International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ENHANCED BLOCKCHAIN SECURITY FOR GST BASED ON SHUFFLE CHAIN LINK PROOF AGREEMENT

[1] Ms. Gayathri B, [2] Dr. Vishwa Priya V,
Research Scholar, Department of Computer Science,
Vels Institute of Science, Technology and Advanced Studies, Chennai.
Email Id : gayaramesh0304@gmail.com
Orcid: 0009-0008-8447-0187
[2]Assistant professor, Department of Computer Science
Vels Institute of Science, Technology and Advanced Studies, Chennai.
Email Id : drvishwapriyathamizharasu@gmail.com
Orcid: 0000-0002-4678-9516

Abstract

With the rapid advancement of blockchain technology, smart contract execution and executio n infrastructure have increased importance in recent years. Blockchain technology is the primary enabler of smart contracts and offers assurance on their effectiveness due to its robust and secure base. Blockchain's transparency, decentralization, and security make it an innovative technology that is indispensable in modern society. The Goods and Services Tax (GST) blockchain for the delivery of goods and services is a multi-layered intermediate tax system that extends from producers to end users. The primary issue with current solutions is that security and resilience are not balanced in their design. Crucial Compromise Unauthorized access tools and a lack of authenticated services could endanger important data. To overcome the issues, we proposed the method Shuffle Chain Link Proof Agreement Based Elliptic curve cryptography (SCLPA-ECC) with Proof of Authority (PoA) Algorithm for validating the trust GST smart contract transaction. User Identity Verification (UIPV) ensures secure transactions in cloud environments. A decentralized blockchain stores each data in a different location within the block. It creates a hash ID for each Goods and Services Tax (GST) chunk and encrypts it using a hash-indexed subset selection (HIS) based key value. Chain-link integration sequentially generates unique keys for each block, enabling secure communication and transactions in a decentralized blockchain environment. Using a Proof of Authorization (PoA) technique for data access, it approves user transactions. The Master Node Key Policy (PNKP) uses confirmed keys from the master to regulate block generation. The cost is made simpler during the user authentication stage by using searchable attribute key access points. The security analysis concludes by demonstrating that a decentralized blockchain network can achieve conventional centralized audit, publication, and certificate verification outcomes, hence enhancing security and transparency.

Keywords: Goods and Services Tax, blockchain, Hash Indexing, Proof of Authority, Chain Link, Elliptic curve cryptography, private key, Attribute, Primary Node, smart contracts, security.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

Blockchain technology could make tax procedures more efficient. A range of goods and services that are provided by various suppliers or service providers throughout the production and service stages are subject to the Goods and Services Tax (GST), sometimes known as the Goods and Services Tax. GST on the purchase of various goods and services. There are two main parts to GST. They are the Central Goods and Services Tax (CGST) and the State Goods and Services Tax (SGST)/Union Territories Tax (UGST). The administration and collection of GST is a rather complex process. Let's now examine how a distributed ledger platform, one of blockchain's advantages, aids in the administration of the overall tax management system.

In order to connect and record the GST transactions of different stakeholders involved in GST administration in a single chain, the GST chain was created utilizing blockchain technology. The GST chain keeps track of the taxpayer's current tax obligations and tracks all of their transactions. Three main decentralized storage designs exist. Rich resources, including network management and capacity, are available through public distributed storage management and are inexpensively accessible via the Internet. Second, clients have independent capacity control authority, and private, dispersed storage is protected by the company firewall. Third, 50/50 distributed storage offers cloud management on-premises and in the public domain. focuses on satisfying the accessibility requirements of the client. Information is out of the customer's actual control and security is severely jeopardized when dealing with the overhead expenditures of administrative staff and warehouse facilities near the consumer.

When sending data to dispersed storage media, the client must handle information security concerns. Information is typically transmitted in an encrypted format. The potential examination of jumbled data is commonly referred to as reliable monitoring. Reconciliation time and errors can be greatly decreased by using smart contracts to automatically match data between buyers and sellers. Smart contracts are a reliable mechanism as they don't require middlemen like banks or attorneys to monitor transactions. A cost-effective method of carrying out a number of activities, such as supply chain management, financial transfers, and real estate transactions, is through smart contracts.

To address the issue of how to use the server to finish the search while the hashing information is stored in the cloud, researchers created the Random Chain Connection Proof Protocol Shuffle Chain Link Proof Agreement Based Elliptic curve cryptography (SCLPA-ECC) is proposed. Innovation is explored in Proof of Authority (PoA). Decentralized blockchain is a quick invention that came about as a result of extensive digital innovation. Client processing effort is decreased by decentralized blockchain. A searchable feature Cost calculations are made easier at the user authentication level by using key access points. According to the report, decentralized blockchain networks replace public, authentication verification judgments, hence boosting transparency and point-to-point security over traditional centralized audits.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

.

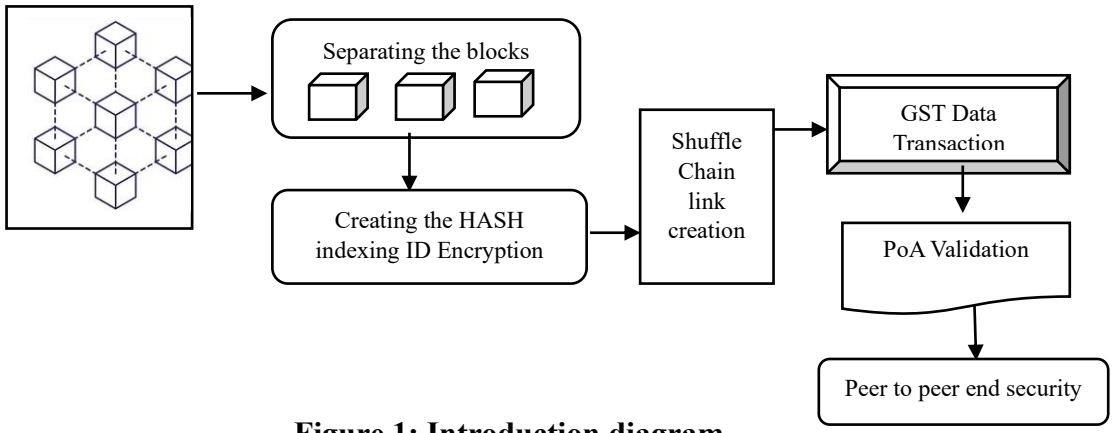

Figure 1: Introduction diagram

Figure 1 described Blockchain Transaction Diagram for Encrypted PoA Algorithm-Based GST Data Transactions A period, an encoded hash, and the hash value of the blocks before it in the chain are all included in each block. Information on the blockchain is thus shielded against corruption. Information security is provided by blockchain, and some users are participating customers who are worried about the security of GST. Peer-to-peer endpoint messages can be monitored thanks to information security and protection. The consensus mechanism of the blockchain network ensures that the data recorded on each node is consistent. PoA is a technique where an attacker avoids loss in exchange for recovering commodities or services with every transaction.

2. Related work

Blockchain-based payments on trustless chain networks will be made possible by this transaction, which attempts to address the issue of poor on-chain scalability. One of the main issues with current designs is that they fail to strike a balance between security and resilience. If it could offer comfort without compromising elasticity, it would be even more practical [1]. When paired with blockchain, user privacy is safeguarded and data harm can be prevented to a great degree. Despite blockchain's ability to secure mobile communications, operating expenses continue to increase [2]. The evolution, architecture, development framework, applications, problems, features, and security issues of blockchain technology were all thoroughly examined [3].

Businesses only provide manufacturing documents to regulators for examination if the vaccine is going to be sold. It is simple to falsify and fabricate manufacturing documents. [4] to address the drawbacks of conventional centralized administration. Permissioned blockchains are being used by businesses more and more to handle and preserve company data and transactions on an unchangeable, private ledger. The complete development of permissioned blockchains as B2B application facilitators depends on interoperability, which enables communication and information sharing between platforms.

Recognized the advantages of blockchain technology beyond its successful application in bitcoin. Blockchain technology has been shown to have uses in supply chain management, the energy and financial trading sectors, system integrity, equipment networking evaluation, security, and identity. However, the rich functionality of blockchain technology is one

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

distinctive feature that draws scholars to it.[6]. The blockchain ecosystem is made more complex by this distinction. As a result, it is now challenging to obtain a comprehensive and current understanding of the wide variety of existing blockchain and blockchain-like systems [7].

Public blockchains, however, are the subject of most blockchain sharing research. Prior studies were unable to enable stringent transaction atomicity, short availability, multi-shard contract calls, and high cross-shard efficiency for federated chains. These are an alliance chain system's fundamental needs and difficulties [8]. Find out more about implementing blockchain-based telecom network solutions, assessing expenses, contrasting on-premise, IaaS, and BaaS infrastructure alternatives, and selecting the best blockchain platform [9].

Threat agents compromise valuable assets and services by taking advantage of these risks and weaknesses. The most pertinent security risks in blockchain systems are observed and taken into consideration, as well as two security threats (double spend and civil) are investigated using a security risk management (SRM) domain model [10].

Table 1 Existing survey work for Blockchain smart contract transaction

Author name/Year	Proposed Method	Limitations	Performance Metrics
M. Muneeb et al/2022 [11]	Blockchain-based smart contract	Manual contracts not valid	Security-95.09%
A. Saini et al /2022	logical stateless transaction [12]	no provision of prioritizing	Security-98.25%
E. Chen et al/2023	SLC-based SPESC	must not just receive monetary compensation for actions based on consumption [13]	Security-89.65% Time complexity52sec
S. Wang et al/2019	Smart Contract-Based Framework [14]	Security and Privacy Issues	Encryption time-32m.sec Security-98%
Y. Zhu et al /2021	Language for Asset-Driven Smart Contracts Facilitating Ownership Transactions	usufruct, and disposition of asset [15]	length of Transaction-39.2%
Y. Fang et al/2024	Parallel Virtual Machine	inter-contract parallel execution [16]	validation performance-33.4%
Y. Pang et al/2022	Hyperledger Fabric	Possibility of leaking users' privacy [17]	validation performance-58.4%

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Y. Jiang et al/2019	Smart contract-enabled blockchain	lack trust and robustness [18]	service transactions 95.25%
P. G. Hunn et al/2019	Policy based smart contracts	Low efficiency [19]	Validation time 25m.sec
J. Li, et al/2022	Random Contract Approach (RCA) [20]	Low efficiency and rising transaction prices	Cost-44.65%
H. Su et al/2022	smart contract-based methods	Security and Privacy Issues [21]	Encryption time-34m.sec Security-95%
S. Khan et al/2021	Hashed Time Lock Contract (HTLC) [22]	Invites losses	Security-94.25%

To address the authentication data security problem in data transactions and make data transactions auditable, responsible, and comprehensive, suggest a blockchain solution for data transfer authentication that is built on alliance chains and smart contracts. Peer chains made with proof-of-authority systems are quicker and less expensive. Smart contracts may be used safely and conveniently thanks to the alliance chain [23]. The challenges that people from many areas face while reading, comprehending, and working together to create smart legal contracts, Advanced Smart Contract Language (ASCL) was created. However, commercializing such a language has been challenging because there is currently no effective method for converting ASCL into executable smart contract applications [24]. Automatic verification and signing of the unique contract occur when the predetermined requirements are met. Smart contracts are utilised in various facets of social life, not only financial transactions. Despite its clear benefits, smart contract technology is still in its infancy and has a number of problems that need to be fixed [25].

The gathered data is used to compute a number of statistics regarding the smart contract's ether balance, naming strategy, transactions, activity, and other dimensions that define its use and intent. We discovered that the quantity of balances and transactions has a power-law distribution, and software index measures are more volatile but generally have lower values than their typical software equivalents [26]. A computer program that cannot be changed is called a smart contract. Smart contracts can be used in a variety of situations due to their adaptability and security. Specifically, legally permissible contracts can be automated with smart contracts [27].

The Indian Constitution governs the implementation of the Goods and Services Tax (GST). The primary goal of the GST is to give everyone access to a single taxing system. In India, the VAT on the provision of goods and services is replaced by the Goods and Services Tax (GST). In order to track products and services, value added tax has been digitalized as goods and services tax. Indirect taxes like VAT and GST have the same tax rates. A complex, multi-layered, target-specific integrated system makes up GST [28].

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

All users pay GST through the trading system, which calculates the tax based on the total of the production and profit costs [29]. It shields you from a variety of unfavourable outcomes, such as bewilderment and change. To ensure the system's integrity and the integrity of the evidence, which is necessary for its admissibility in court, these and other instances must be avoided. All that the Chain of Custody is simply an ongoing record-keeping process [30].

3. Proposed work

Blockchain technology could be used to record these transactions in order to impose GST. Decentralized, transparent, interoperable, and extremely secure computing is made possible by blockchain technology. The PoA algorithm secures every transaction on the blockchain. In order to prevent unwanted data interception on the chain, the system is based on Shuffle Chain Link Proof Consensus-Based Elliptic Curve Cryptography (SCLPA-ECC). This technology has proven extremely valuable in government and other industrial applications since it provides excellent security and speed of operation at a low cost—safe and decentralized information sharing. Digital encryption and blockchain technology have become popular. Promoting blockchain requires the protection of user data and transaction information. The advancement of cryptographic technology restricts blockchain growth while enabling growth.

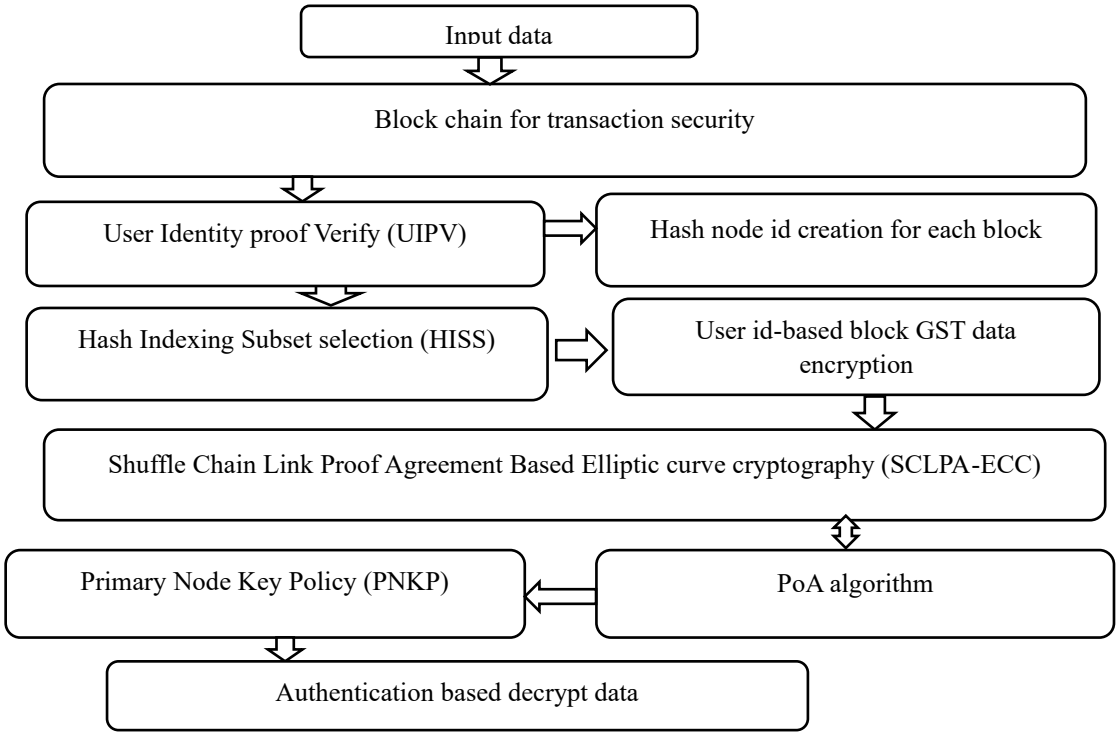

Figure 2 Proposed flow diagram

Figure 2 describes the, proposal involves integrating a Shuffle Chain Link Proof Agreement Based Elliptic curve cryptography (SCLPA-ECC) with master nodes for secure access using encryption. Initially we creating a blockchain phases for GST data transaction and first verifying the User Identity proof Verify (UIPV) Identification of user profiles and access points for transactions and authentication in User id-based block GST data encryption then the

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

centralized Hash Indexing Subset selection (HISS) Information in block phase using for primaty node key policy for PoA algorithm peer to peer authentication and encryption is provided by master node-based token entry validators.

3.1 Blockchain phase

Blockchain provides an advanced way to store GST information transactions, and establish trust in data sharing and data integration in a decentralized and open GST transaction network environment. Once the block is accessed and the necessary data extracted, the blockchain generation scenario is activated. Once access is granted to the user accesses the data and retrieves the required data. This method extracts user-accessible possessions from the data.

Input: GST Data (D), Feature Access (AF), Attributes Feature Count (FAC)

Output: Block Chain (BC), Data blocks (DB)

Begin

Read D, AFL, AT. // GST Data (D), Feature Access (AF), Attributes Feature Count (FAC)

$$Number\ of\ Features\ (Nf) = \int_{f=1}^{size(D)} \sum D(f) \in Af$$

For each feature (F) of fes

$$Select\ Block\ (Bs) = \int_{f=1}^{size(at)} Shuffle(f) == F, at(f).Block\ values)$$

Here, use the attribute AT to select the best encryption policy and key from the combination of technology and key. properties of the generated key scrambling information and encryption map. Likewise, this method takes the set Z*P and turns it into an odd number R. It establishes how many blocks should be made in the chain. The method splits the data into R blocks and builds a blockchain given a value of R. It performs dynamic block-level encryption and decryption using a blockchain and information blocks.

3.2 User Identity proof Verify (UIPV)

using identity systems with blockchain user-proof identity systems as well as the possible advantages of utilizing blockchain technology to create identity systems that are more effective. Blockchain-based User Identity Proof Verification (UIPV), digital identity verification, and registration authentication. Identity verification and User Identity Proof Verification (UIPV) can be carried out more quickly and securely while maintaining the identity holder's identity when compared to traditional identity systems. Blockchain-based identification solutions do away with middlemen and wait for authorization and authentication queues by utilizing the trust structure of the blockchain. Sequence recognition chains are made possible by the accumulation of evidence. Finding the block hash is easier than calculating a lot of hashes in order to build a chain with a high block generation rate.

$U = (x_1, y_1)$, be the efficient block point then $2u = P = (x_3, y_3)$, $v = (x1, y_1)$ be the matching point at 2x be pointed are round link of stack argument.

$$x_n = x^2 + \frac{a6}{{x_1}^2} + y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x$$

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

An interaction index Rn at each point of the additional set of data forms at a rotation point A+B in rotation point to hold the proof of each block to constant link. x = $(x1, y1)$ Then $y_2 = (x_3, y_3)$ then x + y = U = (x_3, y_3) p1, and p2 be the link point at proofing p3 in a, b hash blocks.

To maintain the resource of each block constant, the correlation index Rn of each point in the extra data set is produced at rotation point. x = $(x1, y1)$ and $y_2 = (x_3, y_3)$ then x + y = U = (x_3, y_3) Verify the hash of a and b connection point p3 on p1 and p2.

Verify user role agreements inside blocks of each advertising level using peer review, core principles, and source responses.

3.3 Hash node id creation for each block

Each Block CA selects $bk \in h_x^*$ at the chance and calculates $h_n = \alpha_k Q$. For each element $CK, x \in \check{a}_k$,

$xki \in S\_x\hat{} *$ To determine the secret cryptographic function, select any value between Ax and Ay.

Schedule the key exchange at random., then set $x\_ij \in S\_x\hat{} * q$ to distribute the selected value at random as the two-party key exchange's hash node id creation seed.

// A CA executes out the agreement to assign restrictions and rights to a resource.

If Task (ω, as, t) = true, then

$N\omega \leftarrow$ established number of establishments;

$T\omega \leftarrow$ the Threshold values;

End if

$$SRF = \left(\frac{x_k y_j}{x_j + u}\right)$$ The capability C_k - public keys as

$$PKk = yk,\ Tk, i\ i \in \{1,2,\ldots,nk\}$$

E and the private (secret) keys as $SKk = D\ \alpha k, xk,\ skj\ j \in \{1,2,\ldots,N\}\{k\}$,

$$tk, i\ i \in \{1,2,\ldots,nk\}\ E\ .$$

Therefore, skj = sjk is set. Cj and Ck select xi and xj, respectively, that ∈ Z ∗ q. A total of The two parameters of each attribute are nω and ω, an entry to regulate the feature. A data consumer must first obtain tω authorisation from the nω attribute authority in order to access attributes.

3.3.1 User id-based block GST data encryption

Numerous users in a blockchain ecosystem access cloud-based services and data. A wide range of data belonging to various users and clients can be found on the cloud. Unauthorized access to other data must be controlled by users. Access control based on hash identification can do this. To ensure that a user's access permissions meet all required attributes, you can use profile categorisation each time they request access to specific data. It is also used to evaluate how users act after being granted access to data. The hash code's value connects the keys.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Input: Data log (DL), request (r), and profile.

Output: Block Trust Values

Start

Block values to Read. // Data log (DL), request (r), and profile

Data Identify (DI) = (D.i.)

Provide the information.

Utilise the following formula to categorise Fl's noteworthy features: Fl = Pro on the feature list. Qualities

To find features that are available, use feature.

Feature List (FL) =

$$\int_{x=1}^{siz\,(p)} \int_{x=1}^{size(Fl\,)} Fl\ (\mathrm{y}) \in \mathrm{P(x).\,User} == \mathrm{Ur}$$

Compute Access Trust (AT) value

$$\frac{\sum_{x=1}^{size(T)} T(x).\mathrm{User==Ur}\ \&\&T(x).Access=complete}{\sum_{x=1}^{size(T)} T(x).\mathrm{User==Ur}}$$

Compute Hash idEvaluate using $\frac{Size(FL)}{Size(FL)} XAT$

$If\ Block\ id\ >\ Fl, then$

$Return\ true.$

$Else$

$Return\ false.$

End

Control access by using a hash identity metric calculated for a specific user request UIPV method restricts the access of the user based on the value.

Encryption

Block GST data = Encrypt (Fl, De. Key.)

Encrypted data (Ed) = combine Feature (F)

Random (Ra) =$\int random\_block\ \ value(5,7)$

Feature count (Dc) =$\int Sep(F)$

Initiate Blockchain using block id

Generate Dc (No. blocks (Nb))

$$Bc = \int_{x-0}^{size(DI)} \sum(blocks \in Bc) \cup generate\ blocks \qquad (3)$$

End

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This technique uses a distinct encryption algorithm and key for each attribute. The data is also divided into blocks, and the construction of a blockchain is determined by the number of blocks.

3.4 Hash Indexing Subset selection (HISS)

Every transaction on the blockchain is hashed before being included to the block. By storing hash values of data from previous blocks, a hash index connects each block to its predecessors. Since every block is connected to every other block, the information on the blockchain remains constant. An entity's unique hash value for a particular transaction is called a hash function, and it varies with each new block containing the hash code.

$$Hash_{i_d}(Index + Existing\ Hash\ value + Timestamp + Feature\ value + \text{not once}\ value) = Hash\ value \quad (7)$$

A valid hash is found using this value. determines the current value that, when combined with the block's other data, creates a valid hash.

The encryption key used in the hash code is identified by a token that users can obtain. The user can decrypt the ciphertext and retrieve the original message by changing the keys. Information is encrypted using a key set consisting of several keys in the suggested framework. Important choices are made by prime numbers and polynomial programming. Numerous distinct characters make up the character set used in this technique. Clients receive character sets and keys internally. Based on the size of the character set being used, the approach first produces random numbers.

Input: Random block set (Rbs), Keys(ks), data (d)

Output: Hashing code (Hc), Encode data txt (E.T.)

Begin

Identify Rbs ks, d

$$x1 = \int random\ value\ (1, size(Rcs))\ //add\ limit$$

$$Char\ (y) = Rcs\ (x1)$$

If y (prime)

Then

$$Generate\ Hash\ = y + Random\ (size\ (keyset)))$$

$$Encrypted\ data\ (Ed)\ = Encode\ (keyset\ (ASCII(y) - Random\ size\ (keys)) \quad (8)$$

End if

End

The resulting hash code and the encrypted data block are both appended to the target block. By examining the hash code, the user can ascertain the key that will be utilised to decrypt the text and recover the original content.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.5 Shuffle Chain Link Proof Agreement Based Elliptic curve cryptography (SCLPA-ECC)

Using randomly selected important threads a Elliptic Curve Cryptography encryption method based on the Random Chain Link Proof Protocol creates a hash code. It will take some time for the extra value to be offset by the message's cost.

The matrix is made up of rows from each period, and every new message needs a new periodic key that is part of the matrix. Start with the smallest giant in each row of data to replace it.

uses a collection of altered round key values to calculate an initialization key value.

$sk_{\propto}, sk_{\beta}, sk_{\rho}, h_{key}$ - end key

Check set of keys $sk_{\propto}, sk_{\beta}, sk_{\rho} \in \{0,1,3 \ldots . 3^{10} - 1\}$

Heuristic key $h_{key} \in \{0,1,2, \ldots . 2^{8n} - 1\}$

N→ Based on the number of changes in each block, the characters are sorted as parameters α, ρ, and β, which equal the block size key length h.

$sk_{\propto}, sk_{\beta}, sk_{\rho}, h_{key}$creates a hash value.

These numbers are used as parameters and multiplication factors for calculations requiring loops.

Index of Row $\propto = ax + s_{\propto} \times 10^{-2}$

Index of Column $\beta = y + (s_{\beta} \times 10^{-2})$

Index of Diagonal $\rho = cz + (s_{\rho} \times 10^{-2})$

For all calculates (S) ∈ {random,..,∞} Each block's chain value contains key+1 and an initial w_{if}

$w_{if} = [wi_1, wi_2, .. wi_i \ldots w_{iN^2-1}, wi_{N^2}]$

w_{if} - notation is as follows: each cell in each matrix block has a prime value w(i), and the sum of matrix columns begins with modulo representation.

For each value

$wf_i = (10^2 \times \sum x_{s+i} + y_{s+i} + z_{s+i}) \; mod \; 2^8 \qquad \forall_i = 1,2, \ldots \ldots N^2$

Computes the circular transformation of N index entries to rearrange field and array indices Wf into an N square matrix W.

$w_{if} = [wx_1, wx_2, .. wx_i \ldots w_{xN^2-1}, wx_{N^2}]$

$$Wfi = \begin{bmatrix} wx_1 & wx_2 & \ldots & wx_N \\ wx_{N+1} & wx_{N+2} & \ldots & wx_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ wx_{N^2-N+1} & wx_{N^2-N+2} & \ldots & wx_{N^2} \end{bmatrix}$$

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

random () Stores and replaces a key value that is shifted to an index of row or index of column by theorem. Use h_{key} - The complement of all sequential values of W in the top row of each block.

If the row matrix starts chain link with +1

$wx_{row(0)} = wx_{row(1)} \oplus h_{key}$

Continuity sequences for all link, $wx_{row(i)} = w_{xrow(i)} \oplus wx_{row(i-1)}$

$Wx(i) \longrightarrow \forall_i = 1,2,3, \dots N$

Chain link $S_1 = \sum_{j=1}^{N} w_{ij} x_j \ with\ extra\ bits\ a_{l+1} = \ a_l + m^2 \qquad \forall x = 1,2,3 \dots L$

Compute to create $M \ * \ M$ matrix with unique block as ϕ

$\phi = \{wx_1, wx_2, \dots wx_i, \dots wx_{L-1}, wx_L\}$

Compute the state array form between the supplied computed column and the hash code chain.

$$\overbrace{Im \rightarrow [wx_1] \rightarrow [wx_2] \rightarrow \cdots \rightarrow [wx_L]}^{encry\ code \longrightarrow a\ time}$$

For shuffle stack

$$Is = \begin{bmatrix} \rightarrow 4 & \downarrow 3 & \downarrow 1 \\ \uparrow 7 & \downarrow 5 & \downarrow 6 \\ \uparrow 8 & \leftarrow 6 & \leftarrow 7 \end{bmatrix}$$

Code containing keys to generate the correct matrix

$$\overline{Is} = \begin{bmatrix} 5 \rightarrow & 6 \rightarrow & 8 \rightarrow \\ 7 \rightarrow & 8 \rightarrow & 5 \rightarrow \\ 1 \rightarrow & 2 \rightarrow & 5 \rightarrow \end{bmatrix}$$

Each block chain link key CT→chain link key CT (Pki)

Block is Return Ct (Pk)

End if

End for.

When characters are being transferred back and forth on stage, the most costly approach is to transmit the exact demand for the same least significant bit (LSB) shift. This is because long strings in conventional printing cause keyboard blocks and loops. This includes all solutions (a,b) and the infinite point O. The security of the elliptic curve encryption method depends on how difficult it is to solve the elliptic curve. Assume that G and Q are two of the points of a curve E. where x is the elliptic curve's single logistic issue.

$$b^2 + ab + by = a^3 + ca^2 + da + e$$

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

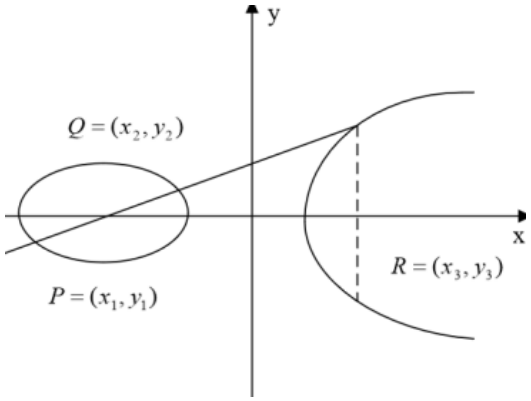

Figure 3Elliptic curve cryptography

Let the base fields F, a, yb belong to F and satisfy the following

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

$$E: y^2 = x^3 + ax + b$$

$$x^3 = \Delta^2 - x_1 - x_2$$

$$y^3 = -x_1 + \Delta(x_1 - x_2)$$

A symmetric encryption technique is used to encrypt the data, and a shuffle encryption algorithm is used to encrypt the symmetric key in order to ensure the confidentiality of the particular data source on the blockchain in figure 3.

3.6 PoA Algorithm

The consensus method called Proof of Authority (PoA) is used in permissioned networks, where a select few reliable authorities are selected as transaction validators based on their reputation and identification. In contrast to other systems, PoA increases transaction and energy efficiency by relying on a small number of validators to obtain consensus rather than requiring a lot of processing. This approach, however, forgoes decentralization and could place control on public networks.

To generate blocks, the organization uses a mining rotation mechanism. This is predicated on the idea that at least N/2+1 trusted nodes exist if there are N authorities. Both approved and illegitimate networks can use the PoA algorithm. The authors show, however, that PoA is inappropriate because permissioned blockchains are inconsistent. Enhance the performance of the network. However, only specific applications can employ PoA due to the use of a central authority.

By modifying the PoS solution, PoA is seen as a hybrid of Proof of Stake (PoS) and Proof of Work (PoW). The majority of the nodes in each node will mine the block if a miner wishes to transmit some transactions in that block to mine a new block before submitting that generated block to the repository. As indicated in the figure 4, sign the verification.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

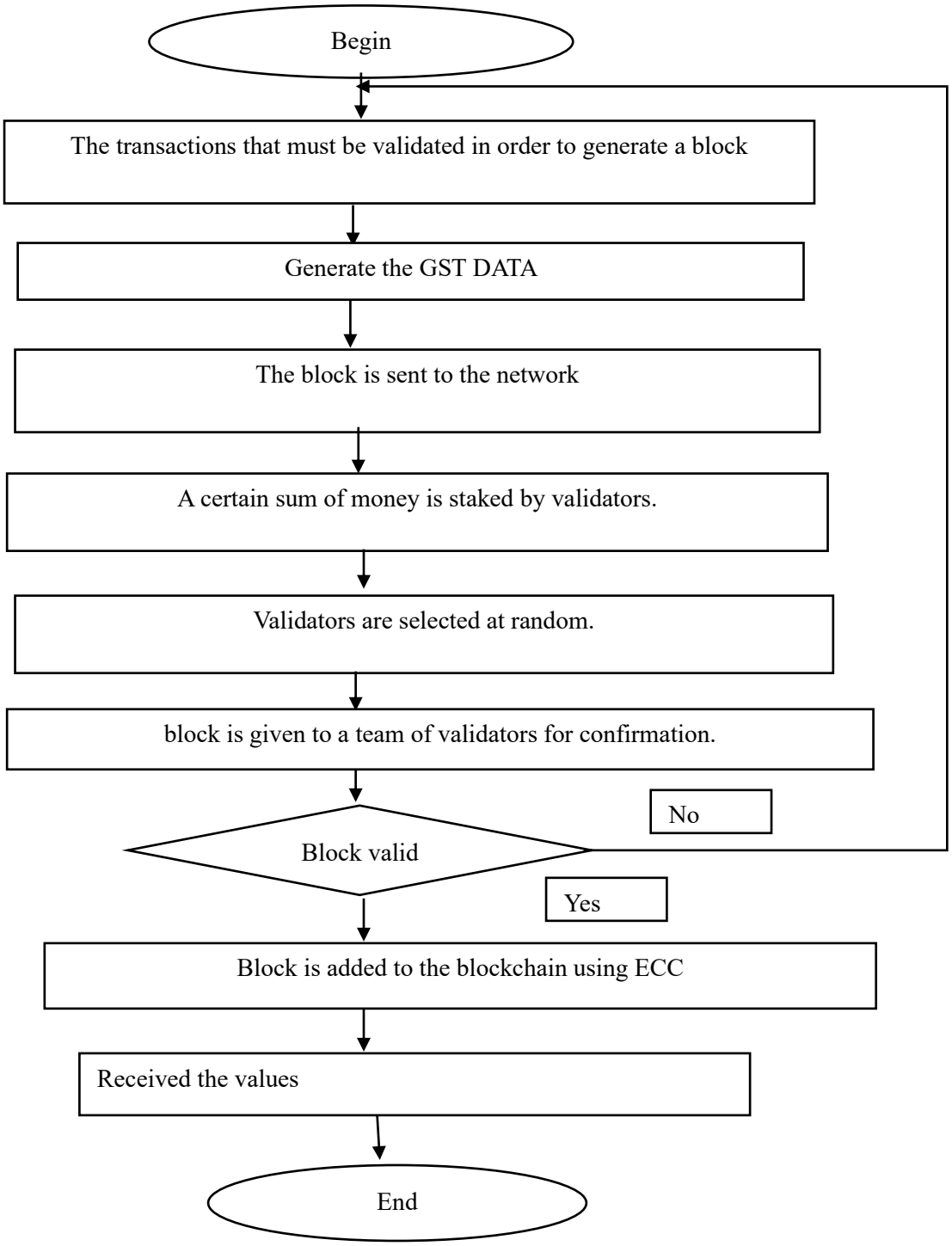

Figure 4 PoA algorithm flow chart

3.7 Peer to peer end security

In code times, peer-to-peer authentication takes more preparation to set up authentication between nodes than in a standard server-based client/server setting because nodes communicate directly with one another. For token sessions conversed peer authentication makes use of central authority solutions and central authority-based authentication methods. Secure information sharing between parties is possible with blockchain technology.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Steps: Peer verification

Input: Accessing time for Data Transfer (DT)

Output: Peer completion received data

Start peer verification

Compute the two blocks created in peer completion (X) and user id (UI).

For all the block identity block

Find the closest peer to the target companion when sending

If closest Peer = target peer?

Peer Validation Based Code Limitation

Else if

Closest peer = Last contact peer?

No peers to get close peers

Else if

Closest peer and ask for closest peer to target

Else

Avoid using encryption designed for data transport (BLenc)→ur

Receiving data (D)

Return the block on data access

End if

End for

End peer verification

In this case, a peer-to-peer request for a primary address culminates in the necessary participant verification, and an anonymous sending address is obtained using this shared secret. Only if are in charge of creating these addresses may it promote them.

4.Implementation

A number of parties are involved in the whole tax process. Given the inherent mistrust between various authority regions, blockchain technology could be used to influence the current tax system. Nonetheless, they wish to conduct trades on a single platform. These parties are all reliant on the state. Take, for instance, a pair of shoes. Every participant pays taxes levied by the federal and state governments from the point of production to the point of sale. The main concern is that everyone must have faith that the quantity will be promptly returned to each individual amount variations made at intermediate stages of production. Businesses that submit GST refund forms and are eligible to get a return after making tax adjustments. The tax officer's responsibility is to compute all of these and make the necessary modifications.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This collection of code, which is automatically carried out by checks, makes up a smart contract. It establishes who pays for what, at what stage of production, who uses the service last, and who utilizes the service. middle-class or good consumers. By writing a particular set of codes in accordance with the guidelines established by the GST Act, smart contracts can be created to regulate the entire chain. All of the adjustments can be made automatically using this smart contract.

This smart contract will recognize to purchase particular raw materials and utilize them to produce shoes, compute taxes appropriately, and automatically adjust the additional price paid for the raw materials. Government account receives a direct deposit of the remaining sum, which is the actual taxable amount. It completes the entire process in real time and streamlines it.

4.1 Result and discussion

The suggested investigation findings, which were conducted using the Visual Studio tool and the C#.net language, are shown in this part. When compared to the Policy Agreement Random Contract Approach (RCA), Markov Chain Monte Carlo (MCMC), and Hashed Time Lock Contract (HTLC) approaches, the suggested algorithm, Shuffle Chain Link Proof Agreement Based Elliptic curve cryptography (SCLPA-ECC), is superior.

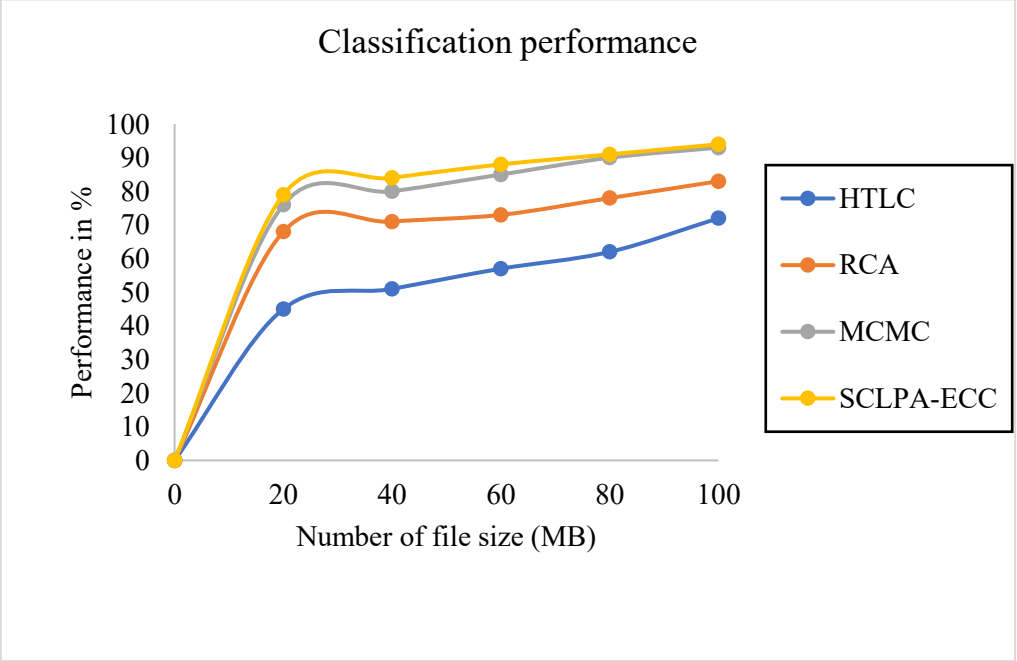

Figure 5Impact of Classification Performance

The performance of classification for GST records with varying file sizes is explained in the figure 5. For 100 MB files, the classification performance of the suggested technique is 94%. In a similar vein, the outcomes of the current approaches are GST Data security performance.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

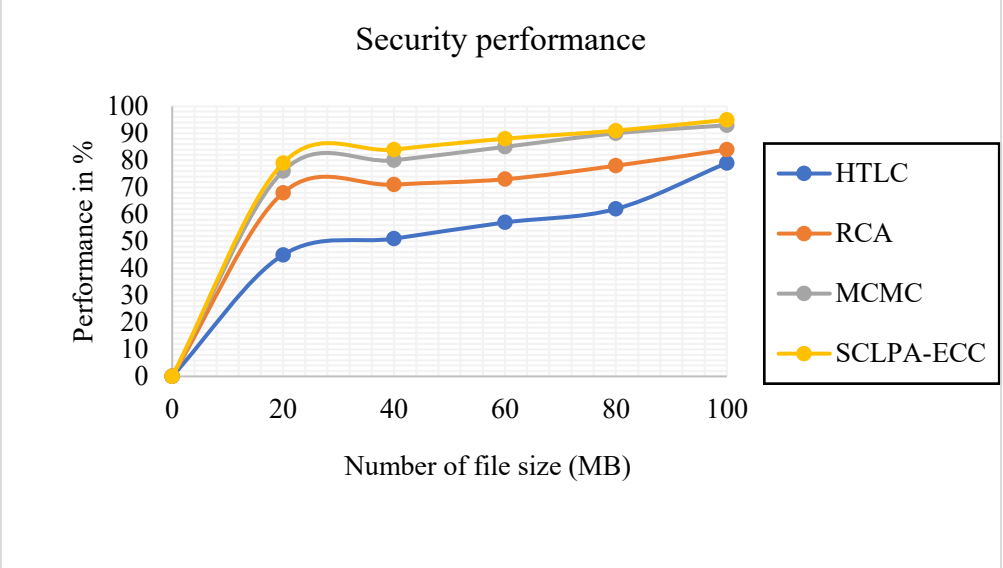

Figure 6 Impact Of Security Performance

The security performance for safe data sharing of GSTrecords in a cloud environment is explained in the figure 6. For 100MB files, the suggested method's security performance is 95%. Likewise, the outcomes of the current approaches are GST Construction of Key Agreement Protocol (CKAP) security performance is 84%, while data security performance is 79%.

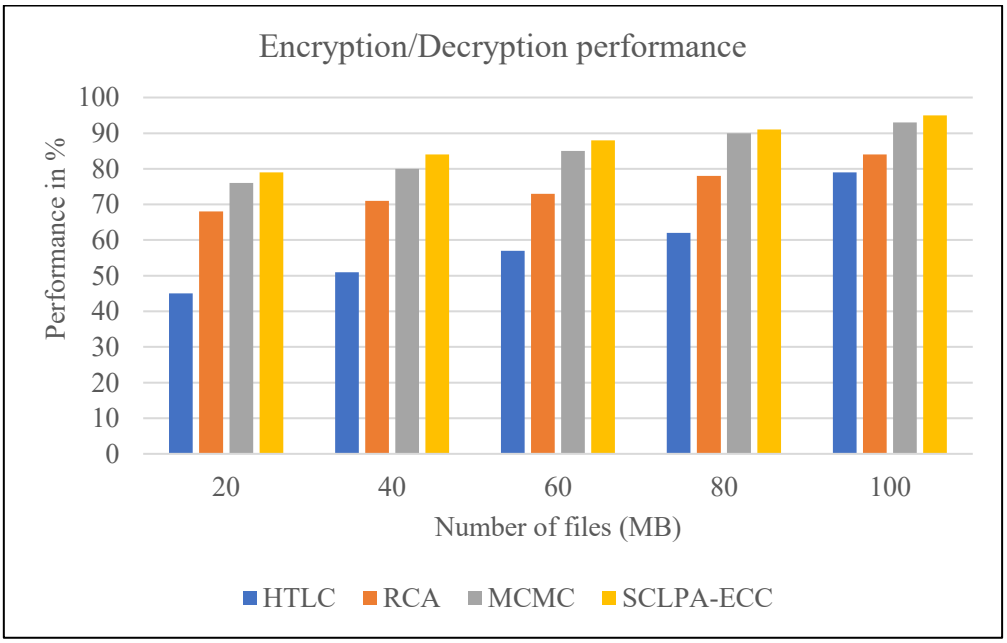

Figure 7 Encryption and decryption Performance

The encryption and decryption performance for safe cloud data sharing of GST records is explained in the figure 7. For 100MB files, the suggested method's performance is 95%. Additionally, the outcomes of the current approaches are GST Performance of data

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

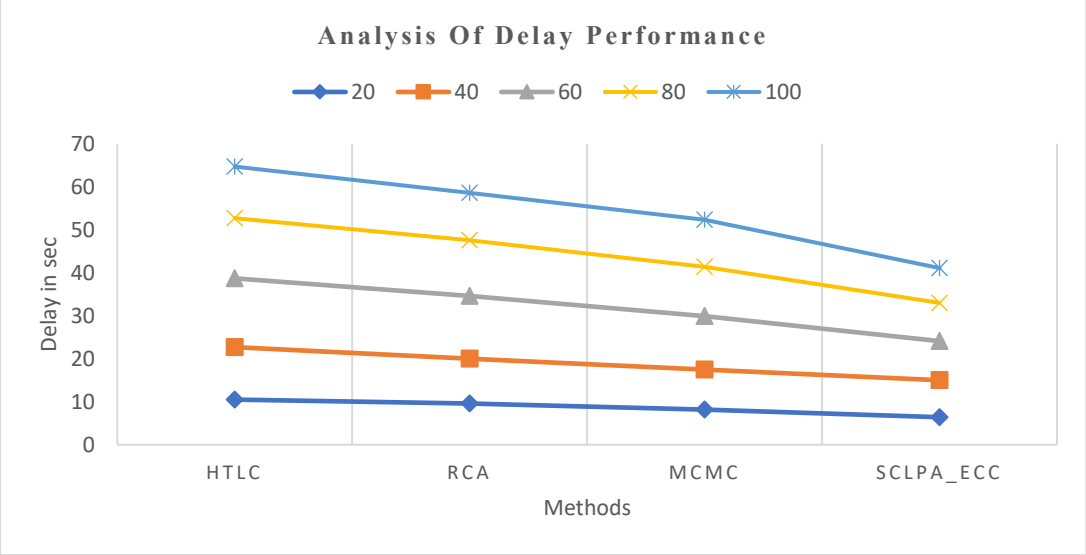

Figure 8: Analysis of delay performance

Figure 8 displays the results of the analysis of the delay performance comparison. The proposed SCLPA-ECC method takes 8.1 seconds for a 100 MB file size. In contrast, the RCA method takes 12.4 seconds, the HTLC approach takes 14.6 seconds, and the MCMC algorithm takes 16 seconds for a 100 MB file size.

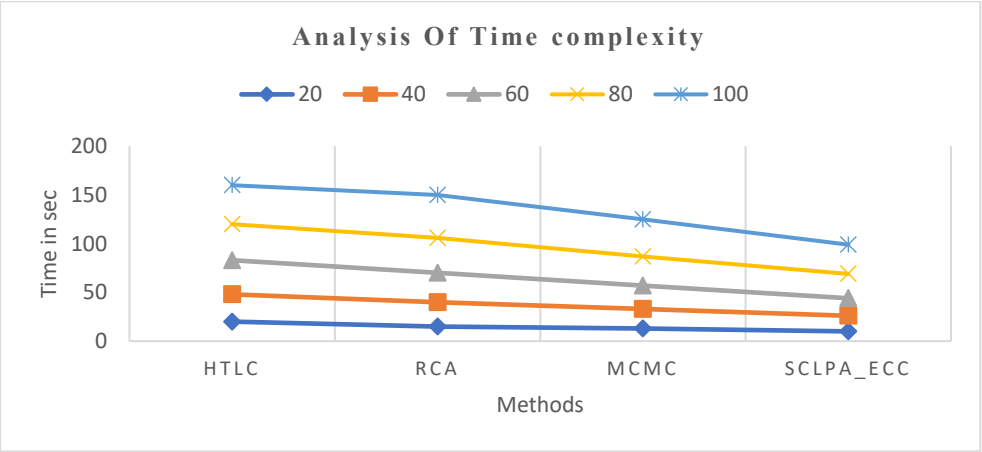

Figure 9: Analysis of Time complexity

The time complexity analysis in comparison results based on Big O notation time complexity analysis is defined in Figure 9. The suggested SCLPA-ECC technique takes 30 seconds for files up to 100 MB in size. Likewise, the 40-second RCA algorithm was the prior algorithm.

5. Conclusion

In a centralized GST system, the vast volume of transactions that occur every day is too much for the GST module to manage. The GST system's strong foundation is the reason for its success. The current system is plagued by numerous conflicts connected to IT. It is challenging for all parties involved, especially the government, to handle massive amounts of big data with various industry characteristics, transactions, and GST refund.

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Blockchain is an innovative form of database that is formed in an encrypted digital ledger and stores all past data in digital blocks. Attacking distributed ledgers is difficult by nature. Ensure total openness and a thorough audit trail across the chain. This allows for real-time evaluation of transactions and their chain of origin in addition to precise tracking and prompt decision-making about refunds and other compliances.

Blockchain's privacy and security features are crucial for enhancing its dependability and encouraging cutting-edge research and development. Evidence Based on Shuffle Chain Link Consensus Elliptic Curve Cryptography (SCLPA-ECC) is a suggested solution for privacy and security systems that will be crucial to the advancement of blockchain technology and its uses in the future. The suggested Random Link Proof Consensus (SCLPA-ECC), which is based on Elliptic Curve Encryption, has 97% security performance, 26 and 31 millisecond encryption and decryption operation times, 97% access control performance, and 9.1 second latency analysis performance.

Reference

1. W. Jie et al., "A Secure and Flexible Blockchain-Based Offline Payment Protocol," in IEEE Transactions on Computers, vol. 73, no. 2, pp. 408-421, Feb. 2024, doi: 10.1109/TC.2023.3331823.
2. S. Ma, S. Wang and W. -T. Tsai, "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus," in IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1825-1829, Sept. 2022, doi: 10.1109/LWC.2022.3183197.
3. M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
4. S. Peng et al., "An Efficient Double-Layer Blockchain Method for Vaccine Production Supervision," in IEEE Transactions on NanoBioscience, vol. 19, no. 3, pp. 579-587, July 2020, doi: 10.1109/TNB.2020.2999637.
5. A. Alhussayen, K. Jambi, M. Khemakhem and F. E. Eassa, "A Blockchain Oracle Interoperability Technique for Permissioned Blockchain," in IEEE Access, vol. 12, pp. 68130-68148, 2024, doi: 10.1109/ACCESS.2024.3400672.
6. S. N. G. Gourisetti, M. Mylrea and H. Patangia, "Evaluation and Demonstration of Blockchain Applicability Framework," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1142-1156, Nov. 2020, doi: 10.1109/TEM.2019.2928280.
7. B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi and A. Mezrioui, "Drawing the Boundaries Between Blockchain and Blockchain-Like Systems: A Comprehensive Survey on Distributed Ledger Technologies," in Proceedings of the IEEE, vol. 112, no. 3, pp. 247-299, March 2024, doi: 10.1109/JPROC.2024.3386257
8. P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3562-3574, Dec. 2022, doi: 10.1109/JSAC.2022.3213326.

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9. N. Afraz, F. Wilhelmi, H. Ahmadi and M. Ruffini, "Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis," in IEEE Access, vol. 11, pp. 95653-95666, 2023, doi: 10.1109/ACCESS.2023.3309423.
10. M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.
11. M. Muneeb, Z. Raza, I. U. Haq and O. Shafiq, "SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management," in IEEE Access, vol. 10, pp. 23687-23699, 2022, doi: 10.1109/ACCESS.2021.3135562.
12. Saini, D. Wijaya, N. Kaur, Y. Xiang and L. Gao, "LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare," in IEEE Internet of Things Journal, vol. 9, no. 15, pp. 14005-14017, 1 Aug.1, 2022, doi: 10.1109/JIOT.2022.3145406.
13. E. Chen, S. Wang, Y. Fan, Y. Zhu and S. S. Yau, "SaaSC: Toward Pay-as-You-Go Mode for Software Service Transactions Based on Blockchain's Smart Legal Contracts," in IEEE Transactions on Services Computing, vol. 16, no. 5, pp. 3665-3681, Sept.-Oct. 2023, doi: 10.1109/TSC.2023.3267489.
14. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
15. Y. Zhu, W. Song, D. Wang, D. Ma and W. C. -C. Chu, "TA-SPESC: Toward Asset-Driven Smart Contract Language Supporting Ownership Transaction and Rule-Based Generation on Blockchain," in IEEE Transactions on Reliability, vol. 70, no. 3, pp. 1255-1270, Sept. 2021, doi: 10.1109/TR.2021.3054617.
16. Y. Fang, Z. Zhou, S. Dai, J. Yang, H. Zhang and Y. Lu, "PaVM: A Parallel Virtual Machine for Smart Contract Execution and Validation," in IEEE Transactions on Parallel and Distributed Systems, vol. 35, no. 1, pp. 186-202, Jan. 2024, doi: 10.1109/TPDS.2023.3334208.
17. Y. Pang, D. Wang, X. Wang, J. Li and M. Zhang, "Blockchain-Based Reliable Traceability System for Telecom Big Data Transactions," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12799-12812, 15 July15, 2022, doi: 10.1109/JIOT.2021.3138462
18. Y. Jiang, Y. Zhong and X. Ge, "Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things," in IEEE Access, vol. 7, pp. 180856-180866, 2019, doi: 10.1109/ACCESS.2019.2959771.
19. P. G. Hunn, "Smart Contracts as Techno-Legal Regulation," in Journal of ICT Standardization, vol. 7, no. 3, pp. 269-286, 2019, doi: 10.13052/jicts2245-800X.735.
20. J. Li, T. Liu, D. Niyato, J. Li and Z. Han, "On Sidechain-Assisted Transaction Service Management for Internet of Things: A Random Contract Approach," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 5, pp. 3437-3453, 1 Sept.-Oct. 2022, doi: 10.1109/TNSE.2022.3181114
21. H. Su, B. Guo, Y. Shen and X. Suo, "Embedding Smart Contract in Blockchain Transactions to Improve Flexibility for the IoT," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 19073-19085, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3163582.

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

22. S. Khan, M. B. Amin, A. T. Azar and S. Aslam, "Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability," in IEEE Access, vol. 9, pp. 116672-116691, 2021, doi: 10.1109/ACCESS.2021.3106384.
23. W. Xiong and L. Xiong, "Data Trading Certification Based on Consortium Blockchain and Smart Contracts," in IEEE Access, vol. 9, pp. 3482-3496, 2021, doi: 10.1109/ACCESS.2020.3047398.
24. E. Chen et al., "SPESC-Translator: Towards Automatically Smart Legal Contract Conversion for Blockchain-Based Auction Services," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 3061-3076, 1 Sept.-Oct. 2022, doi: 10.1109/TSC.2021.3077291
25. C. Wu, J. Xiong, H. Xiong, Y. Zhao and W. Yi, "A Review on Recent Progress of Smart Contract in Blockchain," in IEEE Access, vol. 10, pp. 50839-50863, 2022, doi: 10.1109/ACCESS.2022.3174052.
26. Pinna, S. Ibba, G. Baralla, R. Tonelli and M. Marchesi, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," in IEEE Access, vol. 7, pp. 78194-78213, 2019, doi: 10.1109/ACCESS.2019.2921936.
27. V. Capocasale and G. Perboli, "Standardizing Smart Contracts," in IEEE Access, vol. 10, pp. 91203-91212, 2022, doi: 10.1109/ACCESS.2022.3202550.
28. B., G. ., & Priya V. , V. (2024). Improving the Security and Speed of GST Tracking by Use of Artificial Intelligence's Blockchain Real Time Technology . International Journal of Intelligent Systems and Applications in Engineering, 12(15s), 294–298. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4748
29. Rishab Ranka, Niranjan Sharma, Naman Talati and Nikita Rai, 'An Efficient System for Implementation of Goods and Service Tax in India using Blockchain', International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, 2021.
30. Dr. S. Harihara Gopalan, S. Akila Suba et al., Digital Forensics Using Blockchain, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019.

Received: August 10, 2025