The Scientific Temper (2025) Vol. 16 (10): 4879-4891

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.10.06

https://scientifictemper.com/

RESEARCH ARTICLE

Enhanced Block Chain Financial Transaction Security Using Chain Link Smart Agreement based Secure Elliptic Curve Cryptography

S. Mohamed Iliyas[1*], M. Mohamed Surputheen[2], A.R. Mohamed Shanavas[3]

Abstract

Blockchain technology to offer transparency and Security within financial management in the banking industry. By building a financial data information collection, information exchange, and information security information Agreement mechanism to improve the efficiency of the existing financial control system, a more effective financial control mechanism can therefore be introduced, and through it, significantly drive down the cost of financial data, the audit cycle, and enhance the Security of information. The current problems of data security, inefficiency of low information, accelerated transactions, and the cost and exchange rate of information under traditional financial control systems, which are supposed to guarantee data integrity. The proposed method, Chain Link Smart Agreement based on Secure Elliptic Curve Cryptography (CLSA-SEC^2), aims to generate a secure authentication key for data encryption and decryption. The initial step is Primary Key Node Generation (PKNG) for User Identity Verification, which transfers secure financial data into blocks.A decentralized blockchain divides each block of data into blocks stored at different locations. In chain-link aggregation to produce a unique key to each block series sequence, to ensure the process of communication and Transaction is secure under a decentralized block chain. And it validates the user transaction based on the Access Block Sequence Rate (ABSR) in data access. Build blocks are controlled by a key that is verified from the controller node. A Sequential Searchable Attribute Key (S^{2}AK) is used to simplify the calculation of the user authentication phase's cost. Lastly, its security analysis demonstrates that a decentralized block chain network will render the traditional system of centralised audit systems obsolete, providing digitally sealed and verified results of certification and enhancing financial transparency and Security.

Keywords: Decentralised, Blockchain, Security, Elliptic Curve Cryptography, Information, Financial Data, Authentication.

[1]Research Scholar, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

[2]Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

[3]Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

***Corresponding Author:** S. Mohamed Iliyas, Research Scholar, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India, E-Mail: iliyasjmc@gmail.com

How to cite this article: Iliyas, S.M., Surputheen, M.M., Shanavas, A.R.M. (2025). Enhanced Block Chain Financial Transaction Security Using Chain Link Smart Agreement based Secure Elliptic Curve Cryptography. The Scientific Temper, **16**(10): 4879-4891.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.10.06

Source of support: Nil

Conflict of interest: None.

Introduction

International financial activities also enable businesses worldwide to conduct their financial transactions by establishing connections among them. The existing solutions for international money transfers imply a poor quality of performance, high costs, and a low level of Security. Facilitating transactions through banks and clearinghouses as intermediaries also reduces operational speed, as more parties are involved in the process, creating added exposure to fraud and the threat of cybercrime. Businesses that fail to track their data flow cannot be trusted by their partners and must operate within tighter rules. Blockchain technology is one possible solution, as it operates on a decentralised database that cannot be modified (Zhou, 2025). Transactions based on these approaches no longer require third-party facilitation, since the involved parties have trust in a common data source for all transactions. With financial trends, the blockchain technology is increasingly contributing to the sector in terms of its applicability. Digital currency (DC) and smart contracts are applications that are

Received: 14/09/2025 **Accepted:** 06/10/2025 **Published:** 16/10/2025

well supported by blockchain technology because of the features of decentralisation and immutability of information.

A decentralised technology known as blockchain allows us to record information transparently and securely, without the input of a central authority. To put it simply, a blockchain is composed of multiple data blocks that have been generated by transactions verified by a network of users. A chain is produced that cannot be altered by cryptographically connecting each block to the one before it. Security: The design of the reach agreement, which requires the consent of every network user to validate a transaction before it can be included in the block, contributes to the technology's Security. This reduces the likelihood of fraud and data manipulation, which typically occur in centralised systems where anybody can alter or manipulate data.

Counter the drawback of Smart Agreement in the limitation of Access to on-chain data. While smart Agreements do currently retrieve on-chain information with the help of an oracle that can be hacked to tamper with customers (Li, 2023), it is also possible to use off-chain data as well, such as the ScaleBOT system, which uses the services of Google to determine a location in terms of longitude and latitude (Chishti, Sufyan, and Banerjee, 2022). Decentralisation is one of the primary benefits offered by the blockchain technology, implying that there is no single organisation that owns and controls the entire system. As the system depends on a system of computers (nodes) to authenticate and record transactions, thesystem has to be affirmed by most of the nodes that are on the network to validate any updates or alterations to the blockchain (Islam and Apu, 2024). Blockchain technology has significantly improved Security and transparency, two issues that have been problematic in the banking industry. Every Transaction may be explicitly logged on a blockchain, and once registered, it is immutable, boosting consumer and bank trust. Additionally, operational costs can be minimised, including transaction fees and the duration of the verification procedure and transaction completion (Al-Jaroodi and Mohamed, 2019), thanks to the use of blockchain.

The potential mechanism of direct access to blockchain data through smart agreements is the indexing of the parameters of a transaction in each block using the Chain Link Smart Agreement-based secure elliptic curve cryptography (CLSA-SEC^2). The goal is to enhance financial applications through blockchain-based data transparency. This is to make the blockchain applications more transparent in terms of data. Maintains the Sequential Searchable Attribute Key (S2AK) that can access transactions in (B) satisfying specific criteria in O (B). The difficulty is further reduced to O(B/k) by fragmenting the blockchain information into k distinct sets, allowing for parallelisation of the search protocol.

It applies an Improved Chain Link Smart Agreement -verified Secure Elliptic Curve Cryptography (CLSA-SEC^2) blockchain specifications in remotely distributed Banking systems. The given proposal employs the S^{2}AK blockchain technology to ensure the financial privacy of the parties and the immutability of data. This work is the assistance of:

- First, Blockchain technology aggregation with structure proposes a Sequential Searchable Attribute Key (S^{2}AK) predicates in Financial data transaction systems, where the number of Access Block Sequence Rate (ABSR) increases with the number of authorised Access.
- Second, a significant problem for many officers is collaborating in attacks. As a way of mitigating this risk, the two organisations share random functional seeds and keep them confidential. Key Generation uploading each company's own Key (secret Key) into the financial Transaction (public) Key
- Lastly, using the computational assumption, the schemes will be proven to be secure against selective prediction in a randomised oracle model and provide perfect privacy to the participants without involving any financial leakage. This demonstrates the higher performance of this scheme.

Related work

In blockchain-based application scenarios, where blockchain consumption patterns are involved, the logic of an application is composed of a series of continuous transactions, and the start of one of them is delayed until the response from the previous one. This requires that continuous transactions be handled in a proper sequence. Blockchain-based not particularly efficient at continuous transaction processing, as it is expected that the process of confirming continuous transactions takes considerable time (Ni, Xiao, Zhang, Li, Li, and Jin, 2023). An electronic application is also integrated to eliminate a third-party intermediary and supports transactive communications (Okoye and Kim, 2022).

Blockchain limitations in terms of scalability, resulting in reduced throughput and increased delay time. However, sharding faces obstacles concerning the elevated cross-shard transaction fraction as well as the difficulty of cross-shard transactions. Thus, an account-weighted graph transaction sharding algorithm is designed (Li and Ning, 2024). The case is dire for standalone distributed generators (SDGs), which do not provide Access to the utility grid in terms of transactions (Okoye, Yang, Cui, Hussain, Bui, and Espin-Sarzosa, 2024).

Unbalanced dividing of the Transaction (TX) workloads among all blockchain shards because of the deployment strategy of their accounts. Unbalanced transaction distributions will result in hot shards, where cross-shard Transactions can have an unbounded confirmation latency (Sarwar, Khan, Maghrabi, Jaffar, and Akram, 2024). Nonetheless, there are a few drawbacks linked to sharding, including optimising where to place transactions in the shards so that they reduce cross-shard interactions,

Table 1: Survey for financial Transactions in blockchain technology

Authors name	*Year*	*Proposed techniques*	*Limitation*	*Parameters*
Z. Li et al	2024	Trusted Data Synchronisation System (Saba, Haseeb, Rehman, and Jeon, 2024)	Low Security and high cost	Delay, Time complexity
T. Saba et al	2024	Tunicate Swarm Algorithm-Based Optimised Routing Mechanism (TORM) And Routechain	Low data storage and low cost (Tunzina et al., 2024)	Network Throughput, Computing Overhead, Data Delay, Response Time.
T. Tunzina et al	2024	Proof-of-Work (PoW)	Low transparency and efficiency	Security, Encryption and Decryption (Islam and In, 2023)
M. M. Islam et al	2023	Privacy-Preserving, Transparent Unspent Transaction Output (UTXO) Model (Koo, Park, and Yoon, 2024)	privacy, transparency, and auditability	Verification time and Transaction throughput
K. Koo, et al	2024	Suspicious Transactions Based On The Risk-Based Approach	Complex Transaction (Nguyen-Hoang et al., 2024)	Anomaly detection, Error rate and ROC
T. -A. Nguyen-Hoang et al.,	2024	Identity Zero-Knowledge Proof (IZKP)	inefficiencies, lack of transparency (Wu, Lin, Lin, Zheng, Huang, and Zheng, 2023)	Accuracy, Precision
J. Wu et al	2023	Temporal Attribute Heterogeneous Modalities	Lack of industry standards and regulatory rules	Security and time complexity (Fetaji, Fetaji, Hasan, Rexhepi, and Armenski, 2025)
B. Fetaji et al	2025	AI-XGBoost	Lacks of Security	Precision, recall and F1 score (Zhang, 2025).
T. Zhang et al	2025	Trusted Multimedia Scheme With RedactableBlockchain (TMRB)	Fake News, Misleading Multimedia Content, Content Security, And Copyright Management.	Time complexity, Security and key Generation (Singh, Dwivedi, Srivastava, Chatterjee, and Lin, 2023).
R. Singh et al	2023	Efficient Zero-Knowledge Blockchain (EZKB)	Low privacy and Security	Transaction and delay (Li, Liu, Ma, Yang, and Sun, 2023)
R. Li, et al	2023	Graph-learning algorithm TA-Struc2Vec	Difficult to use for financial fraud detection	Precision, F1-score, and AUC (Jahan Sarna et al., 2025)
N. Jahan Sarna et al.,	2025	Graph Neural Networks (GNNs)	Increased the complexity of financial networks	Accuracy, Computational cost and time (Chatterjee, Das, and Rawat, 2024)
P. Chatterjee et al	2024	Federated Learning-Empowered Recommendation Model (FLRM)	Privacy and Security	Data transaction, delay and Security (Baliker, Baza, Alourani, Alshehri, Alshahrani, and Choo, 2024)
C. Baliker et al	2024	Blockchain-based FinTech	Privacy and Security	Transaction and Time complexity (Zhang, Jia, and Chen, 2025)
T. Zhang, et al	2025	Conceptual Framework	Loss of time and productivity	Delay, Transaction and Throughput (Chen, Wang, Fan, Zhu, and Yau, 2023).
E. Chen et al	2023	SLC-based SPESC Agreement (Ren et al., 2024)	Need not only to realise financial payment	Data delivery and Time complexity
Q. Ren et al.,	2024	MPT-enabled off-chain Agreement execution framework	Data availability, financial fairness, delivery fairness, and delivery atomicity.	Throughput, Cost evaluation and delay (Ogeti, Narendra, Patil, Padyana, Rai, and Patil, 2022).

balancing the workload as the number of shards exceeds their capacity, and identifying shards that run transactions maliciously (Amankona Obiri, Gao, Xia, Xia, and Nii Aflah Cobblah, 2025).

Blockchain transaction privacy has widely been explored in an array of application contexts. Nevertheless, such schemes face burdens, such as computing inefficiency, data growth, and insufficient metadata privacy, e.g., timestamp

protection [12]. All of the above, especially the absence of underlying accounting principles in the third entry, as well as compliance and other concerns, have cast doubts over Triple-Entry Accounting (TEA) and resulted in limited practical application to date (Li, Liang, Wen, and Wan, 2024).

Blockchain refers to a digital Transaction log consisting of a set of blocks, eliminating the need for intermediaries and reducing the risk of fraud. The financial sector, where concerns such as trust, high transaction costs, and time consumption in processing have been a headache, has greatly benefited from the use of blockchain (Shoetan and Familoni, 2024). The central findings conclude that blockchain technology is capable of considerably enhancing financial and operational stability by providing a strong infrastructure for transparent, immutable transactions and supply chain management (Singh and S. G., 2023).

The connection between the most significant elements of the networks should be displayed in order to support the understanding of the complex issue between blockchain technologies and AI tools and their role in the enhancement of the Security of financial networks (Tse, Dai, Lee, and Lu, 2024). Blockchains revisited which looks at the wants in consumers, why they want to use financial apps that make use of blockchain technology. Designed the model and identified a set of independent items of perceived privacy, awareness of technology, and confidentiality of information. Also found out that whereas privacy did not affect the users in any discernible way, information security and technology awareness did play a profound effect on the users in terms of their acceptance (Ichsani, Deyani, and Bahaweres, 2019). An indicator of which leader block to use is selected by the Dynamic Butterfly-Billiards Optimisation Algorithm (DB-BOA).

A consensus mechanism is applied to Adaptive Deep Temporal Context Networks (ADTCN), which uses the chosen new leader block to conduct smart agreements in a secure context. In this case, the settings are optimised in DB-BOA. After comparing the developed ADTCN-based financial security system with some other traditional approaches, the algorithms have demonstrated promise (Prabanand and Thanabal, 2025).

Limitations

The previous financial protection model suffers from transparency problems. Besides being insecure due to the use of third-party services, data manipulation is challenging, and there is also the issue of spoofing. Its implementation is poor. It checks fraud transactions efficiently. Nevertheless, it is not easy to cope with such active calculations, which can cheapen the quality of the service. This has enhanced the Security of blockchain transactions and yielded good results. This, however, does not enable flexible authentication, resulting in a complex configuration that compromises the privacy of data owners.This improves the performance and the latency of the model, however the cost of implementing it is too expensive and its performance is too low. Provides Very-high-integrity end-to-end measurements. It is also more secure, traceable and unalterable with data. However, it is incapable of offering sound and safe financial protection, storage, and has issues managing privacy.

Proposed Methodology

This section includes a Banking transaction system model and a detailed Chain Link Smart Agreement-based Secure Elliptic Curve Cryptography (CLSA-SEC^2) framework. The proposal is a Sequential Searchable Attribute Key (S^{2}AK) that can be applied to Financial data transmission using blockchain technology.

In the decentralised blockchain network, as shown in Figure 1, the data owner will be the first to create the primary node key, which is used for user identity verification to authenticate every block in various locations. Then, Access Block Sequence Rate (ABSR) will be verified in sequencing the data to accessing block and using Sequential Searchable Attribute Key (S^{2}AK) the data will be searched with a key in each block access and the last is CLSA-SEC^2 the Generation of encryption and decryption key chain-link aggregation to obtain a distinctive key on each block of series sequence, to ensure the communication and transaction process is secured under a decentralized block chain.

Primary Key Node Generation (PKNG)

The main node key-generation plan is to generate a public property key at each quality and send it to the blockchain. My preferred method of generating primary key values is the *GenerationType.SEQUENCE* , which uses a database sequence to generate unique values. The Key holding the Primary node transmits the data to validate it via the Primary node validation session, and policies are used to control the integrity of the service.

Node Identity Initialization

Each node n_x is uniquely initialized using an attributes:

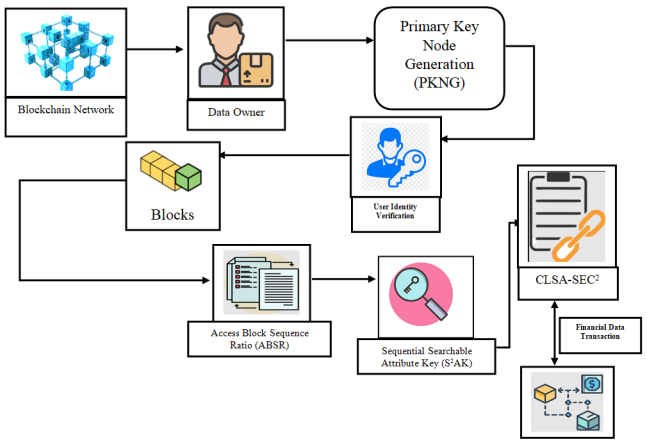

Figure 1: Proposed diagram

$$na_x = K\left(ID_x \| T_x \| R_x\right)$$

$$\{Sk_x, Pk_x\} = Node\,KeyGen(\lambda)$$

Where na_x – primary node , K - Key node, ID_x -unique node id, T_x - Time, R_x -Random key node, Sk_x - private key of node x, λ -Security Parameters, Pk_x -Public key node.

$$Pk_x = K(ID_x \| PK_x)$$

$$Pk_x = K(PK_x \| Nc)$$

$$Pk_x = K\left(PK_x \| ID_x \| T_x\right)$$

$Pk_x \epsilon \mathbb{Z}_x \rightarrow$ Private scalar, $Pk_x \epsilon\, T_x \rightarrow$ public key, $Pk_x \rightarrow$ blockchain key.A primary key can evolve as new modules are added:

$$Pk_x^{(t+1)} = N\left(Pk_x^{(t)} \| Nc_x^{(t)}\right)$$

$\sigma_x = Sig_{pk_x}(Pk_x)$, $Verify(Pk_x, PK_x, \sigma_x) = true$, The node claim the primary key. The multiple nodes in generating the shared primary key,

$$PK_{gruop} = K\left(\sum_{x=1}^{n} Pk_x \| R_x\right)$$

n- Number of contributing nodes, Node N_x can prove it owns Pk_x without revealing it:

$$\pi_x = PN\,gen\left(Pk_x, Sk_x : PK_x == Sk_x.K\right)$$

Add random multiple node sources in blocks, $Pk_x = K(\alpha.ID_x + \beta.T_x + \gamma.R_x + \delta.Pk_x)$, $\alpha, \beta, \gamma, \delta -$ node weights.

Steps

Input: Primary Node (Pn), Block security key verified
Begin
Step 1: Data owner Request (DR)→Request at Access
Step 2: Verified Block key
If (Req. Type R_t== Enter Key) then
Recovering the data to bcheck→TPa.
Transfers theReq (R_trans) ← Key for proper Access
Else if
Req. Type == no match then
Step 3: Decentralised Key authenticate based on the index
If verified, then
Returning Primary data
End if
End
Step 4: Node verified
R←Blocks into the node
End

Where, Tpa- Third party auditing, A key verification form is handed to an access owner who wishes to complete the verification key the privileges that the data owner (data provider) grants. To the maximum, amount of verifiable access securities should be integrated.In the proposed system, data requests are encrypted and transmitted to peers with the assistance of a master key record created by the owner. Introduces improved validation of archived documents and can serve as a single control point for obtaining security keys only. Only after the Key has been verified is decryption of the data permitted.

User Identity Verification (UIV)

Blockchain-based digital identity verification, registration, authentication and user identity verification (UIV). It is even capable of making identity verification efficient, secure and protecting the identity of the identity holder, unlike in the case of conventional identity systems. The use of blockchain as a system of trust can eliminate intermediaries and reduce the need for people to wait to be authenticated and authorised in a blockchain-based identity system.

Due to the calculation of a high number of values, the correct hash value is determined, thus producing a high block generating chain. Each user identity can be reputation-scored,

$$U_s = \sum_{x=1}^{n} w_x * v_x$$

where $v_x \epsilon \{0,1\}$ are validator votes on user identity validity, and w_x are stake-based weights.

$$User\,Identity\,Verified\,(U) \Leftrightarrow U_s \geq T$$

The caching block points at each chain-link A and B, CratesX and Y at the block header, and link points to another block at ranges of 'R' at each point on the link to create a proof hashing index. The equation defines,

$P = (X_1, Y_1)$, be the regular block point then $2p = R = (X_3, Y_3)$, $Q = (X_1, Y_1)$ be the coordination point at 2p be pointed are rounded link of stack point.

At each point of addition, a block of data creates a mutual index Pn at the x circulation point, po, i, which serves as a continuous link to hold the proof of exactly this link.

$$A_n = X_1^{\,2} + \frac{a6}{P_1^{\,2}} + Y_3 = A_1^2 + \left(X_1 + \frac{Y_1}{A_1}\right)A_3 + A_3$$

$A = (X_1, Y_1)$ Then $B_2 = (X_3, Y_3)$ then $A + B = R = (X_3, Y_3)$ p1, and p2 be the link point at proofing P3 in A,B blocks.

$$P_3 = \left(\frac{X_1 + X_2}{P_1 + P_2}\right) + \left(\frac{Y_1 + Y_2}{P_1 + P_2}\right) + P_1 + P_2 + A_2$$

$$X_3 = \left(\frac{X_1 + X_2}{P_1 + P_2} \right) \left(P_1 * P_3 \right) + P_3 + Q_1$$

The proof is available in the consensus of the user role on the user for the block to start each block. The blockchain-link key policy (block-link key policy) defines peer-end verification as a near-majority concern for each block. The non-supportive authentication with a reduced state requires more block verification to mitigate the risk of misfortune and defend the information with respect to the blockchain link point.

Access Block Sequence Rate (ABSR)

The primary objective of the access point ledger is to provide each participant with access control regulations and banking and financial data agreements. A legitimate ID on the access point ledger can be authorized by an authoritative line. Blockchain infrastructures often use public-key cryptography to identify the members of the network. Only the entities required to carry out a data movement of financial information are identified in the Agreement as part of the data privacy and security protection.

$P = \{(R, A, O, D)\}$ → R- Role, A-Access, O-Data contract, D- Time

$$Auth(Ux, A, O) = \begin{cases} 1, & if\ (Attr(Ux) | = P) \wedge verify_{Sig}\ (sig_x, PK_x) = 1 \\ 0, & Otherwise \end{cases}$$

$$Sequence \rightarrow [Policy | IDuser | Access | SigOwner | status]$$

Where IDuser is the participant's identity, Ux -User attributes, $verify_{Sig}$ - authentication, policy is the user access model. Sig_owner is the expiration date of the Agreement, as indicated by the owner's signature, and Access denotes the owner's signature. Only those with a financial relationship are covered by an agreement and are authorised to view, write, update, and delete.

Each access policy of the actions must be approved by consensus,

$$Access(Ux, A, O) = Auth(Ux, A, O) \wedge Attribute\,Consensus\{(Nx)\}$$

Where, Nx - Node validating, $Attribute\,Consensus\ \{(Nx) = 1$, the access control transaction using in blockchain,

$$N_{t+1} = N_x \times T_{xaccess}(Ux, A, O),$$

N_t - Node access time, $T_{xaccess}$ - Transaction access, n - blockchain state. To verify that the participant with the required permits and authorisations has Access to the contract that hasn't been terminated yet, a request to read, write, update, or delete is submitted.

$$Transaction \rightarrow [IDuser | IDledger | Sig \mid data]$$

Where IDuser is the public Key and the signature of the participant respectively, and IDledger is the location of the access point ledger. The global ledger uses the RequestAccess() technique to query the access point ledger, as well as querying whether a contract is valid which is performed using the ContractValidation() element. When the two functions render a positive payoff, the authorization is issued. Otherwise, the Revoke Access () access will not be granted.

Input: ContractArgs, TransDate, Status
Output: Sequence Transaction Response
Response ← TRUE
if ContractArgs ∉ (TransDate, Status) then
Response ← FALSE
End if
Return Response

Verify that the Agreement is legitimate, has not failed, and hasn't been revoked by the controller. GetAttribute() specifies the attribute to be set. An error notice stating that there is no contract to support the request appears if the response is empty. At least one contract has been fetched if the result is not empty. Finally, it uses the policy () method to check if the contract contains the necessary user ID and permissions. If not, it throws an error and returns the access permissions to the user.

Figure 2 shows The proposed blockchain-based access control mechanism integrates cryptographic identity verification, policy-driven authorization, and consensus-

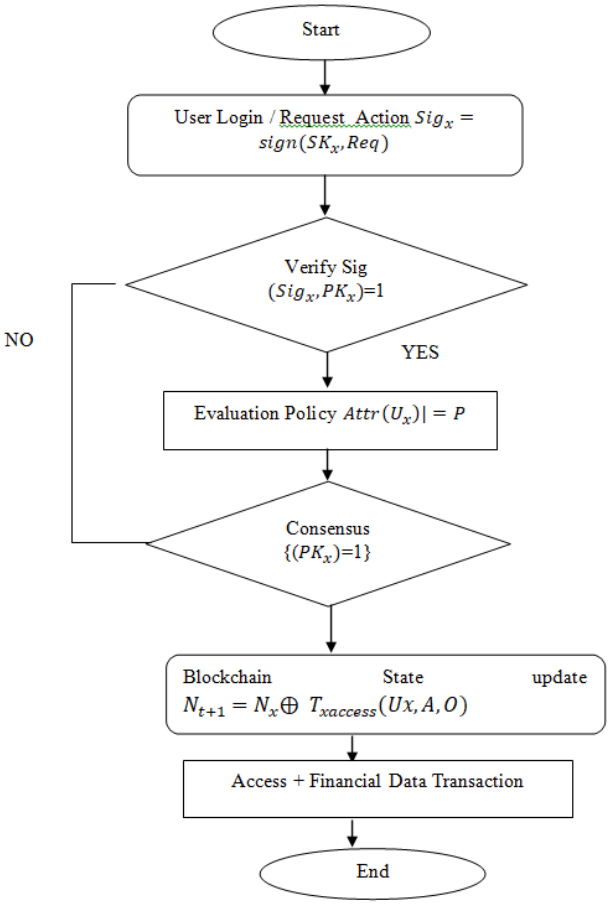

Figure 2: Block diagram for Access control Sequence Rate

based trust validation to ensure secure and auditable resource management. Initially, each user generates a digital signature over the access request using their private key. Proof ensures the authenticity of the request. The system then verifies the user's identity through signature validation, expressed binding the access request to the corresponding public key and blockchain address. Once authenticated, the request undergoes policy evaluation, where user attributes are checked against the predefined access control policy. To prevent unilateral control, the mechanism incorporates blockchain consensus, Finally, the system grants access and logs the event on-chain, guaranteeing accountability, transparency, and non-repudiation. Ensures that blockchain-based access control not only applies security policies but also provides distributed validation and tamper-proof auditing of access activities.

Sequential Searchable Attribute Key (S²AK)

An efficient searchable attribute key access point that can maintain Security even in the event of losing some data. The cryptography using the properties of keys has been recently introduced and tested. To enhance the process of transaction authentication, a searchable attribute key access point comes in that guarantees Security.

Initially, an item–attribute graph can be created using the attribute information A_s for each item in the manner shown below:

$$A_s = (S, B)$$

$$A_s = KeyGen(MSN, Attribute(x_n))$$

Where, $x_n - private\,atribute\,key$, $S\ \{x_n \cup A_s \mid x_n \in B, A_s \in Block\}$,node denotes the set os nodes, containing all the elements or attributes, $B\ \{x_n \cup A_s \mid x_n \in B, A_s \in Block\}$,- block set, and im contains the attribute ak. S²AK model the connectivity attribute sequentially with searchable attributes to aggregate.

For each cipher text index (i)

$$Match(C_i, T_{x,i}) = \begin{cases} 1, if\ attr(x_n) \mid = T \wedge w \in C_i \\ 0,\ otherwise \end{cases}$$

Searches are carried out continuously on encrypted documents, without revealing properties or keywords.

$$B_a^{(s)} = \sum_{a \in B_i^s} \frac{B_a^{(s-1)}}{\sqrt{\left|B_a^s\right|\left|B_i\right|}}, B_a^{(s)} = \sum_{a \in B_i^s} \frac{B_a^{(s-1)}}{\sqrt{\left|B_i\right|\left|B_a^s\right|}}, S = 1, \ldots a$$

Where $e\ B_a^{(s)} \in S$ present the item a and the attribute a's respective insertions in the l-th layer; L is the number of aggregate levels; *d* is the dimension of $\left|B_a^s\right|\left|B_i\right|$ -The items that have the attributes *a*; Added block level security is provided in the proposed access scheme.

To carry out the intent of the object, the user role is used to establish the location of the attribute search and places a User role verification block.

```
While (Transfer file (Tf))
        {
            While (Transfer file id (W) in D)
            {
            If (Find the data user id, D)== False)
            Sequence insert (Data_user Id, W);
            Search sequence a node to N's position
list;
            }
        }
End
```

Step 1: Attributes for sequencing for permission Access Verify to check (S²AK ← Searching Attributes)

To access the data, calculate the connecting chain to the relative block.

Step 2: Access the chain block

Step 3: Return control access.

The proposed access scheme offers additional block-level Security. To implement the purpose of the object, the user role is deployed to define the level of secrecy for the attribute search. It establishes a User role recognition block that prevents each other from being recognized.

Figure 3 Shows the Sequential Searchable Attribute Key (SSAK) framework facilitates secure and fine-grained access to encrypted data by integrating attribute-based key generation with sequential search functionality. In the

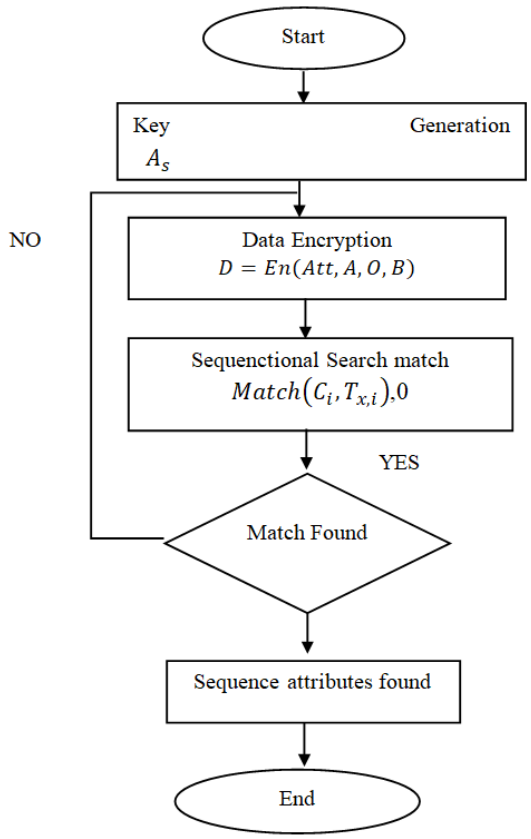

Figure 3: Flowchart for SSAK

initialization phase, the system establishes cryptographic parameters that define the security environment. Subsequently, each user is issued a private key derived from their attribute set, thereby enabling attribute-bound access control. Data owners encrypt documents using both predefined keywords and an associated access policy, ensuring that only authorized entities may query and retrieve the data. The search operation proceeds sequentially over the encrypted document set, and a match is validated only if the user's attributes satisfy the policy and the keyword is embedded within the ciphertext. Upon successful validation, the authorized user is permitted to decrypt the ciphertext and access the underlying document.

Chain Link Smart Agreement based Secure Elliptic Curve Cryptography (CLSA-SEC²)

Blockchain programs are the focus of user encryption, not a generalisation. When relaying using a controller node entity the users may provide their identity over Elliptic Curve Cryptography encryption by disclosing their public Key in chain link access role authentication. The controller node mechanism has proven to be a useful strategy in the verification of data security and privacy among user positions within most of the receiver systems. To begin with, the sender and receiver data must accept the CLSA-SEC² parameters and the parameters of the plan domain. The CLSA-SEC² domain fields are established in the binary case by the pair of P and Q in the case of the original shell P. Ellipse curves are established by the constants R and S. A single element defines a group generated by it, which is arranged. Several log-based procedures are recovered using an elliptic curve.

The identifying key set and utilise it in analysing the index of the sequence of key creation used to encrypt data may be covered by a reversing decryption unit. In each round, the data includes the bytes that should be relocated, computed in terms of the encoded format.

Step 1: The elliptic curve parameters specified by the sender and the receiver should be compatible with the ECC element.

Step 2: The key case P is true, then SEC² parameter ←P; else, 'O' and 'Q' are set as a binary case.

Step 3: Elliptic curve and add the coefficients parameter $s\,a$ and b.

$$r^2 = s^3 + as + b$$

Step 4: Elliptic curves have a finite range.

Step 5: The $G = \infty$ is the prime number to order the crypto value G and check the non-negative number (n).

Step 6: The number of a subsection is to be verified

$$L = \frac{\left| S\left(SG_k\right)\right|}{n}$$

ECC is an encoding scheme which is based on elliptical curves and the complexity of discrete logarithms. ECC has a reputation of being better than other encryption algorithms and has a capability of attaining high amount of cryptographic security with shorter keys.

$$E : y^2 + a_1xy + a_3xy = x^2 + a_2xy + a_4xy + a_5$$

Where $a_i\left(i = 1,2,3,4,\ldots.,5\right) \in N \; and \; \triangle \neq 0$, N-rational number and $\triangle$ – The value of the discriminant of the equation of the elliptic curve:

$$\begin{cases} \triangle - N_2^2 N_8 - 8N_4^3 - 27N_4^3 + 9n_2n_6 \\ n_6 = a_1^2 + 4a_2 \\ n_2 = 2a_4 + a_1a_3 \end{cases}$$

ECC encoding is the selection of an elliptic curve and a point M on curve that will be regarded as the top point. Then just pick a random force r and find elliptical force R=rG where R, G also on the curve. As a form of encryption, the plaintext is appropriately positioned at the position of the elliptic curve and it is the encryption process that is performed through application of the formula that is the public key R. One has to decode the ciphertext using his/her secret key r.

Figure 4 shows to take two points of an elliptic curve P = (x 1, y 1) and Q = (x 2, y 2). The sum is computed as given below:P + Q =(x 3 , y 3)where:

The advantage of the elliptic curves is their symmetry; the group of elliptic curve cryptography or ECC as part of the cryptography can be mentioned as using this property of elliptic curves.

For all access block, the Va chain link created Determine the chain link. Cl keeps blocking aggregation.

$$\text{Cl} = \int_{i=1}^{size(N)} BL\varnothing\left(va - \rightarrow generate\; AES\; K\left(ud\right)\right)$$

End.

$$y2 = x3 + ax + b \; mod \; p$$

$$Pa = nAG \;, Pb = nBG$$

$$Pc = \left\{kG, Pm + k\,Pb\right\}$$

where i is a random integer. The randomisation of the k adds the desired randomness to the ciphertext, hence making it

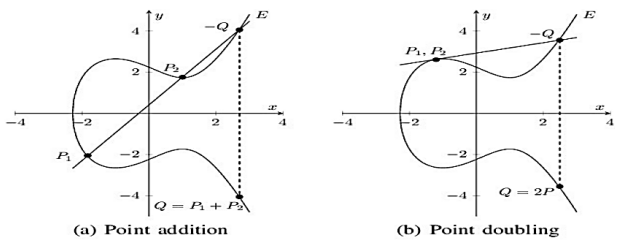

Figure 4: Elliptic Curve

not necessarily similar even when the message is, and that makes it different every time it is generated, even when the message remains the same. Upon decryption, the message is obtained by simply subtracting the coordinates multiplied by nB, --("Pm + kPb"); Light = Pm + kPb -nBkG. The starvation check Key provides the information to modify the check table for the access owner. Limit the rights to access granted by the object owner and the object provider. Integrate end-to-end verifiable access security. Lastly, the authentication key gives one the power to decipher the authentication data.

Result and Discussion

Our experiments will be conducted on a 64-bit Windows 10 version with a processing capacity of 2.90 GHz Intel(R) Core(TM) i5-6267U CPU and 8.00 GB RAM. The C# language was used to package the components required to deploy the software application, ensuring portability and virtualisation. This enabled the application and its dependencies to be executed in a domain-isolated environment, which boosted portability, scalability and manageability. MYSQL database system will be used to manage and store comprehensive financial information (account information, customer information and Transaction information).

The test case is executed with the assistance of a dataset that contains detailed financial data of the account, customer information, transaction records, and indicators of internal controls. A blockchain chain link model recreates the dataset following training, with stored data names that address the variable, conditions, rates, and processes. To this end, a data frame is created by filtering out unscaled/class or imbalanced classes during the algorithm optimisation process. A subset of the data is used in the test, which includes intricate financial data such as account numbers, customer statistics, transaction details, and internal control indicators. A blockchain link model of blockchain reassembles the data in a trained state by using stored data names that are variables, conditions, rates, and processes. To this end, the resulting data frame will be created by discarding unbalanced and unscaled classes in the optimisation of the algorithms.

Dataset Description

A structured set of records that consist of the market, transactional and user attributes that are frequently utilized in financial systems to perform analysis, predictions and risk management. All the records are structured with a variety of fields that contain both quantitative and qualitative data.https://www.kaggle.com/datasets/nitindatta/finance-data?resource=download

Experimental Analysis

The results are authenticated to determine the user-owner relationship, which is based on the client-server request and response mode, as well as the key verification policy in the master node. Security verification begins at the time of Access under the tested simulated user control, as per the logon policy. The results are compared with Chain Link Smart Agreement-based Secure Elliptic Curve Cryptography (CLSA-SEC^2).

The section presents the results of planned experiments conducted on the C# .NET language and Visual Studio tools. Using Financial dataset. The proposed algorithm, CLSA-SEC^2, is compared with existing algorithms, including Trusted Multimedia Scheme with Redactable Blockchain (TMRB), Efficient Zero-Knowledge Blockchain (EZKB), TA-Struc2Vec, Federated Learning-Empowered Recommendation Model (FLRM), and Graph Neural Networks (GNNs).

Figure 6a shows the output of applying the KeyGen algorithm with a fixed number of keys and growing, sequentially, the number of attributes. In the above circumstances, the performance of our program in KeyGen is more in line with the plan and far better than anticipated. More so, our scheme has a better performance than the original scheme when the attributes involved are more

Debenture	Governme	Fixed_Dep	PPF	Gold	Stock_Ma	Factor	Objective	Purpose	Duration	Invest_Mc	Expect	Avenue	What are	Reason_E	Reason_M	Reason_B	Reason_Fl
5	3	7	6	4	Yes	Returns	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Safe Inves	Fixed Retu
2	1	5	6	7	No	Locking Pe	Capital Ap	Wealth Cr	More thar	Weekly	20%-30%	Mutual Fu	Health Ca	Dividend	Better Ret	Safe Inves	High Inter
4	2	5	1	7	Yes	Returns	Capital Ap	Wealth Cr	3-5 years	Daily	20%-30%	Equity	Retiremen	Capital Ap	Tax Benef	Assured R	Fixed Retu
3	7	6	4	5	Yes	Returns	Income	Wealth Cr	Less than	Daily	10%-20%	Equity	Retiremen	Dividend	Fund Dive	Tax Incent	High Inter
3	6	4	5	7	No	Returns	Income	Wealth Cr	Less than	Daily	20%-30%	Equity	Retiremen	Capital Ap	Better Ret	Safe Inves	Risk Free
4	6	3	1	2	No	Risk	Capital Ap	Wealth Cr	1-3 years	Daily	30%-40%	Mutual Fu	Retiremen	Liquidity	Fund Dive	Safe Inves	Risk Free
4	2	5	1	7	Yes	Returns	Capital Ap	Wealth Cr	3-5 years	Monthly	20%-30%	Equity	Retiremen	Capital Ap	Better Ret	Assured R	High Inter
7	4	6	1	5	Yes	Risk	Capital Ap	Wealth Cr	3-5 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Assured R	Risk Free
7	5	3	1	6	Yes	Returns	Growth	Savings fo	1-3 years	Weekly	20%-30%	Equity	Retiremen	Capital Ap	Fund Dive	Safe Inves	Fixed Retu
7	4	5	2	6	Yes	Returns	Capital Ap	Wealth Cr	3-5 years	Monthly	30%-40%	Fixed Dep	Retiremen	Capital Ap	Fund Dive	Assured R	Fixed Retu
7	5	3	1	6	Yes	Risk	Growth	Savings fo	3-5 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Assured R	Risk Free
7	6	3	1	4	Yes	Risk	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Fund Dive	Assured R	Fixed Retu
3	4	5	6	7	No	Returns	Capital Ap	Savings fo	1-3 years	Weekly	20%-30%	Mutual Fu	Education	Dividend	Better Ret	Safe Inves	Risk Free
7	4	5	1	6	Yes	Returns	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Fund Dive	Assured R	Risk Free
7	5	4	1	6	Yes	Returns	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Fixed Dep	Health Ca	Dividend	Better Ret	Assured R	Risk Free
7	5	4	1	6	Yes	Returns	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Health Ca	Capital Ap	Fund Dive	Assured R	Risk Free
7	5	4	1	6	Yes	Risk	Growth	Wealth Cr	1-3 years	Monthly	20%-30%	Fixed Dep	Health Ca	Capital Ap	Fund Dive	Assured R	Risk Free
7	4	5	1	6	Yes	Returns	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Assured R	Risk Free
7	4	5	1	6	Yes	Risk	Capital Ap	Wealth Cr	1-3 years	Monthly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Assured R	Risk Free
6	5	1	2	7	Yes	Risk	Capital Ap	Wealth Cr	3-5 years	Monthly	20%-30%	Fixed Dep	Health Ca	Capital Ap	Fund Dive	Assured R	Risk Free
7	5	3	1	6	Yes	Returns	Growth	Wealth Cr	3-5 years	Weekly	20%-30%	Mutual Fu	Retiremen	Capital Ap	Better Ret	Assured R	Fixed Retu

Figure 5: Dataset description333

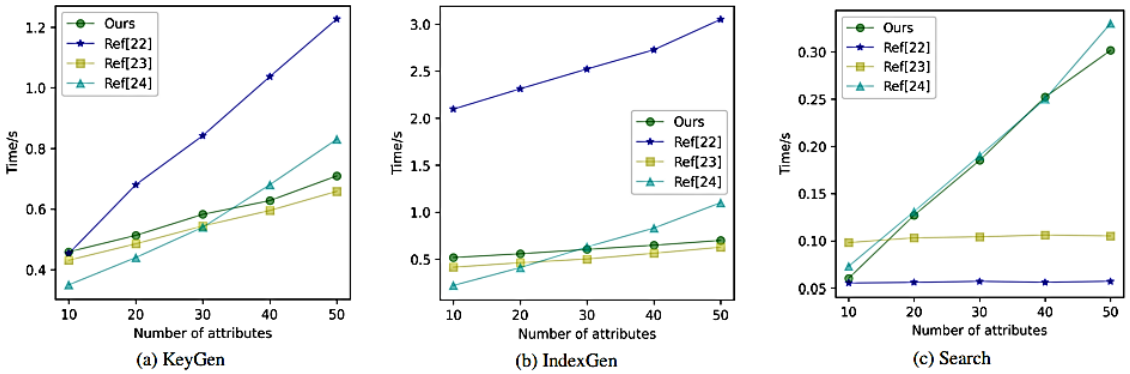

Figure 6: Performance evaluation for 50 keywords.

than a specified amount. Figure 6a shows that the KeyGen algorithm is abiding by the rule. First, the computational cost of both of the KeyGen algorithms is compound by increasing the number of attributes.

The performance of the IndexGen algorithm is assessed in Figure 6b as the number of characteristics increases while the number of keywords remains constant. Even if the scheme performs better, Figure 6b shows its performance. However, as the attribute scale size grows, the plot curves and our plot grow more gradually, indicating that our scenario is more favourable.

Figure 6c presents the result of the searching algorithm when we allow the number of attributes to vary at a close rate and indicate the number of keywords to remain constant. As Figure 6c shows, the two schemes perform in a similar, relatively stable fashion, with the search algorithm performance affected very little by the number of attributes. Nevertheless, both this solution and our solution exhibit poor performance regarding the search algorithms, and the performance level decreases grows linearly with the growing number of attributes.

Figure 7 describes the efficiency of the execution process between encryption and decryption. The suggested system offers a blockchain exchange as part of its mechanism, along with a blockchain cypher policy. The performance of this CLSA-SEC^2 implementation is much improved over other methods.

Figure 8 demonstrates various methods of analysis that will be created by different users to analyse the Security. The CLSASEC^2 proposed system has a greater effect on the performance of Security than the alternative similar techniques.

In this Transaction, the access rate is set by the user through an associated connection, allowing them to monitor the bookee without interruption and retrieve data from a database. Another existing method has a transaction access rate of 97.6% as compared to the proposed CLSA-SEC2 method. Figure 9 indicates this comparison. The current system offers data user access control of 97.6% on a server.

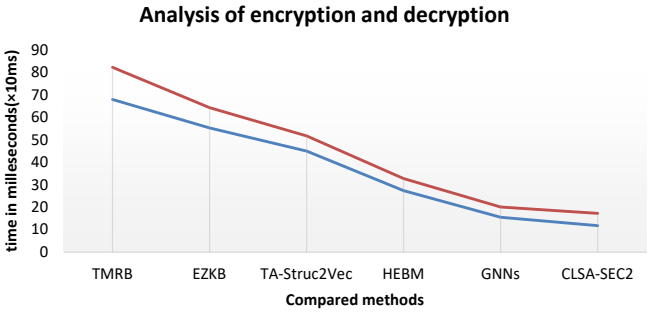

Figure 7: Execution efficiency encryption and decryption

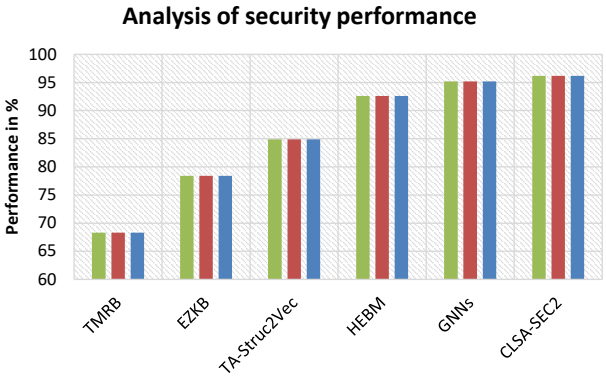

Figure 8: Comparison of security analysis

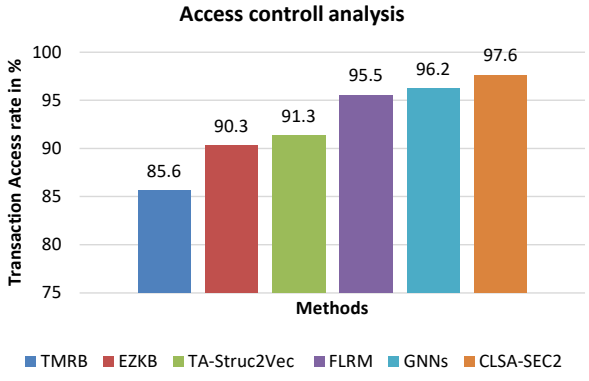

Figure 9: Access control analysis

In Figure 10, the throughput analysis is compared. The CLSA-SEC² methodology has a 540tps higher transaction throughput rate than the other ways employed in this examination of the methodological technique, as suggested. ECC is used as the authentication method in CLSA-SEC² to increase its throughput rate due to its low authentication latency and quick encryption when compared to other authentication methods.

Figure 11 shows the performance comparison of Transaction Accuracy between the proposed and existing results. The Accuracy of transaction performance is 96 per cent for the proposed CLSA-SEC² algorithm. On the same note, the present-day performance of Trusted Multimedia Scheme with Redactable Blockchain (TMRB) is 76%, Efficient Zero-Knowledge Blockchain (EZKB) is 79%, TA-Struc2Vec is 85%, and the performance of Federated Learning-Empowered Recommendation Model (FLRM) is 89% the performance of Graph Neural Networks (GNNs) in transaction accuracy is 93%. The improvement of the proposed algorithm over the existing algorithm in terms of transaction accuracy is increasing.

Figure 12 presents the performance analysis of transaction accuracy in terms of the proposed and existing results, as well as the suggested CLSA-SEC2 algorithm. The Accuracy of transaction performance is 96%. Similarly, the current performance of Trusted Multimedia Scheme with Redactable Blockchain (TMRB) is 76%, Efficient Zero-Knowledge Blockchain (EZKB) is 79%, TA-Struc2Vec is 85%, and the performance of Federated Learning-Empowered

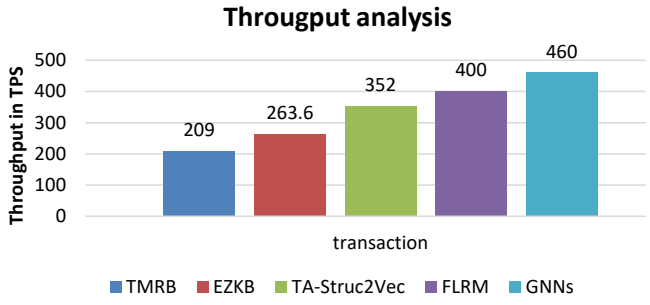

Figure 10: Comparison of throughput analysis

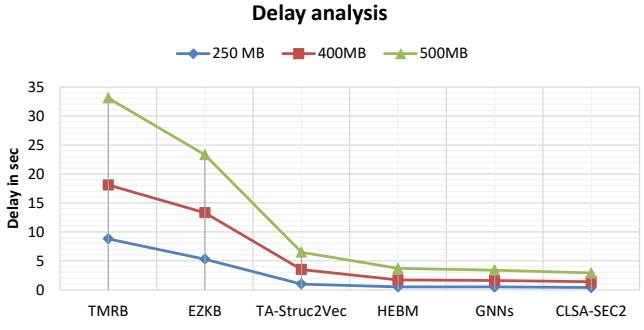

Figure 11: Comparison of authentication delay analysis

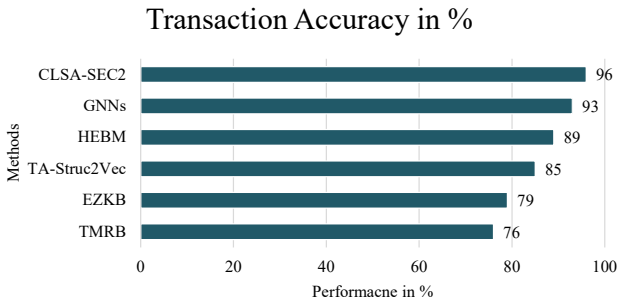

Figure 12: Analysis of transaction accuracy

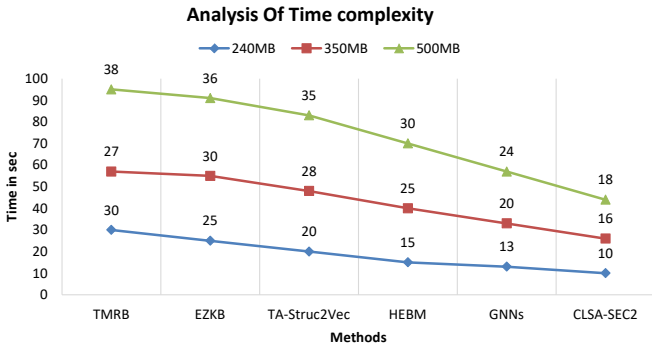

Figure 13: Time complexity

Recommendation Model (FLRM) is 89%. Graph Neural Networks (GNNs) achieve a transaction accuracy of 93%. The performance of the proposed algorithm is improving transaction accuracy over the existing algorithm.

Figure 13 illustrates the comparison of time complexity analysis according to the Big O notation. The processing time of the proposed CLSA-SEC² algorithm is 18 seconds on a 500MB file. Likewise, the prior TMRB algorithm takes 38 seconds, EZKB takes 36 seconds, TA-STRUC2VEC takes 35 seconds, HEBM takes 30 seconds, and GNNs take 24 seconds to process a 500MB-sized file.

Conclusion

In conclusion, the CLSA-SEC² system design for blockchain can provide added Security of information, including time and efficiency, in the Banking sector. The system enables the outsourcing of data storage through a distribution network of service providers. Enhancing data integrity through the role of blockchain technology in Financial verification policies. Client-side encryption enhances the data security; therefore, a distinct keyword search has been designed to search through the encrypted data sets. Blockchain supports the issuance of anonymous credentials, the verification of the credentials, and the discovery of a secret key.Moreover, an analysis of the main differences between the blocks of the Blockchain approach is performed, which allows one to analyse the effectiveness and Accuracy of the detection of suspicious transactions in the financial industry. Lastly, using one of the models that considers financial transactions,

considerable results were obtained regarding the internal control's ability to detect suspicious transactions. The proposal presents a secure cloud storage system that uses a chain-based encryption process. The data owner may assign a decentralised peer access authority to verify the Accuracy of the data. To protect the privacy of the original data in the decentralised blockchain, controller node key verification is carried out during the audit process rather than using outsourced encryption. Using our system, the CLSA-SEC^2 system, we achieve 97% efficiency and complexity reduction in outsourced encryption, enhancing Security and storage.

Acknowledgements

The authors would like to express their sincere gratitude to Jamal Mohamed College for providing the necessary facilities and support to carry out this research work. We also thank our college management, heads, co-researchers, colleagues and reviewers for their valuable feedback and constructive suggestions, which greatly improved the quality of this manuscript.

References

Al-Jaroodi, J., and Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access, 7,* 36500–36515. https://doi.org/10.1109/ACCESS.2019.2902501

Amankona Obiri, J., Gao, J., Xia, Q., Xia, H., and Nii Aflah Cobblah, C. (2025). Hiba: Hierarchical high-performance blockchain architecture. *IEEE Transactions on Networking, 33*(1), 311–326. https://doi.org/10.1109/TNET.2024.3481488

Baliker, C., Baza, M., Alourani, A., Alshehri, A., Alshahrani, H., and Choo, K. K. R. (2024). On the applications of blockchain in FinTech: Advancements and opportunities. *IEEE Transactions on Engineering Management, 71,* 6338–6355. https://doi.org/10.1109/TEM.2022.3231057

Chatterjee, P., Das, D., and Rawat, D. B. (2024). Federated learning empowered recommendation model for financial consumer services. *IEEE Transactions on Consumer Electronics, 70*(1), 2508–2516. https://doi.org/10.1109/TCE.2023.3339702

Chishti, M. S., Sufyan, F., and Banerjee, A. (2022). Decentralized on-chain data access via smart contracts in Ethereum blockchain. *IEEE Transactions on Network and Service Management, 19*(1), 174–187. https://doi.org/10.1109/TNSM.2021.3120912

Chen, E., Wang, S., Fan, Y., Zhu, Y., and Yau, S. S. (2023). SaaSC: Toward pay-as-you-go mode for software service transactions based on blockchain's smart legal contracts. *IEEE Transactions on Services Computing, 16*(5), 3665–3681. https://doi.org/10.1109/TSC.2023.3267489

Fetaji, B., Fetaji, M., Hasan, A., Rexhepi, S., and Armenski, G. (2025). FRAUD-X: An integrated AI, blockchain, and cybersecurity framework with early warning systems for mitigating online financial fraud: A case study from North Macedonia. *IEEE Access, 13,* 48068–48082. https://doi.org/10.1109/ACCESS.2025.3547285

Ichsani, Y., Deyani, R. A., and Bahaweres, R. B. (2019). The cryptocurrency simulation using elliptic curve cryptography algorithm in mining process from normal, failed, and fake Bitcoin transactions. *2019 7th International Conference on Cyber and IT Service Management (CITSM),* Jakarta, Indonesia (pp. 1–8). https://doi.org/10.1109/CITSM47753.2019.8965370

Islam, M. M., and In, H. P. (2023). A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs. *IEEE Transactions on Services Computing, 16*(4), 2372–2386. https://doi.org/10.1109/TSC.2022.3226120

Islam, S., and Apu, K. U. (2024). Decentralized vs. centralized database solutions in blockchain: Advantages, challenges, and use cases. *Global Mainstream Journal of Innovation, Engineering and Emerging Technology, 3*(4), 58–68.

Jahan Sarna, N., et al. (2025). AI-driven fraud detection models in financial networks: A comprehensive systematic review. *IEEE Access, 13,* 141204–141233. https://doi.org/10.1109/ACCESS.2025.3596060

Koo, K., Park, M., and Yoon, B. (2024). A suspicious financial transaction detection model using autoencoder and risk-based approach. *IEEE Access, 12,* 68926–68939. https://doi.org/10.1109/ACCESS.2024.3399824

Li, J. (2023). Dynamic financial and monetary security risk assessment based on information service security assessment model and blockchain. *Scientific Reports, 13,* 18707. https://doi.org/10.1038/s41598-023-45977-5

Li, J., and Ning, Y. (2024). Blockchain transaction sharding algorithm based on account-weighted graph. *IEEE Access, 12,* 24672–24684. https://doi.org/10.1109/ACCESS.2024.3365510

Li, R., Liu, Z., Ma, Y., Yang, D., and Sun, S. (2023). Internet financial fraud detection based on graph learning. *IEEE Transactions on Computational Social Systems, 10*(3), 1394–1401. https://doi.org/10.1109/TCSS.2022.3189368

Li, Z., Liang, X., Wen, Q., and Wan, E. (2024). The analysis of financial network transaction risk control based on blockchain and edge computing technology. *IEEE Transactions on Engineering Management, 71,* 5669–5690. https://doi.org/10.1109/TEM.2024.3364832

Ni, J., Xiao, J., Zhang, S., Li, B., Li, B., and Jin, H. (2023). FLUID: Towards efficient continuous transaction processing in DAG-based blockchains. *IEEE Transactions on Knowledge and Data Engineering, 35*(12), 12679–12692. https://doi.org/10.1109/TKDE.2023.3272312

Nguyen-Hoang, T.-A., et al. (2024). Advancing scholarship management: A blockchain-enhanced platform with privacy-secure identities and AI-driven recommendations. *IEEE Access, 12,* 168060–168090. https://doi.org/10.1109/ACCESS.2024.3486078

Ogeti, P., Narendra, S., Patil, K., Padyana, H., Rai, R., and Patil, G. (2022). Blockchain technology for secure and transparent financial transactions. *European Economics Letters, 12,* 180–188.

Okoye, M. O., and Kim, H.-M. (2022). Optimized user-friendly transaction time management in the blockchain distributed energy market. *IEEE Access, 10,* 34731–34742. https://doi.org/10.1109/ACCESS.2022.3162214

Okoye, M. O., Yang, J., Cui, J., Hussain, A., Bui, V.-H., and Espin-Sarzosa, D. (2024). Optimizing the transaction latency in the blockchain-integrated energy-trading platform in the standalone renewable distributed generation arena. *IEEE Access, 12,* 111970–111981. https://doi.org/10.1109/ACCESS.2024.3414966

Prabanand, S. C., and Thanabal, M. S. (2025). An advanced financial

security system using smart contracts in a private Ethereum consortium blockchain with hybrid optimisation strategy. *Scientific Reports, 15,* 6764. https://doi.org/10.1038/s41598-025-89404-3

Ren, Q., et al. (2024). DeCloak: Enable secure and cheap multi-party transactions on legacy blockchains by a minimally trusted TEE network. *IEEE Transactions on Information Forensics and Security, 19,* 88–103. https://doi.org/10.1109/TIFS.2023.3318935

Sarwar, M. I., Khan, I., Maghrabi, L. A., Jaffar, A., and Akram, S. (2024). Tripartite accounting framework: A novel blockchain-based model for recording B2B transactions. *IEEE Access, 12,* 198097–198122. https://doi.org/10.1109/ACCESS.2024.3522093

Shoetan, P., and Familoni, B. (2024). Blockchain's impact on financial security and efficiency beyond cryptocurrency uses. *International Journal of Management and Entrepreneurship Research, 6,* 1211–1235. https://doi.org/10.51594/ijmer.v6i4.1032

Singh, K., and S. G. (2023). Blockchain-powered enhancement of financial network security through AI-based tools. *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON),* Bangalore, India (pp. 1–5). https://doi.org/10.1109/SMARTGENCON60755.2023.10441916

Singh, R., Dwivedi, A. D., Srivastava, G., Chatterjee, P., and Lin, J. C.-W. (2023). A privacy-preserving Internet of Things smart healthcare financial system. *IEEE Internet of Things Journal, 10*(21), 18452–18460. https://doi.org/10.1109/JIOT.2022.3233783

Saba, T., Haseeb, K., Rehman, A., and Jeon, G. (2024). Blockchain-enabled intelligent IoT protocol for high-performance and secured big financial data transaction. *IEEE Transactions on Computational Social Systems, 11*(2), 1667–1674. https://doi.org/10.1109/TCSS.2023.3268592

Tse, W. K., Dai, X., Lee, Y. M., and Lu, D. (2024). User acceptance of blockchain technology in financial applications: Information security, technology awareness and privacy aspects. *Blockchains, 2*(3), 299–311. https://doi.org/10.3390/blockchains2030014

Tunzina, T., et al. (2024). Blockchain-based central bank digital currency: Empowering centralized oversight with decentralized transactions. *IEEE Access, 12,* 192689–192709. https://doi.org/10.1109/ACCESS.2024.3517147

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., and Zheng, Z. (2023). Financial crimes in Web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society, 4,* 37–49. https://doi.org/10.1109/OJCS.2023.3245801

Zhang, T. (2025). TMRB: Trusted multimedia scheme with redactable blockchain. *IEEE Transactions on Consumer Electronics, 71*(2), 3099–3107. https://doi.org/10.1109/TCE.2025.3542637

Zhang, T., Jia, F., and Chen, L. (2025). Blockchain adoption in enabling disruptive supply chain finance innovation: Toward a research agenda. *IEEE Transactions on Engineering Management, 72,* 1519–1531. https://doi.org/10.1109/TEM.2025.3559468

Zhou, L. (2025). Blockchain in finance: Enhancing transparency and security in cross-border transactions. *Journal of Applied Economics and Policy Studies, 17,* 56–60. https://doi.org/10.54254/2977-5701/2025.21075