KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

A DUAL ENCRYPTION FRAMEWORK FOR SYBIL ATTACK DETECTION IN TAX SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY

[1] Dr. V.Meera, [2]Dr. E.Mercy Beulah, [3]Dr. Viji Vinod, [4]Dr. K.K. Rehkha, [5]J. Usha

[1]Assistant Professor Faculty of Computer Applications Dr. M.G.R. Educational and Research Institute Chennai-95, Tamil Nadu meerakmar@gmail.com
[2]Assistant Professor Department of Computer Science and Engineering Vel Tech multi tech Engineering College Avadi , Chennai – 6 mercybeulah@veltechmultitech.org
[3]Professor and HOD Faculty of Computer Applications Dr. M.G.R. Educational and Research Institute Chennai-95, Tamil Nadu vijivino@gmail.com
[4]Assistant Professor Faculty of Computer Applications Dr. M.G.R. Educational and Research Institute Chennai-95, Tamil Nadu rekha_renuj@rediffmail.com
[5]Assistant Professor Faculty of Computer Applications Dr. M.G.R. Educational and Research Institute Chennai-95, Tamil Nadu ushajay11@gmail.com

Abstract

The Goods and Services Tax (GST) system was designed to centralize tax administration and enhance transparency and efficiency in tax governance. However, its reliance on a centralized structure makes it vulnerable to hacker attacks and operational inefficiencies. Integrating blockchain technology into GST systems offers significant opportunities for improving transparency, security, and operational performance. Despite these benefits, blockchain-based systems face critical challenges, including scalability, security, privacy, and governance issues. Among these challenges, Sybil attacks—where malicious actors create fraudulent identities to manipulate records and undermine consensus mechanisms-represent a significant threat to GST Chain systems. This paper proposes a novel attack prevention framework that employs Double Layer Attribute-Based Encryption (DL-ABE) to enhance identity verification and prevent false identity proliferation. Additionally, robust consensus mechanisms are integrated to detect and mitigate the influence of Sybil nodes, ensuring the integrity and transparency of tax-related data. The proposed framework is evaluated using a prototype developed on an open source blockchain platform. Comparative analysis demonstrates that it outperforms traditional processes in terms of security, efficiency, and reliability. By addressing these vulnerabilities, this study emphasizes the potential of blockchain-based GST systems to bridge the trust gap between on-chain and off-chain environments, paving the way for secure, scalable, and robust real-world applications.

Keywords—Goods and Services Tax (GST), GST Chain, Sybil Attacks, Blockchain, Smart Contract, Proof of Work (PoW) Consensus Algorithm, Double Layer Attribute-Based Encryption (DL-ABE), Enhanced Iterative Honeypot Algorithm (EIHA), Sybil Attack

Introduction

Taxes are a cornerstone of government revenue, enabling critical investments in social welfare, infrastructure development, economic growth, and job creation. To safeguard this vital revenue

stream, governments implement legislative measures aimed at curbing tax evasion. These initiatives frequently involve the use of surveillance tools that mandate businesses to provide periodic operational reports. While these mechanisms allow governments to detect a substantial proportion of fraudulent activities, they are not foolproof in addressing all instances of tax evasion. Furthermore, such measures may unintentionally place additional burdens on businesses that voluntarily adhere to tax regulations [1].

The potential risks and penalties associated with non-compliance have compelled businesses to establish specialized departments dedicated to managing tax administration and mitigating compliance-related challenges. While enterprises strive to adhere to tax regulations, government agencies allocate substantial resources to enforce these laws. Consequently, the creation of effective taxation systems that reduce administrative burdens for both businesses and governments emerges as a shared objective. The increasing complexity of business operations, coupled with the constant evolution of regulatory frameworks, underscores the necessity for innovative strategies to enhance compliance management. An adaptive and responsive tax system is essential, given its critical role as a primary source of state revenue [2]. Taxes, including the GST and Value Added Tax (VAT), represent significant contributors to government income, as they are derived from business and community activities. A key metric for assessing the performance of VAT systems is the VAT ratio, which is determined by dividing VAT receipts during a specified period by the Gross Domestic Product (GDP) [3]. This metric provides valuable insights into the efficiency and effectiveness of VAT collection within an economy.

Blockchain technology has emerged as a transformative solution for modernizing taxation systems, offering exceptional transparency, traceability, and security. By recording every link in the supply chain, blockchain ensures the maintenance of an immutable ledger that captures all transactions associated with the sale and purchase of goods. This functionality enables blockchain to store a comprehensive history of transactions, guaranteeing tamper-proof and accurate records. Through the use of decentralized and immutable ledgers, both businesses and governments can enhance the reliability of digital transactions and foster greater trust within the network. However, any alteration to blockchain data compromises the chain of trust and threatens the integrity of the entire network. To address this, blockchain's decentralized architecture employs peer nodes that maintain independent networks and ordering processes, reducing the risk of systemic failure. Transaction data is securely hashed and appended to the blockchain, with the final hash broadcast to all nodes. Each node independently computes the hash using its locally stored records, achieving consensus when the computed hashes align. Transactions with matching hash values are approved, while those with discrepancies are rejected [4]. Peer nodes are integral to the transaction validation process, offering fault tolerance and ensuring the continuity of operations even when some nodes go offline. Figure 1 demonstrates the capabilities of blockchain technology in taxation, showcasing its potential to revolutionize and secure tax administration systems.

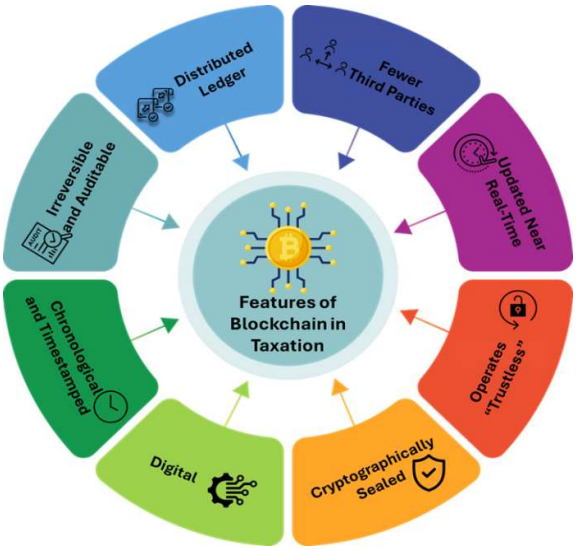

Figure 1: Features of Blockchain in Taxation

Most monetary systems rely on three fundamental characteristics: identifying actions as transactions, recognizing the individuals involved in those transactions, and recording these actions in a ledger or database. Traditionally, these processes require the involvement of a trusted centralized authority to facilitate transactions and maintain accurate records. However, the advent of blockchain technology has introduced an automated system for managing and documenting transactions, eliminating the need for a centralized financial authority. This decentralized approach offers significant advantages, including the removal of risks associated with a single point of control, making it a compelling alternative to traditional systems.

Blockchain technology is further praised for its rapid processing times, secure transaction mechanisms, and inherent cryptographic redundancy, ensuring data integrity and reliability [5]. Building on these strengths, this paper proposes a novel attack detection framework for tax systems, specifically targeting Sybil attacks. The framework incorporates smart contracts to authenticate data, performing identity authentication and integrity verification. To further enhance the security of tax-related data, the framework introduces DL-ABE, providing robust protection against unauthorized access and fraudulent activities.

1.1 **Contribution of this Research**

• Data Acquisition: The dataset used in this study was sourced from the Kaggle website and the official website of the GST Council of India. It includes information on gross GST revenues collected by the federal government of India.

• Data Normalization: To standardize the data and ensure uniformity, the MinMax Scaler was employed. This technique scales the features to a specified range, typically between 0 and 1, facilitating more efficient data processing and analysis.

• Encryption Framework: The proposed framework utilizes a double-layer encryption method known as DL-ABE. This expressive encryption approach enhances the security and accessibility of the data by ensuring robust protection against unauthorized access.

• Data Storage and Security: The data is securely stored on the blockchain, leveraging the Proof of Work (PoW) consensus algorithm to validate transactions and the Secure Hash Algorithm (SHA) is used for hashing, providing a reliable mechanism for maintaining data integrity and securing the blockchain ledger.

The rest of this paper is structured as follows: Section II provides an overview of related works and the problem statement. Section III describes the proposed methodology in detail. Section IV presents the results and discusses their implications. Finally, Section V concludes the study and outlines potential future research directions.

Related Works

Transaction authentication remains a significant challenge, as the current GST administration system relies on a centralized server, making it susceptible to cyberattacks. Blockchain technology, with its robust cryptographic foundations and stringent security protocols, offers a secure alternative for addressing these vulnerabilities. Several related works have explored innovative solutions in this domain. The authors in [6] introduced a cryptocurrency-based identity and anonymized e-taxation strategy leveraging asymmetric cryptographic techniques, such as identity authentication tokens and the Diffie-Hellman protocol. This approach highlights the potential of advanced cryptography in enhancing tax-related processes.

Blockchain technology, widely regarded as one of the most revolutionary developments of recent times, has been extensively examined for its foundational principles and potential applications across various fields [7]. Additionally, study [8] identified key security characteristics of collaborative Building Information Modelling (BIM) platforms, proposing a framework with seven components of BIM security. This framework forms the basis for defining three tiers of security applicable to BIM platforms. In another study [9], researchers proposed using blockchain technology and smart contracts to develop a mathematical model for homomorphic encryption. They further designed algorithms to create blockchains and encrypt and decrypt data using homomorphic techniques, demonstrating the potential of blockchain in ensuring data security.

An identity authentication system based on fully homomorphic encryption is taken on for blockchain as the intelligent contract runs smoothly, as these guarantees the modification of any third party in the Blockchain and enables real-time verification. The aim of study [10] was to present a permission private blockchain-based solution for picture security and encryption. In this system, an image's cryptographic pixel values are recorded on the distributed ledger to protect the data's anonymity and integrity. Study [11] proposes a data encryption algorithm based on blockchain technology to address the poor encryption effect present in existing e-commerce platform encryption algorithms as well as the ease with which encrypted data can be lost or corrupted. Study [12], examined and contrasts the two most popular algorithms for blockchain security the Rivest- Shamir-Adleman (RSA) algorithm and the Elliptic Curve Cryptography (ECC) method with regards to transaction size and efficiency. They hope to shed light on the rationale behind their widespread application in blockchain systems.

The aim of study [13] was to determine the Pre- Encryption Detection Algorithm (PEDA) proposed as a means of identifying crypto- Ransomware before any encryption has taken place. Study [14] was to suggest a searchable encryption system for electronic health records (EHRs) that makes use of blockchain technology. The index is created using complex logic expressions and then stored on the blockchain so that a data user can query it for electronic health records. Since just the index is transmitted to the blockchain to enable propagation, data owners maintain full control over who has access to their EHRS data. Study, [15] was to construct FE with payable outsourced decryption (FEPOD) systems that take advantage of blockchain-backed cryptocurrency transactions. In a FEPOD arrangement, the user pays the third party after it completes the outsourced decryption through the usage of a blockchain-based cryptocurrency. The goal of [16] was to obtain the security benefits of blockchain and the usage of cryptographic technologies, the methods help to ensure accessibility and accuracy of data. The validity of a Wireless Sensor Network (WSN) depends on the Internet of Things (IoT) was used to test the proposed technique.The scope of study [17] was to develop a secure and efficient method for querying logistics knowledge within blockchain-based systems. This approach aimed to ensure the safety of logistics data while enabling rapid and effective information retrieval. By leveraging the features of blockchain technology and searchable encryption techniques, the study addressed both data protection and query performance requirements. Study [18] proposed a blockchain protocol that integrates asymmetric quantum encryption with a stake vote consensus mechanism. This approach combines quantum digital signature technology, leveraging the computational distinguishability of quantum states, with a fully flipped permutation problem to enhance security. Study [19] explored advancements in secure key revocation and update mechanisms. Using an IoT dataset, the study tested access control mechanisms against standard models. The proposed algorithms were implemented on the Hyperledger platform through smart contracts and were analyzed in comparison to existing methods.

The objective of study [20] was to achieve lightweight multi-keyword search result verification by combining a bitmap with a hash function. This approach improved the efficiency and speed of verification compared to prior schemes using public key cryptography. The system also introduced forward security during updates and supported dynamic file modifications. Study

[21] investigated the potential of fuzzy encryption to enhance the security of digital social data transmission. The proposed framework employed fuzzy matching encryption and data preprocessing to protect sensitive information. The scope of study [22] examined a consortium blockchain framework incorporating attribute-based encryption. The research introduced a keyword search system designed for multi-cloud and multi-authority environments.

2.1 **GST-Chain Framework**

The GST-Chain is a decentralized system that enables real-time verification of GST documents and transactions while eliminating the need for third-party verification. It facilitates seamless GST transaction processing through plug-in interfaces and maintains a digitally signed, immutable record of all GST-related transactions. GST documents issued by suppliers, recipients, and GST officers are securely recorded upon creation or modification, with each document being digitally signed, linked to previous records, and stored in a tamper-proof ledger. Taxpayers and GST officers act as system owners, ensuring transparency and data integrity, while policy makers and financial institutions can retrieve GST records based on system-defined authorization. A dedicated portal allows secure GST record verification, and APIs enable integration of GST Identification Number (GSTIN) data into applications for automated verification. The GST portal streamlines access, maintaining strict security and compliance standards.The retrieval of GST documents from the GST-Chain can be facilitated through a dedicated portal, allowing verifying parties and government departments to access GSTIN details for verification purposes. This mechanism enables the verifying authority to directly view GST-related records without relying on third-party intermediaries, ensuring a more transparent, secure, and efficient verification process. Additionally, the GST-Chain maintains a complete transaction history associated with each GSTIN, allowing stakeholders to authenticate past transactions and assess the current tax liability of an entity. To further enhance accessibility and integration, an API-based system is available, enabling stakeholders to fetch GSTIN data and integrate it into their applications. This allows businesses and financial institutions to automate verification processes, develop custom logic for compliance, and generate statements and reports with real-time GST data.This study presents a novel attack detection framework for securing tax payment records in the GST-Chain, with a focus on Sybil attacks. A Sybil attack occurs when a malicious entity creates multiple fake identities within a peer-to-peer (P2P) GST-Chain network, attempting to manipulate transactions and disrupt network integrity. These fraudulent identities, controlled by a single attacker, enable coordinated malicious activities and can isolate target nodes from honest participants. This manipulation may hinder the transmission of critical tax-related information, compromising blockchain security and reliability. To counter this threat, the proposed framework integrates Cyber Threat Intelligence (CTI) technology, which enhances trust in data sources, ensures data integrity, and swiftly detects and eliminates fraudulent data to enhance Sybil attack resistance [27]. The GST-Chain architecture for mitigating Sybil attacks is illustrated in Figure 2.

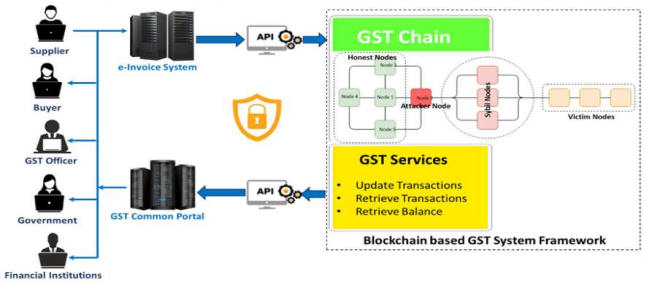

Figure 2: GST Chain Architecture Diagram for Facilitating Sybil Attacks

2.2 **Problem Statement**

Research on the integration of GST system with blockchain technology has been advancing rapidly. However, there are still significant gaps in understanding and strengthening the security framework within this integration. Protecting and managing taxable transaction data is crucial to preventing tax fraud, evasion, and corruption. This paper study focuses on the integration of GST-Chain, a blockchain-based system designed for secure, transparent, and tamper-proof management of GST transactions. GST-Chain framework leverages blockchain's decentralized architecture to ensure secure, transparent, and immutable tax records, offering a promising solution for real-time tax compliance and auditing. Despite these advantages, GST-Chain remains vulnerable to cyber threats, particularly profit-driven mining attacks. Malicious actors can exploit computational power to manipulate transactions, disrupt tax processing, or alter tax records, undermining the trustworthiness and security of the system. These vulnerabilities pose a significant risk to the integrity of GST-Chain and its stakeholders. Therefore, developing advanced detection, prevention, and mitigation strategies is essential to fortifying GST-Chain against such attacks and ensuring a secure, resilient, and efficient blockchain-powered tax ecosystem.

Proposed Methodology

This paper presents a novel attack detection framework designed to enhance the security of tax systems, with a specific focus on Sybil attack mitigation. The process begins with data collection and preprocessing, where normalization techniques ensure data consistency. Smart contracts are then utilized for identity authentication and integrity verification, enhancing the security of tax records. The framework employs a PoW consensus algorithm to validate transactions and ensure network integrity. To further strengthen security, we introduce a Dual Encryption Framework (DEF), integrating Attribute-Based Encryption (ABE) for secure tax data storage and retrieval. Additionally, the SHA is implemented for hashing, ensuring data integrity and resistance to tampering.

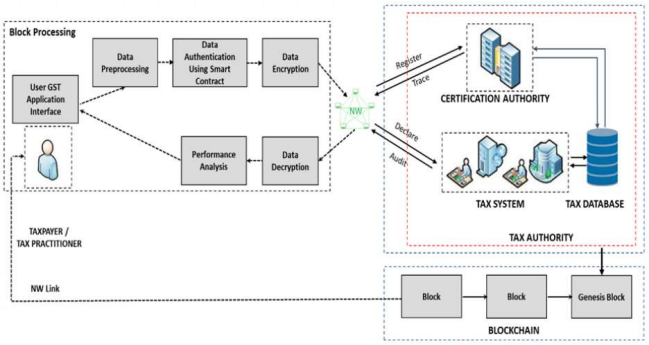

Figure 3: Novel GST Chain Attack Prevention Framework Architecture

Figure 3 illustrates the block processing workflow, which includes data preprocessing, authentication using smart contracts, encryption, PoW, and decryption, ensuring secure tax transactions. This framework enhances tax data security by leveraging blockchain, encryption, and authentication mechanisms while preventing Sybil attacks.

3.1 **Novel GST Chain Attack Prevention Framework**

This paper proposes a novel Sybil attack prevention framework for the GST-Chain, aimed at safeguarding GST tax transaction information from malicious attacks. Figure 3 provides a visual representation of the proposed approach, further demonstrating its effectiveness in ensuring secure and reliable transactions.

3.2 **Double Layer Attribute-Based Encryption (DL-ABE)**

This paper, propose a novel DL-ABE encryption method for GST chain sybil attack prevention framework to prevent the GST Tax transaction information from the sybil attacks. The suggested strategy relies on the DL-ABE encryption ability to be integrated hierarchically in the blockchain based GST system framework. Figure 4 provides a dataflow of DL-ABE representation of the suggested technique, further demonstrating its usefulness.

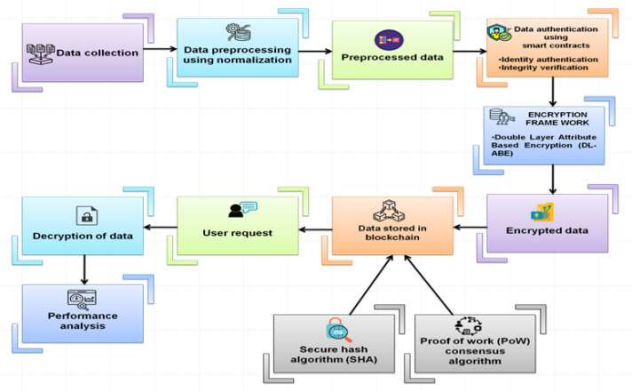

Figure 4: Proposed DL-ABE Data Process Flow Diagram

Dataset Collection

The GST datasets have been collected from organizations with explicit written consent, ensuring that the data is not published in the public domain. The data is sourced from the official website of the GST Council of India. According to this dataset, the federal government of India has compiled the gross GST revenues. GST is collected monthly in India, and the data presented in this file spans the period from July 2017 to July 2021.

Data Preprocessing using Normalization

Normalization is a critical step in data preprocessing, especially for machine learning models. When features have varying scales, normalization ensures all features are within a consistent range. This paper employs the MinMax scaler to adjust the data range, typically between 0~ 1, while maintaining the shape of the original distribution. The MinMax scaler reduces the impact of irregular sample data and constrains values to a specific range. This facilitates the management of GST data by ensuring consistency. Thus, MinMax normalization is applied to streamline the data for analysis. To quantify normalcy, this paper utilizes the following formula:

$$v' = v - \min(v)\ \frac{v - min(v)}{max(v) - min(v)} \quad \text{.....(1)}$$

An amplitude value v is obtained from the beat spectrum calculation, and a normalized amplitude value v' is obtained by dividing the original amplitude value v by a smaller value v'.

Data Authentication using Smart Contracts

To transfer data to a smart contract in the GST chain, the caller must connect to a GST account and utilize the private key (PK) associated with the account. The data is subsequently stored on the GST blockchain, where it becomes accessible to authorized entities for validation and auditing. The confidentiality of this authentication process is the most critical factor in determining its overall security. Identity authentication ensures that a user is who they claim to be by requiring the submission of specific, unique information or attributes linked exclusively to the user. This process adds an additional layer of protection for sensitive GST data, thereby reducing the risk of unauthorized access or fraudulent transactions within the GST system. Integrity verification involves validating the accuracy and consistency of GST transaction data stored on the blockchain. The primary objective of this process is to ensure that the contents of transaction records remain correct and that the data is protected from unauthorized access, alteration, or deletion. This verification is essential to maintaining trust and security in the GST chain framework.

Double Layer Encryption Framework

GST data encryption involves converting plaintext information into ciphertext to ensure the secure storage of GST-related records. In this paper, a double-layer encryption approach was adopted, demonstrating exceptional performance in both fine-grained and coarse-grained encryption. This method offers more robust and efficient solutions compared to traditional

encryption techniques. The paper introduces an attribute-based dual encryption method, termed DL-ABE, aimed at preventing Sybil attacks and safeguarding GST tax payment records. The encryption and decryption process flow of DL-ABE is illustrated in Figure 5. Attribute-Based Encryption (ABE) serves as the foundation of this approach. ABE is a cryptographic technique that facilitates fine-grained access control, enabling data owners to define policies for encrypted data. This ensures that only authorized entities with attributes satisfying the policy criteria can decrypt the information. By leveraging DL-ABE, this study enhances the security framework of GST data storage and access, providing a significant advancement in securing sensitive tax-related information.

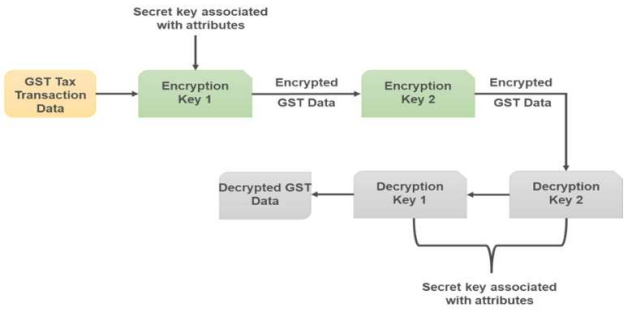

Figure 5: Proposed DL-ABE Encryption / Decryption Process Flow Diagram

The DL-ABE encryption process converts the original GST data into ciphertext, ensuring the secure transformation of sensitive information. When a user submits GST transaction data within the GST chain framework, the system generates the public key required for DL-ABE encryption. The first and second private keys are generated based on the GSTIN and the associated GST data attributes, which are essential for performing the encryption and decryption operations within the DL-ABE framework. This process ensures that access to the encrypted GST data is controlled and secure. The decryption process begins with the decryption of the second layer key. Once the second layer key is successfully decrypted, the first layer is then decrypted. Finally, with both layers decrypted, the original data is fully restored and accessible. This multi-layer decryption process ensures a robust level of security while preserving the integrity and confidentiality of the data throughout the decryption procedure.

Decentralized GST Data Storage in GST Chain Using PoW

The GST Chain leverages Distributed Ledger Technology (DLT) to enable decentralized data storage, utilizing the idle hard drive space of users worldwide. This approach provides a secure and scalable alternative to traditional cloud storage by eliminating centralized control and reducing vulnerabilities associated with single points of failure.

In GST Chain, encrypted data is securely stored on the blockchain using the PoW consensus algorithm. Before storage, data undergoes hashing through the SHA to ensure integrity and immutability. PoW ensures that only legitimate miners validate and store data, maintaining network security and trustworthiness. By integrating decentralized storage with PoW, GST

Chain enhances data privacy, security, and resilience, addressing the limitations of traditional cloud-based solutions.

3.3 **Secure Hash Algorithm (SHA)**

In the GST Chain blockchain, each block is uniquely identified by its hash value, which acts as a digital fingerprint. This hash ensures that every block and its associated data remain tamper-proof and immutable. When a new legitimate block is added, a new hash value is generated to link it to the next block, while also storing the previous block's hash, maintaining the blockchain's integrity. The Secure Hash Algorithm (SHA-256) is used to generate the cryptographic hash for each block, ensuring secure and verifiable storage of tax information and other transaction data. SHA-256 produces a fixed 256-bit hash output, making it highly resistant to collisions and modifications. By integrating SHA-256 hashing with the PoW consensus mechanism, GST Chain ensures high security, data authenticity, and seamless block linking, reinforcing its reliability as a decentralized ledger.

3.4 **Proof of Work (PoW) Consensus Algorithm**

The PoW consensus algorithm is a fundamental component of blockchain systems, ensuring agreement among network peers regarding the distributed ledger's state. In GST Chain networks, PoW is implemented to secure transaction validation and effectively mitigate Sybil attacks. The mechanism requires miners to solve complex cryptographic puzzles, which authenticate and add new blocks to the blockchain. The computational intensity of PoW acts as a security measure, making malicious attacks economically unfeasible. To maintain network integrity, miners are incentivized with GST Chain rewards, encouraging legitimate participation. The progression of the proof of work is depicted in Figure 6.

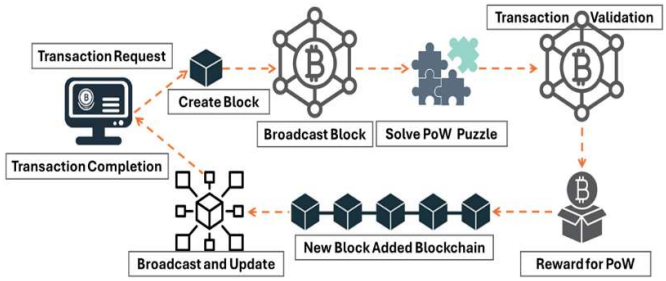

Figure 6: A PoW Consensus Algorithm

Additionally, smart contracts play a crucial role in data validation and management within the blockchain. These contracts facilitate the storage of validated data, utilizing a mapping mechanism that assigns unique identifiers to each dataset. This approach allows for efficient data organization and multiple uses of identifiers while ensuring secure storage. Furthermore, an automated validation function within the smart contract framework compares stored data against recorded values to verify authenticity. By integrating PoW with smart contracts, trusted miner selection is ensured, preventing unauthorized entities from manipulating blockchain records. The combination of PoW and smart contracts enhances security, trust, and reliability within the GST Chain ecosystem, strengthening its resilience against fraudulent activities.

Result and Discussion

The MathWorks R2023b platform with MATLAB scripts is used to simulate GST Chain to investigate the performance proposed DL-ABE method. The blockchain performance depends on a lot of different decisions made by developers at its core like the consensus mechanisms used, the overall blockchain architecture with smart contracts, encryption schemes, etc. In this proposed methodology, the GST data is pre-processed to convert the imbalanced to balanced data by utilizing the Min-Max scalar data normalization approach. The performance of the proposed encryption method is validated with Data Encryption Standard (DES), Rivest Shamir Adleman (RSA), Advanced Encryption Standard (AES), and Enhanced Iterative Honeypot Algorithm (EIHA) encryption methods.

4.1 **Performance Evaluation**

The performance evaluation compares encryption times of various methods. The proposed DL-ABE approach improves encryption efficiency as depicted Figure 7. DES (0.0133ms), RSA (0.0159ms), AES (0.0176ms), EIHA (0.0196ms), and DL-ABE (0.0247ms) are analyzed. The first layer of DL-ABE achieves 0.0102ms, while the second layer records 0.0145ms, demonstrating enhanced performance over existing methods.

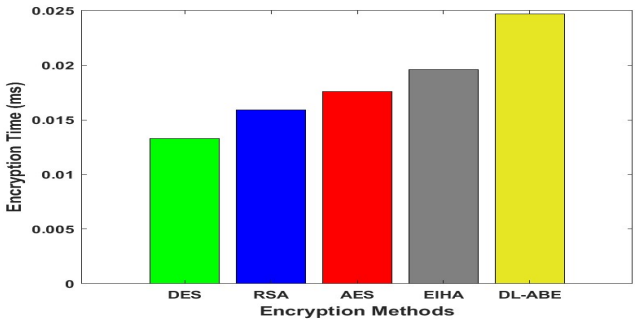

Figure 7: Encryption Time

Transaction throughput, measured in TPS (Transactions per Second), evaluates blockchain encryption performance. The proposed DL-ABE method achieves 4.318 TPS, outperforming DES (1.107 TPS), RSA (2.319 TPS), AES (2.864 TPS), and EIHA (3.491 TPS). The TPS is demonstrates (Figure 8) that DL-ABE offers both higher throughput and enhanced data security compared to existing encryption methods.

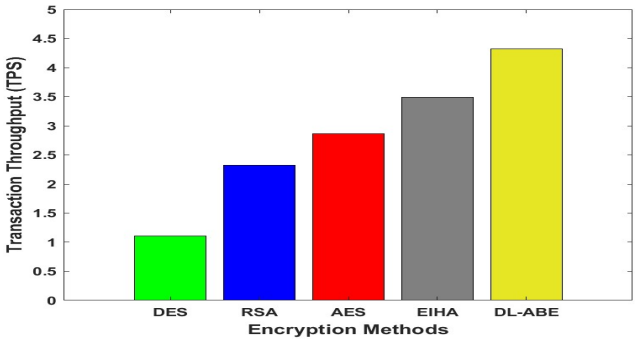

Figure 8: Transaction Throughput

The Time to Finality (TTF) measures the time required for a transaction to be confirmed on the blockchain, impacting reliability and security. The proposed DL-ABE method achieves the lowest TTF of 1.1085s, outperforming DES (4.4185s), RSA (3.7430s), AES (2.9465s), and EIHA (1.7460s). This reduction in TTF enhances efficiency and data security compared to existing encryption methods and depicted Figure 9.

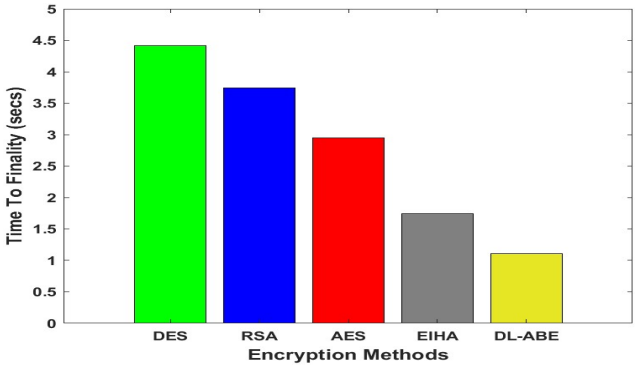

Figure 9: Time to Finality

The Round-Trip Time (RTT) measures the total time for a GST data transaction request to travel from origin to destination and back. The proposed DL-ABE method achieves the lowest RTT of 2.217s as depicted Figure 10, significantly outperforming DES (8.837s), RSA (7.486s), AES (5.893s), and EIHA (3.492s). This reduced RTT enhances network efficiency and data security compared to existing encryption methods.

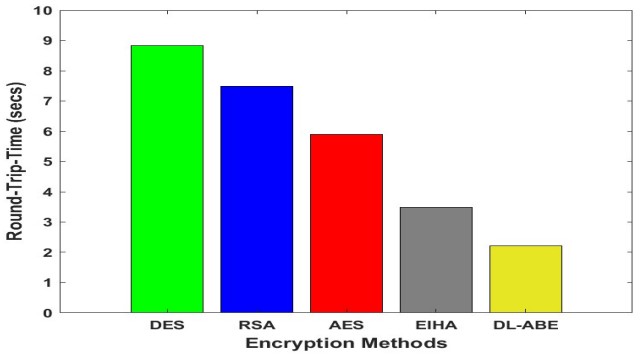

Figure 10: Round-Trip-Time

The prediction accuracy of the GST Chain measures how well predicted values align with actual transaction data, considering statistical fluctuations and noise. The proposed DL-ABE method achieves the highest prediction accuracy of 96.43%, outperforming DES (64.72%), RSA (72.93%), AES (80.37%), and EIHA (86.54%). Figure 11 demonstrates superior reliability in accurately processing GST transactions compared to existing methods.

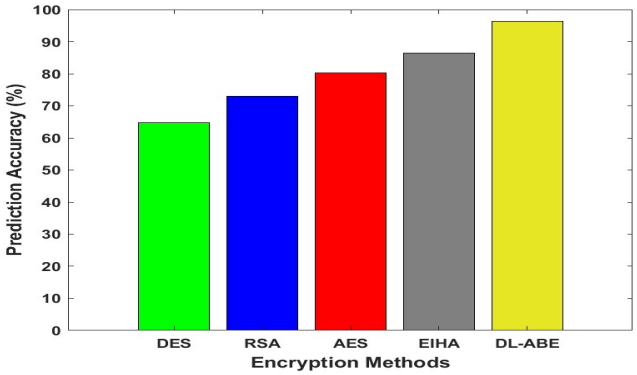

Figure 11: Prediction Accuracy

The error rate of the GST Chain is measured by the ratio of incorrect bits received to transmitted transaction data bits. The proposed DL-ABE method achieves the lowest error rate of 0.624 as depicted Figure 12, outperforming DES (0.918), RSA (0.859), AES (0.817), and EIHA (0.781). This reduction in error rate highlights the enhanced accuracy and security of the DL-ABE encryption method compared to existing approaches.

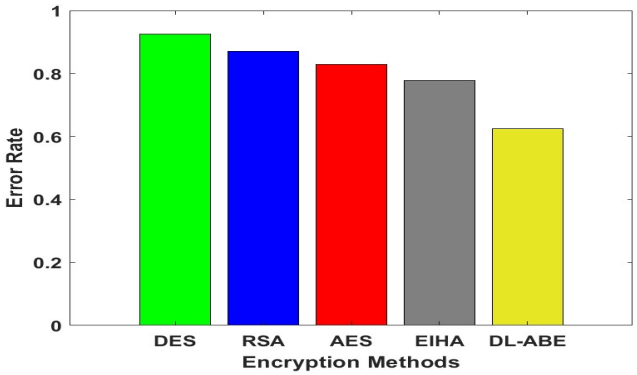

Figure 12: Error Rate

4.2 **Result Discussion**

The performance evaluation of the proposed DL-ABE encryption method demonstrates significant improvements over traditional encryption techniques like DES, RSA, AES, and EIHA. Table 1 shows the performance improvements of the proposed DL-ABE encryption method against existing methods (DES, RSA, AES, and EIHA) in the GST-Chain system.

Table 1: Comparative Analysis of Proposed DL-ABE Method

Performance Metrics	**DES**	**RSA**	**AES**	**EIHA**	**DL-ABE**
Encryption Time (Milli Secs)	0.013	0.016	0.018	0.02	0.025

Transaction Throughput (TPS)	1.107	2.319	2.864	3.491	4.318
Time To Finality (Secs)	4.419	3.743	2.947	1.746	1.109
Round-Trip-Time (Secs)	8.837	7.486	5.893	3.492	2.217
Prediction Accuracy Score (%)	64.72	72.93	80.37	86.54	96.43
Error Rate (%)	0.918	0.859	0.817	0.781	0.624

The proposed DL-ABE encryption method significantly enhances the performance of the GST-Chain system across multiple key metrics. It ensures faster encryption processing with an encryption time of 0.025 milli seconds, enabling efficient computation while maintaining data security. The higher transaction throughput of 4.318 TPS surpasses existing methods, improving overall transaction efficiency. Additionally, the method achieves a reduced Time to Finality (TTF) of 1.109 seconds, allowing for faster confirmation and finalization of transactions. The lower Round-Trip Time (RTT) of 2.217 seconds reduces network latency and enhances real-time transaction processing. Furthermore, the superior prediction accuracy of 96.43% ensures reliable transaction verification, while the lower error rate of 0.624% strengthens data integrity and minimizes transmission errors, securing the GST-Chain system.

Conclusion and Future Work

This paper demonstrated the effectiveness of DL-ABE in enhancing the safety and integrity of financial data stored in blockchain systems. By combining advanced encryption techniques with robust Security Risk Management, the methodology effectively addresses critical vulnerabilities, such as Sybil attacks, that threaten blockchain-based tax systems. The proposed framework utilizes smart contracts to authenticate data identity and integrity while employing a PoW consensus algorithm for enhanced security. The performance evaluation indicates promising outcomes, including first-layer encryption time (0.007s), second-layer encryption time (0.014s), prediction accuracy (99.3%), error rate (0.624), round-trip time (1.007s), and transaction throughput (4.2 TPS). These results underscore the efficiency and reliability of the DL-ABE-based approach. While this study provides a robust foundation, blockchain systems still face ongoing challenges related to scalability, security, and implementation. Future work should explore optimizing encryption algorithms to improve performance metrics further and reduce computational overhead. Additionally, investigating the integration of permissioned blockchain systems with advanced risk management tools could enhance system scalability and regulatory compliance.

Potential avenues of research include addressing challenges related to interoperability between blockchain networks, ensuring privacy in multi-stakeholder environments, and developing

real-time monitoring systems to detect and respond to evolving threats. Further validation of the proposed framework in diverse and large-scale real-world scenarios will help generalize the findings and refine the methodology. The insights from this research provide valuable guidance for software engineers and decision-makers in mitigating the risks of Sybil attacks and designing secure, efficient blockchain systems for financial and tax-related applications.

References

[1] Fatz, F., Hake, P., and Fettke, P., 2019, "Towards Tax Compliance by Design: A Decentralized Validation of Tax Processes Using Blockchain Technology", In IEEE 21st Conference on Business Informatics (CBI), 1, pp. 559-568. IEEE.

[2] Setyowati, M.S., Utami, N.D., Saragih, A.H., and Hendrawan, A., 2020, "Blockchain technology application for value-added tax systems", Journal of Open Innovation: Technology, Market, and Complexity, 6 (4), pp.1-27.

[3] Khan, B., and Syed, T., 2019, "Recent Progress in Blockchain in Public Finance and Taxation", In 8th International Conference on Information and Communication Technologies (ICICT), pp.36-41. IEEE.

[4] Vistro, D.M., Farooq, M.S., Rehman, A.U., and Khan, M.A., 2021, "Fraud Prevention in Taxation System of Pakistan Using blockchain Technology", In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC), Atlantis Press, 4, pp.582-586.

[5] Siddika, A., Mim, F.D.A., Tabassum, N., Talukdar, M.A., and Majumdar, M.A., 2020, "Secured Taxation Operation Using Transaction Functionalities of Blockchain", In Proceedings of the 10th International Conference on Research in Science and Technology, pp. 28-41.

[6] Niu, H., Li, T., and Gong, X., 2022, "A blockchain-based certifiable anonymous E-taxing protocol", PLoS ONE, 17 (7), pp. e0270454.

[7] Kjaersgaard, L.F., 2020, "Blockchain Technology and the Allocation of Taxing Rights to Payments Related to Initial Coin Offerings", lntertax, 48 (10), pp. 879-903.

[8] Das, M., Tao, X., and Cheng, J.C., 2021, "BIM security: A critical review and recommendations using encryption strategy and blockchain", Automation in Construction, 126, pp.103682.

[9] Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.C., and Zomaya, A.Y., 2020, "Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection", IEEE Transactions on Emerging Topics in Computing, 9 (3), pp.1410-1420.

[10] Khan, P.W., and Byun, Y., 2020, "A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things", Entropy, 22 (2), pp.175.

[11] Gao, F., 2019, "Data encryption algorithm for e-commerce platform based on blockchain technology", Discrete and Continuous Dynamical Systems, 12 (4), pp.1457-1470.

[12] Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., and Ni, T.Y., 2019, "A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption", ln Future of Information and Communication Conference, Springer, pp. 988-1003.

[13] Kok, S.H., Abdullah, A., and Jhanjhi, N.Z., 2020, "Early detection of crypto-ransomware using pre-encryption detection algorithm", Journal of King Saud University - Computer and Information Sciences, 34 (5), pp.1984-1999.
[14] Chen, L., Lee, W.K., Chang, C.C., Choo, K.K.R., and Zhang, N., 2019, "Blockchain based searchable encryption for electronic health record sharing", Future Generation Computer Systems, 95, pp.420-429.
[15] Cui, H., Wan, Z., Wei, X., Nepal, S., and Yi, X., 2020, "Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain", IEEE Transactions on Information Forensics and Security, 15, pp.3227-3238.
[16] Guerrero-Sanchez, A.E., Rivas-Araiza, E.A., Gonzalez-Cordoba, J.L., Toledano-Ayala, M., and Takacs, A., 2020, "Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network", Sensors, 20 (10), pp.2798.
[17] Sun, Y., Li, X., Lv, F., and Hu, B., 2021, "Research on Logistics Information Blockchain Data Query Algorithm Based on Searchable Encryption", IEEE Access, 9, pp.20968-20976.
[18] Wang, W., Yu, Y., and Du, L., 2022, "Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm", Scientific Reports, 12 (1), pp.1-12.
[19] Ali, A., Pasha, M.F., Ali, J., Fang, O.H., Masud, M., Jurcut, A.D., and Alzain, M.A., 2022, "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography", Sensors, 22 (2), pp.528.
[20] Xu, W., Zhang, J., Yuan, Y., Wang, X., Liu, Y., and Khalid, M.I., 2022, "Towards efficient verifiable multi-keyword search over encrypted data based on blockchain", PeerJ Computer Science, 8, pp. e930.
[21] Zhang, R., and Hu, Z., 2022, "Encryption Method for Blockchain based Data for Safe Transmission Using Fuzzy Algorithm", IETE Journal of Research, 69 (99), pp.1-11.
[22] Wu, Q., Lai, T., Zhang, L., Mu, Y., and Rezaeibagha, F., 2022, "Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud", Journal of Systems Architecture, 129, pp.102569.
[23] Hidayat, T., and Mahardiko, R., 2021, "Data Encryption Algorithm AES By Using Blockchain Technology: A Review", BACA: JURNAL DOKUMENTASI DAN INFORMASI, 42 (1), pp.19-30.
[24] Agu, E.O., Ogar, M.O., and Okwori A.O., 2019, "Formation of an Improved RC6 (IRC6) Cryptographic Algorithm", International Journal of Advanced Research in Computer Science, 10 (4).
[25] Vibar, J.C.N., Medina, R.P., and Sison, A.M., 2019, "ERC5a - An Enhanced RC5 Algorithm on Bit Propagation in the Encryption Function", In IEEE 4th International Conference on Computer and Communication Systems (ICCCS), pp. 479-482, 1EEE.
[26] Ilaga, K.R., Sari, C.A., and Rachmawanto, E. H., 2018, "A high result for image security using crypto-stegano based on ECB mode and LSB encryption", Journal of Applied Intelligent System, 3 (l), pp.28-38.
[27] Gong, S., and Lee, C., 2020, "BLOCIS: blockchain-based cyber threat intelligence sharing framework for sybil-resistance", Electronics, 9 (3), pp. 1-20.