptographic data. The system effectively addresses transaction malleability by verifying hashes before confirmation. Modular architecture enables scalability and future enhancements. Administrative monitoring adds governance without compromising decentralization. Overall, the project successfully combines blockchain principles, cryptography, and multi-signature protocols to build a secure and reliable DeFi transaction framework.

REFERENCES

[1] Q.Wang and D. Wang, ‘‘Understanding failures in security proofs of multi-factor authentication for mobile devices,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 597–612, 2023.

[2] B. Aggarwal, D. Rai, N. Kumar, and G. Aggarwal, ‘‘Evaluation of search engine optimization based on blockchain technology,’’ in Proc. 3rd Int. Conf. Technol. Advancements Comput. Sci. (ICTACS), Nov. 2023, pp. 529–534.

[3] S. Mollajafari and K. Bechkoum, ‘‘Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy,’’ Sustain ability, vol. 15, no. 18, p. 13401, Sep. 2023.

[4] A. Nasir, K. Shaukat, K. I. Khan, I. A. Hameed, T. M. Alam, and S. Luo, ‘‘What is core and what future holds for blockchain technologies and cryptocurrencies: A bibliometric analysis,’’ IEEE Access, vol. 9, pp. 989–1004, 2021.

[5] Z. Wang, H. Jin, W. Dai, K.-K.-R. Choo, and D. Zou, ‘‘Ethereum smart contract security research: Survey and future research opportunities,’’ Frontiers Comput. Sci., vol. 15, no. 2, Apr. 2021, Art. no. 152802.

[6] Y. Li, K. Chen, S. Collignon, and D. Ivanov, ‘‘Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability,’’ Eur. J. Oper. Res., vol. 291, no. 3, pp. 1117–1131, Jun. 2021.

[7] X. Feng, J. Ma, H. Wang, Y. Miao, X. Liu, and Z. Jiang, ‘‘An accessional signature scheme with unmalleable transaction implementation to securely redeem cryptocurrencies,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 4144–4156, 2023.

[8]U.Rajput,F.Abbas,R.Hussain,H.Eun,and H.Oh,‘‘Asimpleyetefficient approach to combat transaction malleability in Bitcoin,’’ in Proc. Int. Workshop Inf. Secur. Appl., in Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2015, pp. 27–37.

[9] Y. Liu, X. Liu, L. Zhang, C. Tang, and H. Kang, ‘‘An efficient strategy to eliminate malleability of Bitcoin transaction,’’ in Proc. 4th Int. Conf. Syst. Informat. (ICSAI), Nov. 2017, pp. 960–964.

[10] Akinapalli, S. (2025). Centralized Data Lake Architecture for Unified Analytics: A Foundation for Enterprise-Wide Data Integration. Journal Of Engineering And Computer Sciences, 4(8), 414-422.

AUTHORS Profile



Mrs. K. MAMATHA has received her B. Tech in IT from JNTUH, Hyderabad in 2011, M. Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and She has been dedicated to the teaching field for the last 6 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



Mr. ALLALA SADHVIN RAO pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.