



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Certificateless Signcryption for Data Secure Transmission based on Hook Curve Revised Hash Authentication

M. Kayathiri ¹, Dr. M. Ramakrishnan ², S. Venkatesan ³

¹ Research Scholar, Department of Computer Science, Madurai Kamaraj University, Madurai, Tamil Nadu, India.

E-mail: sivamadhu9714@gmail.com

² Professor and Head, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India.

E-mail: ramkrishod@gmail.com,

³ Department of Computer Applications, Madurai Kamaraj University, Tamil Nadu, India. E-mail: venkatesan708@gmail.com

Abstract

The Consumer demand growth in the blockchain enables the communication of several facts at each instant. Signcryption can simultaneously analyze encryption and cross with lower computational economy and statement above those of the outdated sign then encrypt method. The certificateless cryptosystem describes the key escrow problem in the identity-based cryptosystem and simplifies the public key management of the outdated public key cryptosystem. Several certificateless Signcryption structures have been evaluated in the proposed approach. Blockchain technology will enable the approach to be distributed, transparent, and highly secure. All blockchain transactions are secured using a cryptographic hash. However, they are either insecure or inefficient. To overcome this issue, we proposed the Hook Curve Revised Hash Authentication (HC-RHA) method for encrypting the data during the network of transmission using one-time padding encryption crypto policy (OTPCP). To create new node transactions in the network based on the PoA Pre-Ack decentralized chain link (PoA-PA). During transmission, the MTNBR is analyzed in the transaction node to improve the network trust rate based on the improved weight data designed a block hash index using user behavioral policy to form chain link in Blockchain. The HC-RHA trust policy is applied to verify the transaction framework to check if the transaction approach is valid. A security analysis shows that a distributed blockchain network will certify verification results and improve Integrity and access control

Keywords: Security, Blockchain, certificateless Signcryption, Encryption Crypto Policy, transaction node, public key.

1. Introduction

The signcryption algorithm can logically do both encryption and signature tasks simultaneously. Signcryption algorithms are widely used in electronic payments, the Internet of Things, and other fields because they are less expensive to calculate and communicate than the predictable approach of validation first and then converting. Within a plausible logical step, signcryption may perform the tasks of public key cryptography and digital signatures. Many certificateless signcryption scheme agreements are proposed, and its calculation and statement costs are lower than those of the conventional sign-then-encrypt approach.

However, a standard signcryption strategy is ineffective when the amount of signcryption is greater. Multiple ciphertexts can be gathered using aggregate signcryption, which also offers batch quantity verification. Verification of signcryption and communication transmission efficiency are increased. The issues of key escrow in identify public key cryptanalysis and certificate Optimization in conventional public key cryptography can both be resolved by certificateless aggregate signcryption. Correspondence and signature verification can be made less expensive in the interim. The ciphertext must be transferred collectively and verified in order to increase the smart grid's correspondence and computation efficiency. To solve the main problem without requiring a public-key infrastructure or the usage of certificates, the idea of certificateless (CL) cryptosystems was presented.

The common description behind a CL structure is to divide sequestered keys into two parts: one conservative but non security partial key unfamiliar to the KGB and one identity-based partial key KGB and so otherwise focus to escrow. In fact, several certificateless encryption methods following from identity-based encryption algorithms have been properly created and confirmed secure under specific conventions, suggesting that this procedure may combine the best aspects of individuality based and security based cryptography. However, defining and analyzing certificateless signatures is still considerably more difficult. As a result, creating

certificateless sign encryption framework has been a challenging task that has only recently been resolved, but the only recognized protocol of this type can barely be regarded as efficient.

A signcryption scheme is a more efficient approach to encrypt and sign a message than using separate encryption and signature schemes. Processing period, bandwidth usage, key management, or any combination of these could be the source of the efficiency gain; it could also unbiased be a reliable method of combining the two primitives to prevent harmful interactions. In this work, develop a security signcryption approach using a relatively unique methodology. By using Hook Curve, extend a certificateless encryption approach with a conventional signature scheme without using security for the latter component, as opposed to combining an identity-based encryption approach with an equally individuality-based signature scheme and alternative the result to a security protocol.

In addition to making certificateless encryption resistant to these two threats, this method can reduce blockchain storage capacity and address challenging certificate management issues. Corresponding experimental results demonstrate that our technique can effectively thwart the kinds of attacks that certificateless encryption systems face and address the main issue. The technology is perfect for areas with limited resources since it drastically lowers computation and communication expenses. Our method preserves forward secrecy while satisfying the required security standards and security analysis shows that the suggested approach is successful and efficient.

2. Related work

The confidentiality of a message can be guaranteed by encryption, while the integrity of a message and the individuality of a signer can be confirmed by a signature. Numerous certificateless signcryption (CLSC) systems have been examined and proposed by cryptography experts in the past in an effort to combine the advantages of encryption and signatures. These techniques might not be strong enough to resist side-channel assaults, albeit [1]. To increase road safety, they use wireless communication to deliver early notice of hazards. As a result, we should guard against message leaks and modifications while they are being transmitted. We suggest a safe and efficient certificateless signcryption technique with numerous messages and multiple receivers to guarantee the security of the communication process.

The L-CLSS is a lattice-based CSE structure. L-CLSS has three advantages. First, the random oracle framework is demonstrated to be indistinguishable against adaptive ciphertext-chosen assaults under the intractability of the learning with errors (LWE) challenge and unforgeable against adaptive message-chosen attacks over the challenge of the small integer solution (SIS) problem. A certificateless signcryption (CLSC) framework, which combines encryption and signature to ensure authenticity, secret, and unforgeability, is an efficient way to address the IoMT data privacy challenge. However, existing CLSC technologies either fail to meet the criteria for covertness or unforgeability or require expensive calculation overhead to complete pairing procedures [4]. As recommended by the 3rd Generation Partnership Project (3GPP), an improved protocol that utilizes a hybrid cryptosystem is proposed to achieve access identification for WLAN user equipment (UE) with identity privacy assurance to get around the security vulnerabilities of authentication protocols in the LTE-WLAN heterogeneous converged network [5]. However, physiological markers are sensitive patient data, making it challenging to confirm data sources while protecting data privacy during IoMT data transfer. Certificateless signcryption is an excellent choice for developing a secure data transfer mechanism in IoMT because of its dual encryption and signature capabilities and ease of delivery [6]. However, "malicious users" and "malicious KGC" are internal opposing forces capable of performing Type I and Type II attacks.

Nevertheless, some low-power biological sensors are frequently used in technology, making them vulnerable to scammers and incompatible with traditional cryptographic techniques. The most significant security concern in IoHT is ensuring the authenticity of online health-related communications [7]. EC can effectively address network congestion, feedback delay, and CS-induced loss of privacy during transmission. This study proposes a certificateless AMS with online/offline encryption based on edge computing (EDC). Consequently, certificateless signcryption (CLSC), online/offline encryption (OOE), and aggregate signcryption technology all shorten encryption times, solve the key management problem, and provide quick user verification [8].

The proposed plot is secured from key security concerns and testaments by the certificateless setting. TSC without pairings enables multisource data collection and synchronous validation with efficient cryptographic manufacturing. Employing the irregular prophet model, the plot achieved secrecy and unforgeability. According to the security analysis, the suggested scheme offers vehicles nom de plume-dependent protection, mystery, and immunity to many known attacks [9]. Cryptographic computations address the security concerns of the IoT network regarding information uprightness and validation for information transmission throughout the company. However, traditional cryptography techniques are laborious, complex, and expensive to compute. Dedicated, useful, lightweight, and efficient computations are consequently required. [10].

Table 1 Existing Survey

Author name/ Year	Proposed Method	Limitations	Results
S. Ma et al/2022	Practical Byzantine Fault Tolerance (PBFT)	Increasing cost and low privacy data	Security-98.6% Accuracy-0.98%
P. Kang et al/2022	Document content storage and distribution that integrates blockchain technology	Illegal security and data access	Error rate-0.0001% Packet loss-0.95%
E. Zeydan et al /2024	blockchain-based network sharing solution	Network sharing issues	Security-95.6% Throughput-0.94%
S. Shao et al/2023	Byzantine fault tolerance	challenge to ensure the privacy and security	Delay-0.52% Data delivery-0.95%
W. Zheng et al/2019	Elliptic Curve Digital Signature Algorithm	Complexity of blockchain	Throughput-0.841%
N. Afraz et al/2023	Convolutional Neural Network (CNN)	Low accuracy and high cost	Transaction speed-300 to 400 TPS
M. I. Khalid et al/2023	Attribute-based encryption (ABE)	Low storage and privacy	Throughput-0.689%
S. Wang et al/2019	Byzantine fault tolerance	Security and privacy issues	Speed-0.97% Time-0.25Sec
M. N. M. Bhutta et al /2021	Digital signature algorithm (DSA)	Privacy Leakages	Security-99.6% Transaction speed-100 to 200 TPs
J. Lee et al /2023	Consensus algorithm and timeslot allocation policy	Risk of resource consumption	Error Rate-0.002%

Table 1 explored the blockchain network security issues and previous existing work experiment results using proposed methods. However, more security issues arise when there are a lot of devices and more messages at the edge. As a result, offering users speedier network services while maintaining data transmission confidentiality and authentication is a crucial area of research. Signcryption has emerged as a novel cryptographic primitive due to its ability to simultaneously encrypt and sign communications [21]. A VNDN-based certificateless sign encryption technique that makes use of edge computing and the security hardness of the hyper elliptic curve cryptosystem. The efficacy of the method is demonstrated by security analysis and comparisons with similar systems [22]. A blockchain-based one-time anonymous certificateless sign encryption (OTACLSC) system. To increase the private key's security, safely use the public channel.

On order to prevent identity leaking, the communication initiator creates a one-time assumed name public key on the blockchain. This prevents the pseudonym public key from being reused by both communication parties. Next, we compare the method with existing schemes and demonstrate its security under the random oracle model [23–24]. Elliptic curve cryptography (ECC) and certificateless cryptography (CLC) are used to create a signcryption technique that concurrently ensures the block information's confidentiality and unforgeability. Additionally, through the use of indexes and Merkle proofs, lower-layer private blockchains and upper-layer alliance blockchains collaborate to achieve intradomain and interdomain authentication more effectively [25].

3. Proposed Method

Hook Curve Revised Hash Authentication (HC-RHA), the suggested technique, distinguishes between authorized and unauthorized users within blockchain networks. Recognize network packets, generate encryption in compliance with permissions and shared resource rules, and verify user and owner identities. A peer-to-peer blockchain network and a public blockchain ecosystem are the end results. For certificateless signcryption, employ an HC-RHA-encrypted data network of nodes that receive the encrypted blocks.

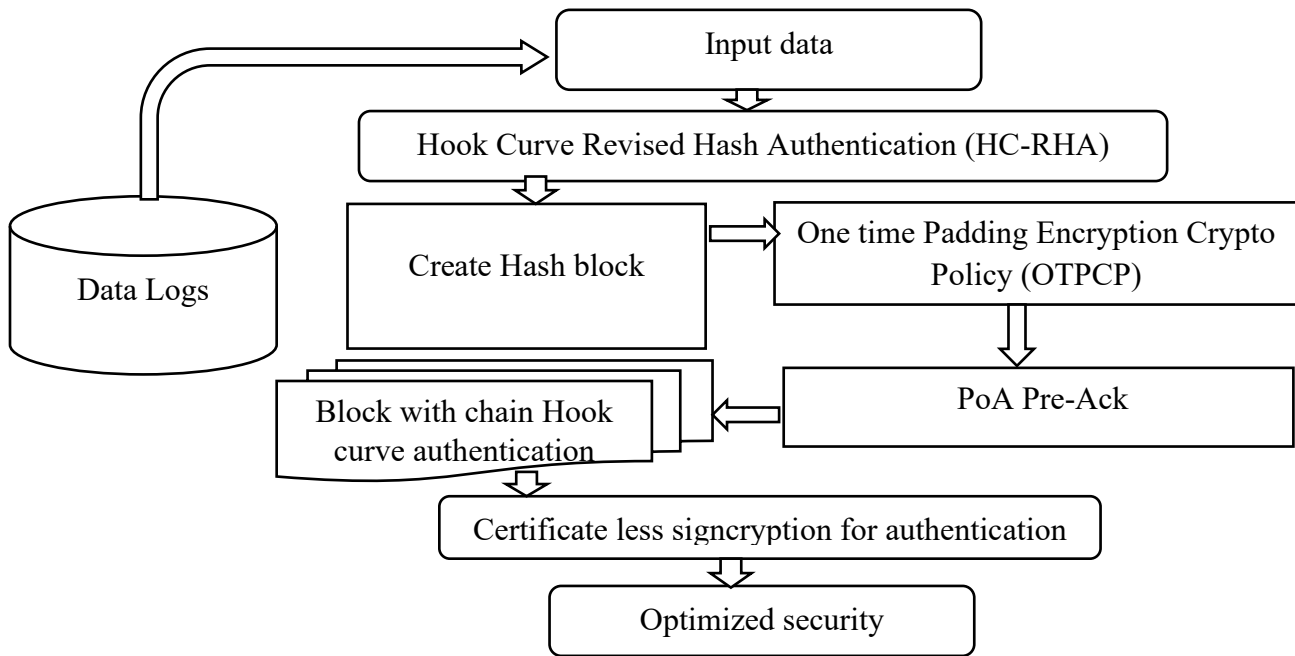


Figure 1: Proposed Architecture diagram

The transaction procedure verifies the dependability of the node network while data is being transferred. Transaction block storage securely stores monitoring data through the use of hash index blocks and chain link policies. The architectural layout of the proposed system is depicted in Figure 1. Cryptography is used to check user profiles, sign encrypted certificates, and sign encryption data using hook curves and padding. A key public encryption solution that optimises the advantages of blockchain architecture is HC-RHA. The team analyses the alert using a specified key agent and retrieves the keys generated by the various agents from an on-site Block server.

3.1 Blockchain Initialization using certificateless signcryption

A threshold of (t, n) A group of n people can be authorized by the distributor using a signcryption system. Any t or more signcrypters can work together to sign the message, but fewer signcrypters cannot. There are numerous uses for threshold sign encryption in distributed environments, electronic elections, electronic auctions, block computing, and block chains. In order to create a secure and effective certificateless threshold signcryption scheme with a secret sharing mechanism that uses Hook curve schemes in computational efficiency, combine threshold signcryption with certificate-less cryptosystems. This will garner a lot more attention in the information security application fields.

In this stage, B_q and B_p are two block of multiplication groups with prime order p, q is a generator of group Block 1

$B: B_1 \times B_1 \rightarrow B_2$ is secure hash functions selected by the KGC, where l is the length of message. The master key is then chosen by the KGC.

A message of any arbitrary length can be used as the input for the hash function, but it always yields a hash code, hash value, a short output of a set length, indivisible, or hash. The fixed-length strings are mapped to bit-strings of any length using a hash function field n bit. One way to define a hash function field is as-

1) In a given multifunction property that contains hash functions.

a) Compression- The hash should take any given (arbitrary) length input and convert it to a fixed and short length output.

b) Ease of Computation Simplicity. It should be easy to calculate the field (X) for any message.

2) If both the original and the hash value are not equal, then HASH is called weak collision resistance. $X: X \neq X'$ such that $\text{HASH}(X) = \text{HASH}(X')$.

3) If the hash is computationally impossible to acquire two different messages X and X' , called strong collision resistance that is $X \neq X'$ such as hash matches there: $\text{hash}(X) = \text{hash}(X')$. Unquestionably strong collision resistance indicates very weak collision resistance.

4) Given the news to digest Y , it is computationally impossible to obtain a field X -like field that $\text{HASH}(X) = Y$

5) If it fulfills the given requirements, it is possible to call it a hash function.

- Any m should be relatively easy to calculate.

- There must be a way of proximity.
- Too much of a conflict with power.

1) Based on the above definition, it may formalize some basic properties of any encryption hash function. To assume two inputs p and p'' and the corresponding outputs k and q :

2) Certificateless signcryption is computationally infeasible to discover any input that hashes to any of the pre-specified hash value. That is, to find any pre-image p'' such that it maps to predefined hash value q : $\text{HASH}(p'') = q$.

To find, has the same output as the previously specified input of the damage" such a hash $(p) = \text{field}(p)$. This property is also known as "weak collision resistance. Signature Verification decrypted message is verified to ensure its validity by examination the signature compared to the sender's public key Certificateless signcryption typically reduces the overhead of managing certificates in blocks.

3.2 Hash block generating

The key is validated initially, followed by validation and proof of validity. It turns out that the peer can access the data because of this validity authentication.

The request Key

$P_B \rightarrow \text{Valid user } V_u$

If verified key is checked during partially corresponding main key authentication

$R \rightarrow \text{At } P_B(V_u) \leftarrow F_q$

To reach the peer end at the determinate set of blocks, use the over shaped important formulation method.

$P_B(V_u) \leftarrow F_q(\text{Encrypted block})$

To reorganize the chain's link, validate the hash index sequence. $H_B \rightarrow P_B(V_u)$

Verify the user key, which is $KB = H_B \rightarrow P_B(V_u)$. Verification of block hash keys

Verify the peer block's machine address during the gathering at $t = \text{Mac } k(\text{Clair text}(9))$.

Decryption computations for permits Block content: $D = t = B_C$

To send data efficiently, just reappearance the verified progress content to protect transactions at the peer end.

Using session requirements to verify the signature establishes validity. This calibration ensures that transactions use both the public and private keys by allocating keys at predefined intervals. Decentralization uses peer-to-peer verification keys to assess proofs and confirm verification. To validate digital signatures and encrypt data, hash indexing techniques rely on HOOK CURVE.

$\text{sign}[(\mathcal{H}: (\mathcal{H}, \text{msg}_1) \rightarrow \{0,1\}^y, \overline{s_k})] \rightarrow \sigma_m$

where s_i – secret key and σ_m r – encrypted Hash

A signature that is digital is an amount..

Verification has characteristics as

Verify session $(n, \sigma_m, p_k) \rightarrow \{0,1\}$

where p_k denotes the public key (11)

$\text{Verf}(n, \sigma_m, p_k) = \begin{cases} 1 & \text{if } \sigma_m \text{ is valid signature } \text{msg}_1 \text{ of under verification key SK} \\ 0 & \text{if not valid} \end{cases}$

Formally, the signature structure = $\{\mathcal{K}, \text{Sign}, \text{Verf}\}$ verifies the digital information by selecting the session time for validating the Encryption and Secret private key to ensure the digital signature.

3.3 One time Padding Encryption Crypto Policy (OTPCP)

Neighboring the nodes cannot get multiple BHs that develop from the exact same data at the same time considering one BH will be the first to be assigned transmission time among each node that caused a block from the same data. However, numerous nodes can simultaneously generate a prevent from the same data at a given time. A node is available to spread the BH to adjacent nodes in its subsequent position after it has produced an actual BH. It can then create a block and add it to a unique copy of the database. Using the recipient's public key for encryption: The recipient's public key, which is obtained from their certificate, is then used to encrypt the OTP-encrypted ciphertext: $\text{Encrypt}(\text{Ciphertext}, \text{Recipient's Public Key}) = \text{Encrypted Cypher Text}$ Confidentiality is thus guaranteed. The sender's private key is used to sign the encrypted ciphertext. This guarantees genuineness and non-repudiation: $\text{Signature} = \text{Sign}(\text{Sender's Private Key}, \text{Encrypted Ciphertext})$. A sign crypted message with the digital signature and the encrypted data is the end result.

$$\mu_{I_x}(a_x) = \frac{a_x - i_x}{y_x - i_x} \text{ for } i_x \leq a_x \leq y_x \quad (1)$$

Where $\mu_{\{I_x\}\{a_x\}}$ is the membership function for feature (a_x) , and (i_x) and (y_x) are the lower and upper bounds of the feature a_x .

Establish a set of one time padding rules that define how the features of the input and the output are related. For example, if have two features a_1 and a_2 , a onetime padding rule might look like:

If a_1 is I_1 and a_2 is I_2 , then b is J

Where I_1 and I_2 are one time padding sets corresponding to the features a_1 and a_2 , and J is the one time padding set for the output b .

To obtain one time padding outputs, apply the one time padding rules to the padding input. The one time padding rules are combined in this step by using logical operations like min, max, etc. The output of each rule Q_i can be computed as:

$$\mu_{J_x}(b) = \min(\mu_{I_1}(a_1), \mu_{I_2}(a_2)) \quad (2)$$

Restore the crisp value to the one time padding output by applying private techniques. The centroid approach is a popular technique that determines the combined one time padding set's center of weight:

$$b = \frac{\sum_{x=1}^N \mu_{J_x}(b) \cdot b_x}{\sum_{x=1}^N \mu_{J_x}(b)} \quad (3)$$

Where b_x are the output values corresponding to each rule Q_x .

Combine the results from the one-time padding inference system to create a model. The equation can be expressed as:

$$\hat{b} = \sum_{x=1}^N h_x \cdot b_x \quad (4)$$

Where h_x is the weight of the x – th rule, often determined:

$$h_i = \mu_{I_x}(a_x) \quad (5)$$

For a simple example with two features a_1 and a_2 the padding equation might look like:

$$\hat{b} = \sum_{x=1}^N (\min(\mu_{I_1}(a_1), \mu_{I_2}(a_2)) \cdot b_x) \quad (6)$$

This method works well for complicated records with a wide variety of data types. This flexibility guarantees thorough examination of various private datasets. This method may improve patient outcomes and boost the effectiveness of services by enabling early diagnosis and prompt intervention through precise analysis of sensitive aspects. In order to promote better solutions and increase the accuracy, robustness, and usefulness of private data analysis approaches offer strong tools for analyzing important aspects of medical records.

3.4 PoA-Ack

The key is validated initially, followed by validation and proof of validity. It turns out that the peer can access the data because of this validity authentication. The master node authentication is shown in Figure 4.

The request Key

$P_B \rightarrow \text{Valid user } V_u$

If verified key is checked during partially synchronized main key verification

$$R \rightarrow \text{At } P_B(V_u) \leftarrow F_q \quad (7)$$

To reach the peer end at the determinate set of blocks, use the elliptic important formulation method.

$P_B(V_u) \leftarrow F_q(\text{Encrypted block})$

Verify the hash index sequence to reorder chain link $H_B \rightarrow P_B(V_u)$

Determine the user key, $KB = H_B \rightarrow P_B(V_u)$, and verify. Proofing of block hash keys

During the session time, check the machine address of the peer block at $t = \text{Mac } k$ (Clair text (9) Permit decryption Calculations Block content $B_C = D = t$

Simply reoccurrence the authorized progress content to safety measure transactions at the peer end in order to send data efficiently.

Step 1: To verify access to V_a , compute the hash-coded blocks.

Test public and private keys by completing a hash key contract to access the block cypher.

Create the partition block order chain connection. Block aggregation is carried out by Cl during the contract.

$$Cl = \int_{i=1}^{\text{size}(Nat)} BL\emptyset(via \rightarrow generate PoA K(ud)[1, n]. set T)$$

Step2: Block L has been chosen for partitioning during split testing.

To link the authentication, divide the data hash code verification and transaction.

Step 3: Hash for all starvation Shk .

$$Sk = \sum(Shk (Key \in K \rightarrow point s) \cup Ekey)$$

Step 4: the divider to create Sk

$Usr \rightarrow$ proofing key for return chain links (Sk)

End

Blocks are categorized by keys based on the identification of significant scenes, which also divides hash keys. Because crypto blocks are closely linked, keys can be safely stored without being aware of the key sequence for a particular block. This divided block structure fortifies Chain Link's security approach and improves transaction verification dependability.

3.5 Hook Curve Revised Hash Authentication (HC-RHA)

Hook Curve Revised Hash Authentication verification analysis the secure data with scalability, security and authentication. Auditing user and end users will discover the Hook Curve key authentication system to be user-friendly. The secure end users don't need complex passwords or security measures efficiently authenticate using the private keys.

The Hook Curve Revised Hash Authentication Key Authenticator is an effective for verification using centralized master node for a high level of security, scalability, and user-friendliness. Using Hook Curve Key authentication and data are safe from attacks and unauthorized access.

Message m , receiver ID_r , and set $R = L \cup \{T_i: ID_i \in L\}$, where $L = \{ID_1, \dots, ID_n\}$ is the collection of n users' IDs, are selected by A_1 and sent to C . The ciphertext σ is returned to A_1 by C . This algorithm uses a (t, n) Hook curve mechanism, where $n > 2t-1$. Assuming that $\{U_1, U_2, \dots, U_n\}$ is a collection of n signcrypters, the key distributor performs the subsequent actions: (1) Select $b_1, b_2, \dots, b_{t-1}$ at random, and create a $(t-1)$ -degree polynomial: (2) Determine $s_i = f(i)$, where $i = 0, 1, \dots, n$, and $s_0 = x_D$; $f(x) = s_0 + b_1x + \dots + b_{t-1}x^{t-1}$; (3) Deliver s_i to each signcrypter U_i in secret ($i \in \{1, 2, \dots, n\}$); (4) Send $y_0 = g^{s_0}$.

$$e(g, y_0) = e(y_{pub}, \xi_r) \prod_{j=0}^{t-1} e(g, y_j)^{j^t} \quad (8)$$

Here, can easily explain that each signcrypter's key sharing is right. U_i ($i \in \{1, 2, \dots, n\}$) by the verification process as follows:

$$\begin{aligned} e(g, y_0) &= e(g, g^{s_i} d_D) \\ &= e(g, d_D) e(g, g^{x_D + ib_1 + \dots + i^{t-1} b_{t-1}}) \\ &= e(y_{pub}, \xi_r) e(g, u_D) e(g, g^{ib_1}) \dots e(g, g^{i^{t-1} b_{t-1}}) \\ &= e(y_{pub}, \xi_r) \prod_{j=0}^{t-1} e(g, y_j)^{j^t} \end{aligned} \quad (9)$$

Here, the correctness of unsigncryption algorithm can be easily proved by the following verification process,

$$\begin{aligned} \kappa &= e(v, \xi_r) \\ &= e\left(\prod_{i=1}^t (y_r y_{pub})^{\mu_i}, \xi_r\right) \\ &= e(r, \xi_r^{x_r} d_r) \\ e(g, h) &= e\left(g, d_D \prod_{i=1}^t h_i\right) \\ &= e(g, d_D) e\left(g, \prod_{i=1}^t \varphi^{\mu_i}\right) e\left(g, \prod_{i=1}^t g^{\eta_i s_i}\right) \\ &= e(y_{pub}, \xi_D) e(r, \varphi) e\left(g, g^{\sum_{i=1}^t \eta_i s_i}\right) \\ &= e(y_{pub}, \xi_D) e(r, \varphi) e(g, u_D) \end{aligned} \quad (10)$$

A Hook Curve master key is required for authentication of this encrypted rate.

Initialize (I_p)

Identity blocks

Select $x, y \in Z_a^*$

Calculates block key (CBK) X and Y

$X = xK, Y = yK$

$M = Enc_{sk}(X||Y) \xrightarrow{m} \text{decrypting } (m) \text{ to } X, Y = Dec_{sk}(m)$

Generates Ack key (δ) = $Ack_{Key pk_m}(X||Y)$

Encrypts $\delta, X, Y, \zeta_k = Enc_{sk}(\delta||X||Y)$

ζ_k
 $\rightarrow$ decrypts (d) to obtain $\delta = Dec_{sk}(\zeta_k)$
 Verifies block key δ

If the block key δ is valid, then saves X, Y

An important example of addition-based security in Block computing is shown in the proposed block diagram. Master nodes are encrypted from the start to provide secure access. HC-MNKA is used to evaluate the outcomes of blockchain network transactions in Block and IoT platforms. The Pre-Ack distributed chain examination of node behaviour inside mutual trust is initially fed this text file. A Hook Curve master key is used for authentication in addition to encryption.

$$MTP \rightarrow PoA : Mi, R, M.T., H3(PSK1 || RPoA) \quad (11)$$

The procedure is primarily identified by the reliable MTP and the alternative key Sk . Also known as the code of silence. If the force is not confirmed, estimate the evolution key εk^* as being most similar to a random integer.

x is equivalent to RMT.

Additionally, there are no more a fragmented process of consolidation for merged interaction. MT constructs session key $PSK1$ using the static access key mentioned below..

$$PK_{Pack} = Pk_2 + H_1(id_{pack} || Pk_2) Pk_1 \quad (12)$$

$$K_1 = s_{ack} k_{pack} + Pk_a \quad (13)$$

$$PSK_1 = H_2(pid_k || PSK_{PoA}) \quad (14)$$

The hash step of the function is retained in all algorithm expressions and is denoted by $PK1$ and PoA as the authentication values. Figure 2 demonstrates the process of verification and analysis.

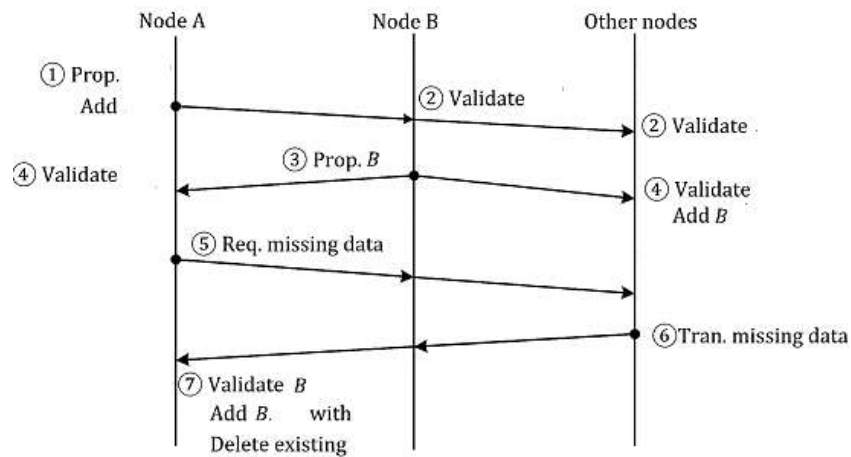


Figure 2 Hook Curve Revised Hash Authentication verification analysis

- One of the nearby nodes, Node B, adds $BK(i)B$ to its existing BCB and propagates $BH(i)B$. The neighbors of node B that received $BH(i)B$ confirm the BH and add $BK(i)$ to their respective BCs with $BH(i)B$ as its header. However, by comparing $BDI(i)A$ with $BDI(i)B$, node A verifies the missing data.

- Node A asks nearby nodes to retransmit the missing information.
- The lost data is retransmitted to node A by nearby nodes.
- Node A confirms BH(i)B after receiving all missing data. Figure 3 depicts the workflow of the entire algorithm.

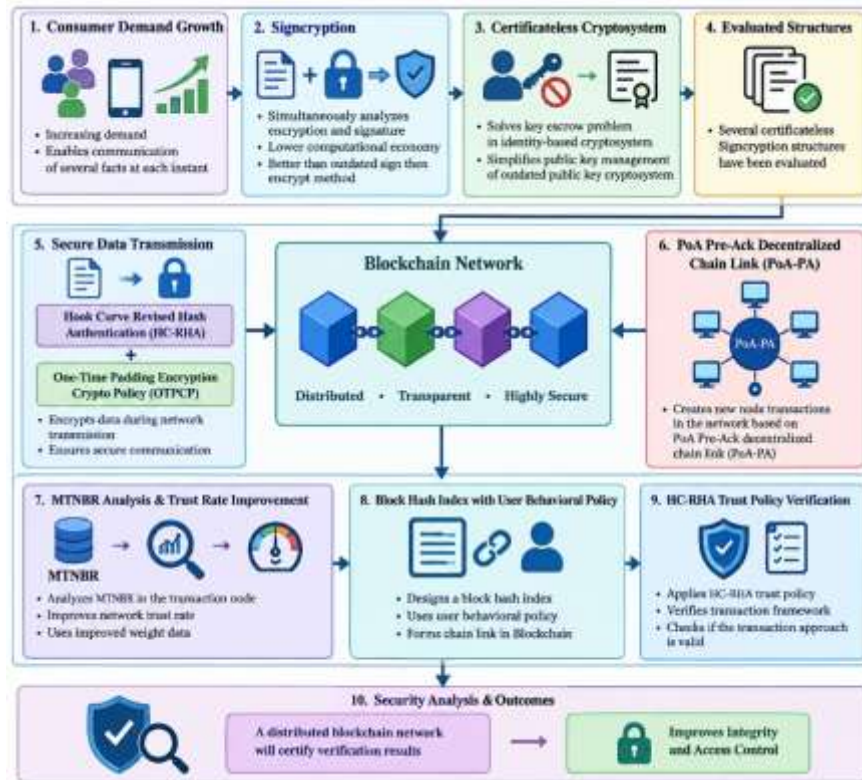


Figure 3: Overall workflow of the proposed work

4. Result and discussion

This section provides the outcomes of prospective tests conducted using the Visual Studio graphical tools and the C#.net programming language. In the tables containing the test and validation datasets, enter the settings and values required to reproduce the blockchain ecosystem. By comparing the suggested approach with previous approaches, the performance tests evaluate average latency, decryption and encryption, standard times, and performance in terms of security.

Proposed implementation test platform is defined by a methodology for evaluating system efficacy. This implementation uses SQL Server authentication and is operated by Visual Studio Framework 4.0. Tested this setup using an Intel i5 processor and 4GB of RAM. A significant obstacle in several domains, such as the military, Internet use, and banking, is information security. There is another network location in front of the file. Many hackers gain unauthorized access to data. The process of converting cypher text is referred to as encryption time, or cypher text decryption time in plain text. Several researchers used a range of approaches and techniques in an effort to overcome this problem. A novel block service for encryption and removal. False events occur during both the encryption and decryption states, or states of verification at the service level of integrity during the key failed state. The algorithm has enough intelligence to help categorize the encryption process at multiple levels of encryption. It takes some time to decode, but the recommended approach encrypts and provides extra protection. The size of the information and the processing mechanism determine how long it takes to encrypt it. At the time that Clair material was changed, the crypto policy security standard was in effect. The recommended approach speeds up data processing and improves security by preventing hackers from taking advantage of the system

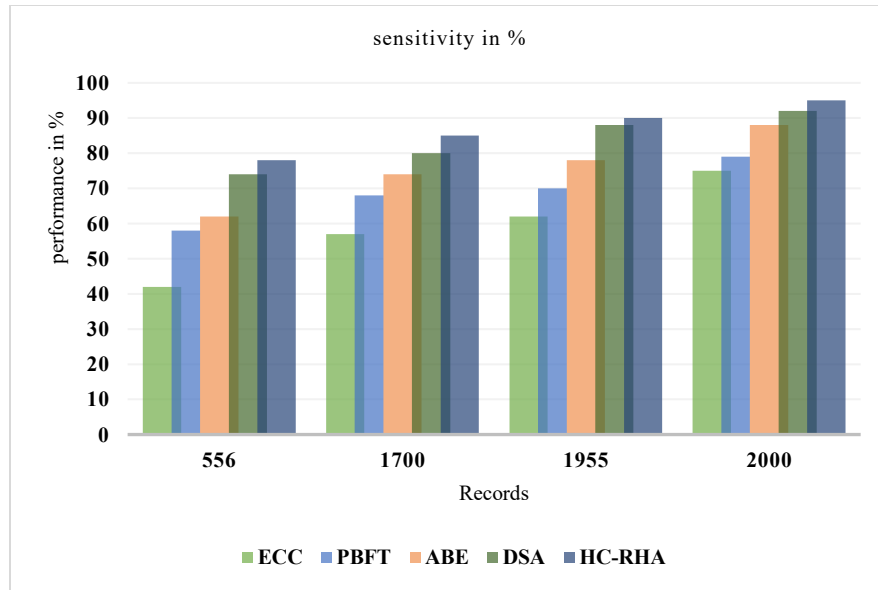


Figure 4: Sensitivity performance

The most effective weight is compared to the positive field to forecast the sensitivity accuracy in figure 4. The sensitivity weight is the proper proportion of the threshold margin caused by sensitivity bias. The best results obtained under various testing levels suggest that the HC-RHA system forecasts the ultimate sensitivity terms. In contrast to other systems, it provides the best performance ratio. The proposed method HC-RHA achieved 95% and compared existing method Certificate less Signcryption 92% of DSA, ABE 88%, PBFT 79% and ECC is 75%.

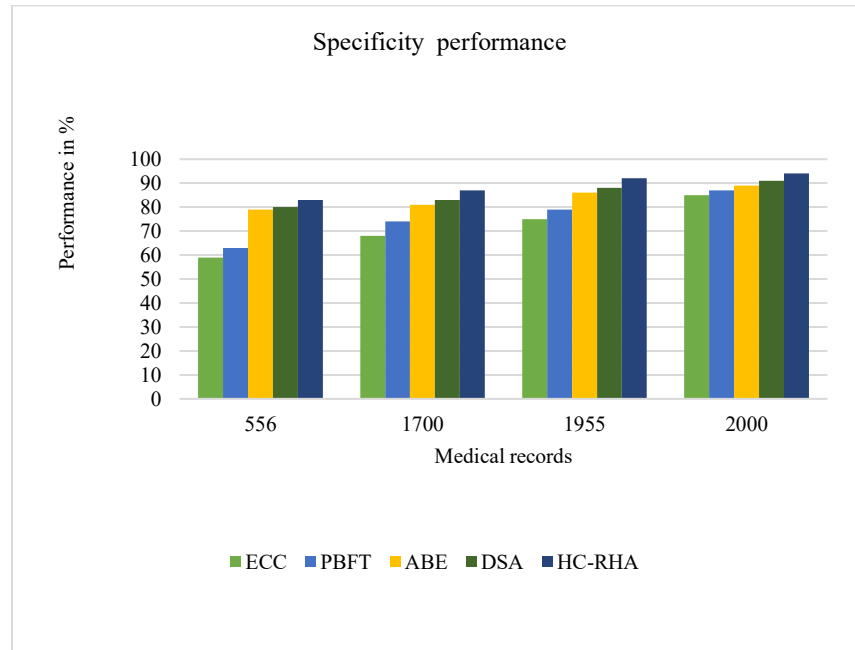


Figure 5: Specificity performance

Marginal Specificity weights are the basis of weights of feature analysis, and the most accurate weights are compared to positive fields to forecast the Specificity accuracy. Finally, as demonstrated in Figure 5, the proposed system predicts sensitive items with outstanding results at different registration levels assessed by existing approaches. The proposed method HC-RHA achieved 94% and compared existing method Certificate less Signcryption 91% of DSA, ABE 89%, PBFT 87% and ECC is 85% using 2000 records.

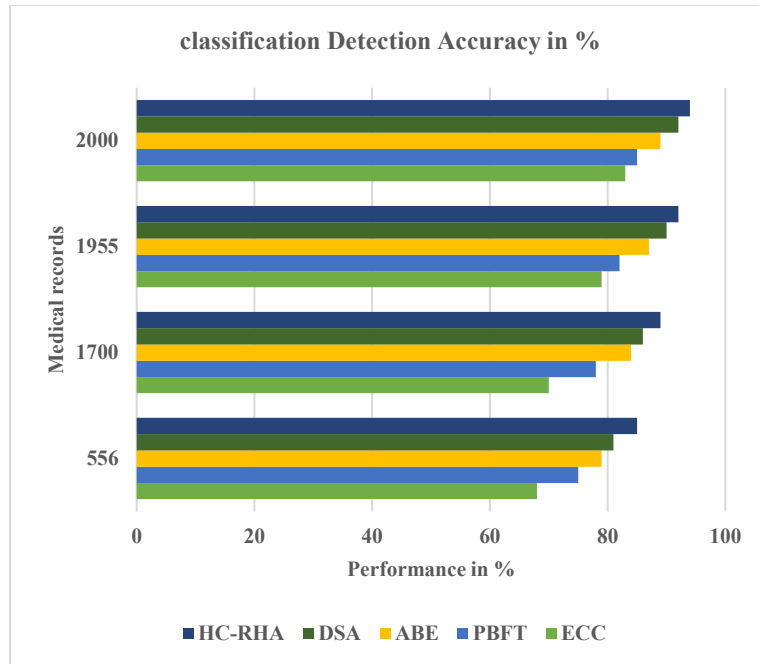


Figure 6: The classification detection accuracy

The detection accuracy values for contrasting the various approaches are shown in Figure 6. When compared to alternative algorithms, the suggested implementation performs better. The proposed method, HC-RHA, is 94% and has a higher detection accuracy than the prior approaches, 92% of DSA, ABE 89%, PBFT 87% and ECC is 85% using 2000 records.

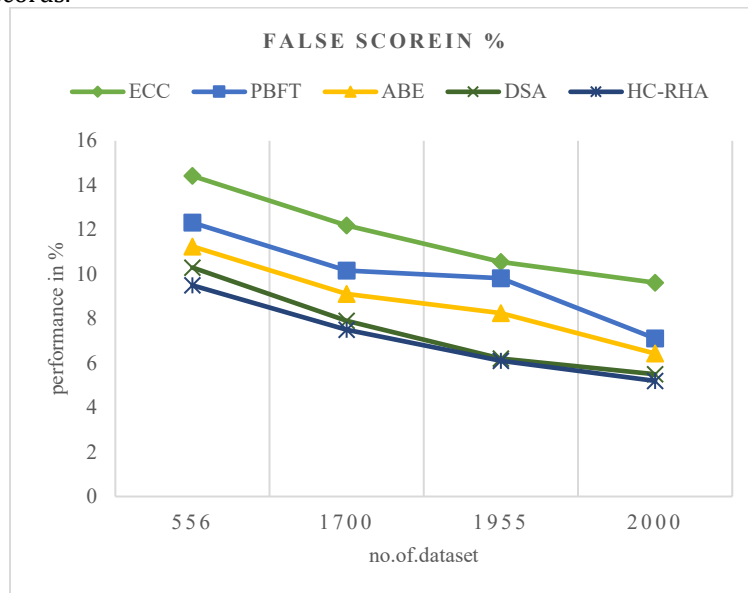


Figure 7: False Score accuracy

In Figure 7, the recommended method performs better than the others regarding error scores. The compromised data is included in the role-based access policy through the encrypted policy imposed by the proposed HC-RHA. Users in the Block environment create access requests, request files based on test ratings, and verify accuracy through security checks. Subsequently, Block policies confirm access requests and provide essential features that improve security.

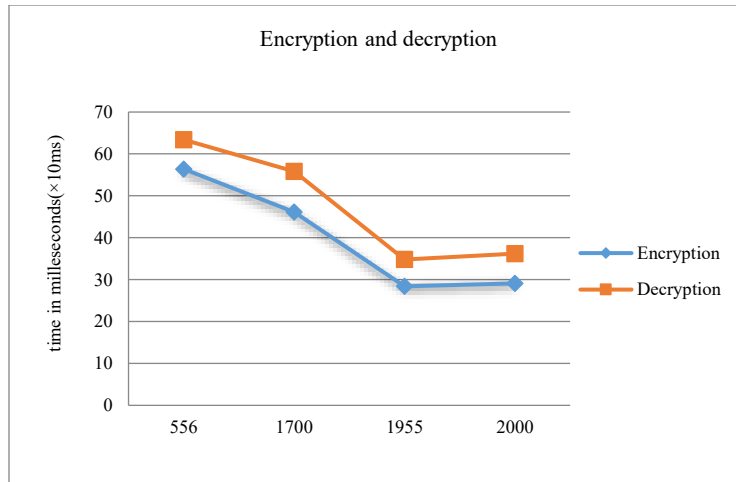


Figure 8: Execution efficiency

The improved decryption and encryption standard performance for lock chain security is estimated using the overall mean period. Both this identified execution and the prior system yield outstanding outcomes. The suggested evaluation and execution efficiency comparison of several approaches are shown in Figure 8.

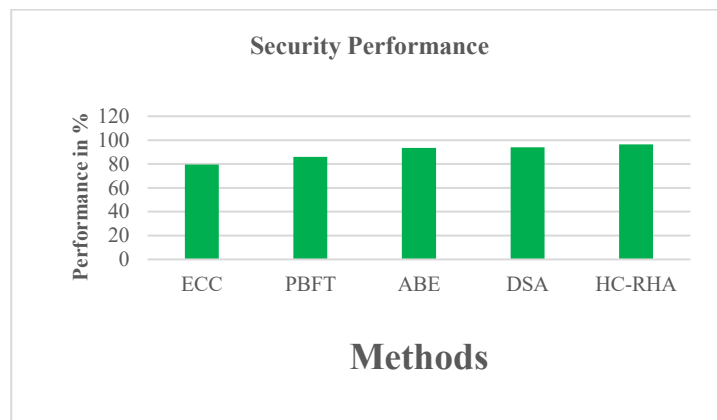


Figure 9: Comparison of security analysis efficiency

The technique is evaluated at various user and owner dependence levels using the security monitoring approach before access permissions are provided. The comparison of security analysis efficiency is displayed in Figure 9. To optimize security, the HC-RHA operates at the best encryption policy-based Blockchain transmission level.

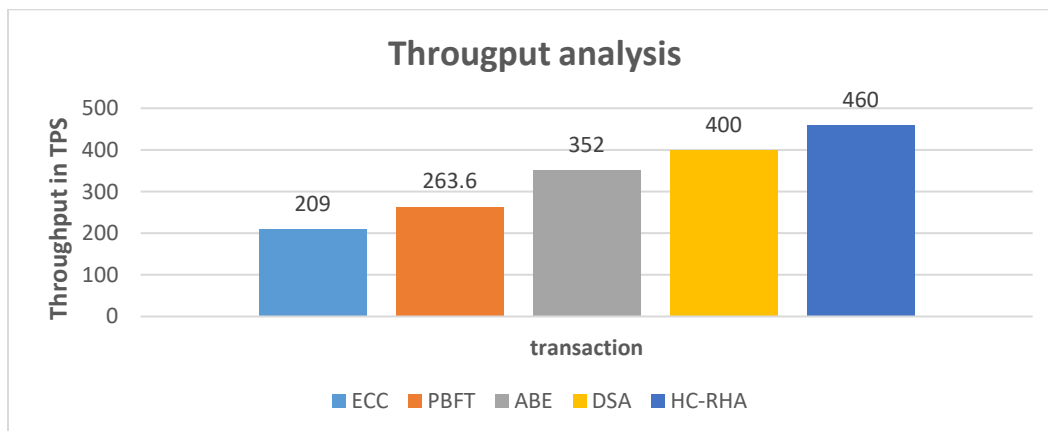


Figure 10: Comparison of throughput Analysis

Figure 10 shows an assessment of the throughput analysis and HC-RHA approach has a 460tps higher activity throughput rate than other current techniques, according to this analysis of the suggested methodology. Block Certificateless Signcryption, which has quick encryption and a short validation a period of time is the foundation of the HC-RHA to authenticate each user request transaction, increasing the throughput rate over alternative techniques.

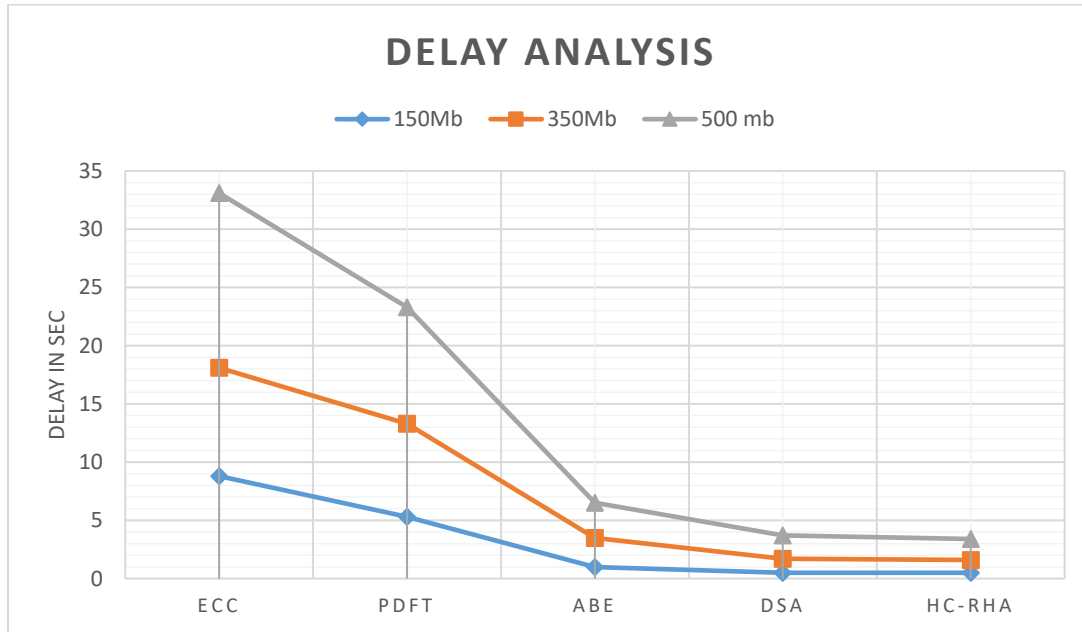


Figure 11: Comparison of Authentication Delay Analysis

In figure 11, the proposed solution depicts the exceptional performance of higher-end security with the minimal authentication delay of a typical crypto blockchain. The proposed approach validates each user policy agreement before providing permission to use the database. For 500MB of data, the proposed, HC-RHA conduct has a low authentication delay of 1.8 seconds.

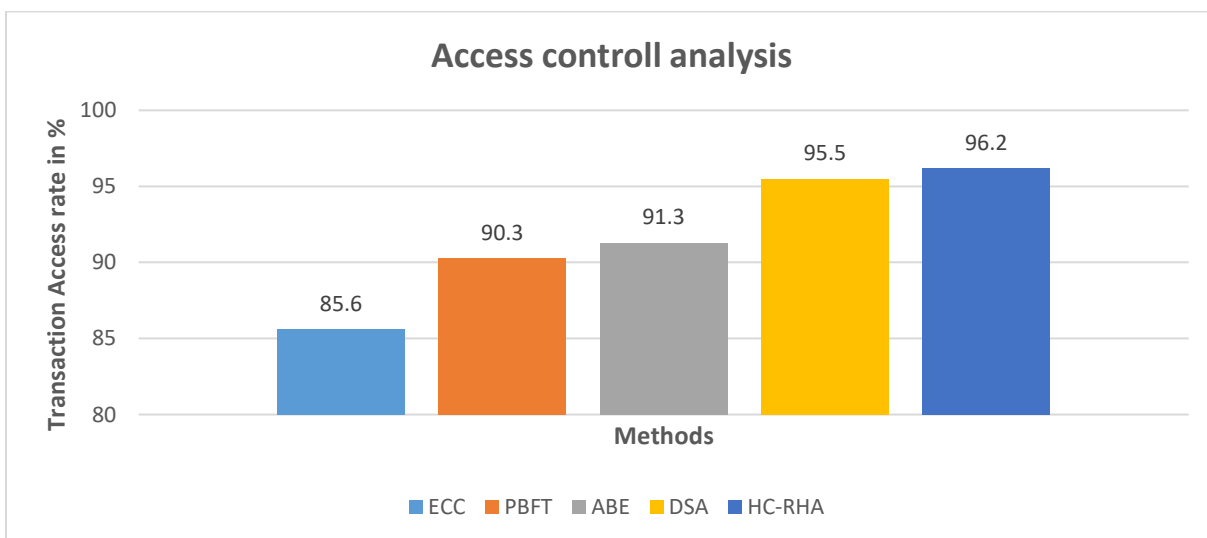


Figure 12: Comparison of Access control Analysis

In this transaction, the access rate is determined by the user accessing the data without interruption and retrieving from a Block database. The proposed HC-RHA method has a 96.2% transaction access rate compared to another existing method. This comparison is shown in Figure 12. The existing system provides permission for Block users at 95.5% of access control in a Block server.

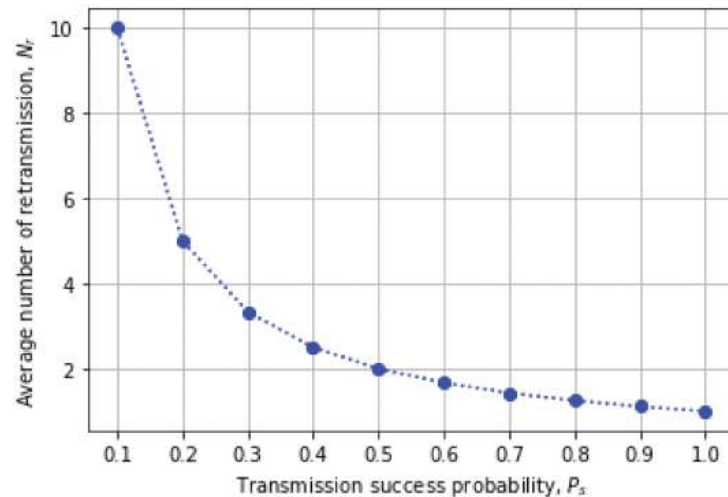


Figure 13: Transmission Possibility

To create an authorised block in the suggested system, nodes must receive all of the data in a block. Energy is used when a node asks a neighbour node to retransmit data that hasn't been received. The average number of retransmissions needed before a node successfully receives a packet is examined in this subsection. When sending data to the node with the worst channel conditions, let P_s be the transmission success probability. Nodes that were unable to receive the packet would send a request for retransmission to the transmission node. Until every neighbour node successfully receives the packet, the transmission node sends calculating the average number of retransmissions. As shown in figure 13

5. Conclusion

In this paper, a blockchain system for certificate-less encryption based on HCRHA is proposed. The suggested solution assigns nodes timeslots based on how they contribute to the blockchain's functionality. This implies that nodes that contribute well are exempt from competing to create the block header. Furthermore, at each node, block formation is carried out from the received header, and just the block header is transmitted. a blockchain-based certificateless sign encryption system. This approach can ensure signature nonrepudiation, stop unauthorised people from using the user's public key, and effectively utilise the nontamperable feature of the blockchain. The findings of a comparative investigation show that our plan has improved in terms of security and efficiency. Signcryption is the least computationally intensive technique, making it ideal for the blockchain.

Reference

1. T. -T. Tsai, Y. -M. Tseng and S. -S. Huang, "Leakage-Resilient Certificateless Signcryption Scheme Under a Continual Leakage Model," in IEEE Access, vol. 11, pp. 54448-54461, 2023, doi: 10.1109/ACCESS.2023.3281612.
2. Y. Zhou, R. Xu, Z. Qiao, B. Yang, Z. Xia and M. Zhang, "An Anonymous and Efficient Multimessage and Multireceiver Certificateless Signcryption Scheme for VANET," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22823-22835, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3305489.
3. H. Yu, L. Bai, M. Hao and N. Wang, "Certificateless Signcryption Scheme from Lattice," in IEEE Systems Journal, vol. 15, no. 2, pp. 2687-2695, June 2021, doi: 10.1109/JSYST.2020.3007519.
4. X. Chen, D. He, M. K. Khan, M. Luo and C. Peng, "A Secure Certificateless Signcryption Scheme Without Pairing for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 10, no. 10, pp. 9136-9147, 15 May15, 2023, doi: 10.1109/JIOT.2022.3233180.
5. L. Cao, Y. Liu and S. Cao, "An Authentication Protocol in LTE-WLAN Heterogeneous Converged Network Based on Certificateless Signcryption Scheme with Identity Privacy Protection," in IEEE Access, vol. 7, pp. 139001-139012, 2019, doi: 10.1109/ACCESS.2019.2941913.
6. J. Zhang, C. Dong and Y. Liu, "Efficient Pairing-Free Certificateless Signcryption Scheme for Secure Data Transmission in IoMT," in IEEE Internet of Things Journal, vol. 11, no. 3, pp. 4348-4361, 1 Feb.1, 2024, doi: 10.1109/JIOT.2023.3298840.

7. Ullah, A. Alkhalifah, S. U. Rehman, N. Kumar and M. A. Khan, "An Anonymous Certificateless Signcryption Scheme for Internet of Health Things," in IEEE Access, vol. 9, pp. 101207-101216, 2021, doi: 10.1109/ACCESS.2021.3097403.
8. Z. Xie, Y. Chen, I. Ali, C. Pan, F. Li and W. He, "Efficient and Secure Certificateless Signcryption Without Pairing for Edge Computing-Based Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 72, no. 5, pp. 5642-5653, May 2023, doi: 10.1109/TVT.2022.3230442.
9. C. Dai and Z. Xu, "Pairing-Free Certificateless Aggregate Signcryption Scheme for Vehicular Sensor Networks," in IEEE Internet of Things Journal, vol. 10, no. 6, pp. 5063-5072, 15 March 2023, doi: 10.1109/JIOT.2022.3222237.
10. G. Srinivasa Rao, G. Thumbur, R. B. Amarapu, G. N. Bhagya and P. V. Reddy, "A New Lightweight and Secure Certificateless Aggregate Signcryption Scheme for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 11, no. 6, pp. 10563-10574, 15 March 2024, doi: 10.1109/JIOT.2023.3327503.
11. 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.
12. P. Kang, Y. Wenzhong and T. Ding, "Blockchain Document Forwarding and Proof Method Based on NDN Network," in IEEE Access, vol. 10, pp. 75312-75322, 2022, doi: 10.1109/ACCESS.2022.3178992.
13. E. Zeydan, S. S. Arslan and Y. Turk, "Exploring Blockchain Architectures for Network Sharing: Advantages, Limitations, and Suitability," in IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 1791-1801, April 2024, doi: 10.1109/TNSM.2023.3331307.
14. S. Shao, W. Gong, H. Yang, S. Guo, L. Chen and A. Xiong, "Data Trusted Sharing Delivery: A Blockchain-Assisted Software-Defined Content Delivery Network," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 11949-11959, 15 July 2023, doi: 10.1109/JIOT.2021.3124091.
15. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.
16. 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.
17. M. I. Khalid et al., "A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks," in IEEE Access, vol. 11, pp. 10995-11015, 2023, doi: 10.1109/ACCESS.2023.3240237.
18. 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.
19. 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.
20. J. Lee and M. Lee, "A Blockchain System for TDMA-Based Tactical Wireless Networks with Constrained Resources," in IEEE Access, vol. 11, pp. 6857-6866, 2023, doi: 10.1109/ACCESS.2023.3237828.
21. G. Xu, J. Dong, C. Ma, J. Liu and U. G. Omar Cliff, "A Certificateless Signcryption Mechanism Based on Blockchain for Edge Computing," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 11960-11974, 15 July 2023, doi: 10.1109/JIOT.2022.3151359.
22. C. N. A. Cobblah, Q. Xia, J. Gao, H. Xia, G. A. Kusi and I. A. Obiri, "A Secure and Lightweight NDN-Based Vehicular Network Using Edge Computing and Certificateless Signcryption," in IEEE Internet of Things Journal, vol. 11, no. 16, pp. 27043-27057, 15 Aug. 2024, doi: 10.1109/JIOT.2024.3399031.
23. Jin, Y., Ye, C., Yang, M., Ye, C. (2022). One-Time Anonymous Certificateless Signcryption Scheme Based on Blockchain. In: Gao, H., Wang, X., Wei, W., Dagiuklas, T. (eds) Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 460. Springer, Cham. https://doi.org/10.1007/978-3-031-24383-7_29
24. ZHANG Tian-xi, WANG Li-peng, FU Jun-jun, CUI Ci, JIN Meng-lu. Certificateless Signcryption Scheme Based on Blockchain[J]. Computer and Modernization, 2022, 0(01): 120-126.
25. C. Jiang, X. Li, D. Du, L. Wu and R. Findeisen, "Cross-Domain Authentication Scheme Based on Distributed Two-Layer Collaborative Blockchains for Cyber-Physical Power Systems," in IEEE Internet of Things Journal, vol. 11, no. 10, pp. 17468-17481, 15 May 2024, doi: 10.1109/JIOT.2024.3359509.