International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

Secure Data Transactions based on Hash Coded Starvation Blockchain Security using Padded Ring Signature-ECC for Network of Things

V.Vijayalakshmi[1] , Dr.K.Sharmila[2]
[1]Research Scholar, Department of Computer Science,
VISTAS, Chennai – 600117.
vijisribangaru@outlook.com
[1]Assistant Professor, Department of Computer Applications,
Lakshmi Bangaru Arts and Science College, Melmaruvathur, Tamilnadu – 603319.
[2]Research Advisor and Associate Professor, Department of Computer Science,
VISTAS, Chennai – 600117.
sharmila.scs@velsuni.ac.in

Abstract—Blockchain is one of the decentralized processes in a worldview that works with parallel and distributed ledger technology, the application process, and service-oriented design. To propose a Secure data Transaction based on Hash coded Starvation Blockchain security using Padded Ring signature-ECC for Network of Things. Initially, the crypto policy is authenticated based on the user-owner shared resource policy and access rights. This creates a Public blockchain environment with a P2P Blockchain network. The owner encrypts the data using optimized ECC through Hash-coded Starvation Blockchain security (HCSBS). This makes the encrypted block's provable partition chain Link (P^2CL). The encrypted blocks are transmitted into the network of nodes monitored by NoT. During the data transmission, the Network of Things monitors the transaction flow to verify the authenticity over the network of nodes. The monitored data be securely stored in transaction Block storage with the hash-indexed block with chain ring policy (HICLP). This creates controller node aggregation over the transaction environment to securely transfer the data to the peer end. The User gets the access Key to decrypt the data with policy aggregated shared resource policy to access the data. The proposed system produces high security as well compared to the previous design.

Keywords—Blockchain security; ECC cryptography; Padded Ring signature; controller node policy; Network of things.

I. INTRODUCTION

A blockchain is a tremendous approach for securing data transactions in a decentralized network environment [1]. Blockchain offers a secured technological revolution to the network of things by monitoring the secured data transaction under verification validation and authentication with fewer infrastructure costs with virtualized resources and storage remaining highly secure in network data transmission [2]. Although in a decentralized network storage transaction environment, security breaches are periodically raised due to transmission attacks, cryptographic failures, transmission deficiency, etc. To analyze the limitations of traditional centralized solutions with blockchain networks based on Proof of work [3]. To find Blockchain based solution. To resolve this problem, we propose an advanced crypto policy using Proof of employment (e-pow) consensus Blockchain-based secured data transmission in a cloud network of things (C-NoT) [4].

The proposed approach is entirely based on a high transaction flow rate collected as a dataset previously extracted from a model for the blockchain network. The test results show that the Proof of Authenticity (PoA) and Proof of Validity (PoV) consensus approach is suitable for detecting intruders and the authenticity of the users involved in the blockchain network to distribute the healthcare documents on the distributed ledger for sharing and verifying the certificates [5]. The outcomes suggest calculating the accuracy of the fake detection using a consensus mechanism and smart contract.

The main contribution of the proposed work is to improve the secured data transaction flow rate and collect block-based transaction data storage with advanced crypto-secured policy in the Blockchain network. This works on the principle of Proof of Authenticity (PoA) and Proof of Validity (PoV) in the Proof of Work (E-PoW) consensus approach for detecting intruders and authenticity of the users who are involved in the Blockchain network during the network data packets accessibility.

The main objective of the proposed system is to improve Blockchain security based on secured data transmission in a cloud network of things. To suggest a secure data Transaction based on Hash coded Starvation Blockchain security using Padded Ring signature-ECC for Network of Things. Initially, the crypto policy is authenticated based on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

the user-owner shared resource policy and access rights. This creates a Public blockchain environment with a P2P Blockchain network. The owner encrypts the data using optimized ECC through Hash-coded Starvation Blockchain security (HCSBS). This makes the provable partition chain Link (P^2CL) for an encrypted block. The encrypted blocks are transmitted into the network of nodes monitored by NoT. During the data transmission, the Network of Things monitors the transaction flow to verify the authenticity over the network of nodes. The monitored data be securely stored in transaction Block storage with the hash-indexed block with chain ring policy (HICLP). This creates primary node aggregation over the transaction environment to securely transfer the data to the peer end. The User gets the access Key to decrypt the data with policy aggregated shared resource policy to access the data. The proposed system produces high security as well compared to the previous design.

Finally, security analysis shows that a decentralized blockchain network will the traditional centralized audit, publishing and certifying verification results, and improving transparency and security.

II. RELATED WORK

The literature previews prior contributions to the subject of study and aids in giving the new generation of researchers**.** The different methods proposed in the literature to address the duplicate detection issue and prevent the issuance of fraudulent certificates are discussed in this chapter**.**

Blockchain-Aided Searchable Attribute-Based Encryption (BC-SABE) is proposed [6] to secure the authentication of every user data. To solve these problems, Blockchain is used to present a cloud computing-assisted security authentication protocol and access control. Hence, Attribute-Based Ciphertext Policy Encryption is to be used (CP-ABE) [7] to apply Blockchain to establish access control to health data stored on cloud servers and ensure data integrity.

To enable secure and efficient keyword search, it has designed a forward and backward privacy (BSPEFB) [8] scheme based on the new Blockchain-Based Searchable Public-Key Encryption Scheme With forwarding And Backward Privacy (BSPEFB) [9] system using smart contracts to verify the accuracy and integrity of search results, and automatically search for proper payment operations to execute. An efficient dynamic audit protocol for cloud storage has many excellent features to solve this problem. One way to ensure cloud computing is to use machine learning (ML) [10].

ML technology has been used to prevent or discover attacks and security vulnerabilities in the cloud. The transaction contract [11] is vulnerable to data privacy behaviour attacks. It will configure compliance challenges and third-party damage audits. It can get the owner of all the data that outsources it [12]. Our new scheme combines the Ethereum blockchain with ciphertext-policy attribute-based encryption (CP-ABE). The existing blockchain network cannot be compared to a decentralized network as it does not access data from a private channel [13].

Ternary Hash Tree Based Integrity Verification (THT-IV) [14, 15] Using blockchain technology, digital degrees and mark cards are possible. Online access to digital degree certificates reduces costs and saves time [16]. The ability to obtain a copy of the original mark card or certificate online in the event of loss or damage to the originals offers great flexibility [17].

Security risk assessment approaches (such as asset-based) need to consider the specific security needs of individual cloud computing clients in security risk assessment [18]. Public audit protocols are essential to the success of cloud computing because they can prevent the outsourcing data of cloud servers from being corrupted [19].

Using distributed ledger technology such as Blockchain to authenticate feedback services can create distributed systems to enable customers to interact with system operators and provide secure, transparent, and detectable flexibility [20]. Blockchain technology also supports the motivation mechanism for users to participate in the service by generating utility tokens and recognizing their contributions.

III. PROPOSED WORK

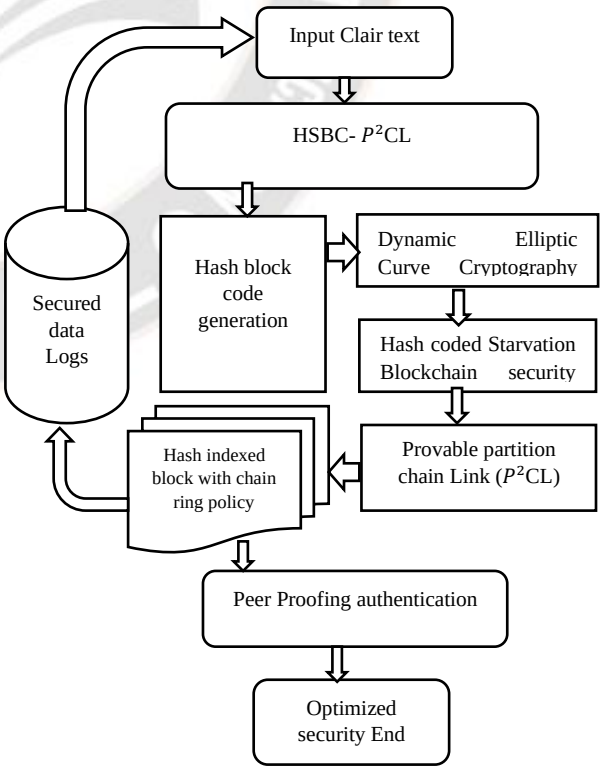

Figure 1. Architecture diagram for the proposed system

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

The proposed system works on the principle of Proof of Authenticity (PoA) and Proof of Validity (PoV) in the Enhanced-Proof of Work (E-PoW) consensus approach for detecting intruders and authenticity of the users involved in the Blockchain network during the network data packets accessibility. The development crypto policy is authenticated based on user-owner shared resource policy and access rights. This creates a Public blockchain environment with a P2P Blockchain network. The owner encrypts the data using optimized ECC through Hash-coded Starvation Blockchain security (HCSBS). This makes the encrypted block's provable partition chain Link (P2CL). The encrypted blocks are transmitted into the network of nodes monitored by NoT.

During the data transmission, the Network of Things monitors the transaction flow to verify the authenticity over the network of nodes. The monitored data be securely stored in transaction Block storage with a hash-indexed block with a chain ring policy (HICLP). This creates primary node aggregation over the transaction environment to securely transfer the data to the peer end. Fig 1: Architecture diagram for the proposed system. The dynamic elliptic curve is cryptographic to authenticate user-profiles and encrypt the cloud data using Padded Ring signature-ECC is an essential public encryption technology with optimized blockchain principle. The group uses specific key agents and analyzes alerts to take keys generated from different agents on field-based cloud servers.

A. Police Adapted Dynamic Elliptic Curve Cryptography (PA-DECC)

Dynamic elliptic curve cryptography enrolls the security policy based on finite set field block encryption F_p having the relational sequence of 256 block level. The limited set parameters a, b $\in$ F_p (a, b) points to the sinusoidal wave in elliptic curve $4a^3 + 27b^2 \neq 0$ representing two consecutive points (x, y) $\in$ F_p. The curve-pointed tangent slope at $y^2 = x^3$ + axe + b in random sequence sets the points E_c (F_p) with the addition midpoint ***O.*** The arbitrary point creates a group of blocks by plotting different cure points dynamically to create block-level encryption.

The elliptic curve $E_c \rightarrow P + O$ pointing line P at (x, y) in finite point Fp

Single point block level plotted curve,

$E_c \rightarrow \sum_P^N (x, y)\ \forall P \in E(Fp)$, likewise $O = P + Q$,

The positive and negative acute angle of the projection point is represented as

p(x, y) is E_c (F_p) at $P(E_c)$

Similarly,

p(x, -y) is E_c (F_p) at $P(E_c)^T$

Let's the dynamic point P = E_c (Ex, Ey) $\in$ E_c (Fp), then (Ex, Ey) + (Ex, – Ey) = O is the negative opinion inverse to the actual slope point.

If the dynamic curve at elliptic projection creates single Block 'B' only at in finite set block is E_c (F_{BP}) sequentially,

P$\rightarrow$$(Ex_1, Ey_1)$, (Ex_2, Ey_2) $\in$ E_c (F_{BP}) creates otherwise $(F_{BP})^T$

This dynamic elliptic curve hides the block-level encryption sequence order relations, virtually making a point of crucial projection in the hash indexing policy.

So the sequence order be,

E_c (F_{BP}) P$\rightarrow$$(Ex_1, Ey_1)$ $\in$ E(F_p) and E_c (F_{BP}) Q$\rightarrow$$(Ex_2, Ey_2)$ $\in$ E(F_p) to hide the intersection of the block.

The absolute rate of the following sequence block having the information, P $\neq$ Q at R = P + Q = (x_3, y_3)) $\in$ E_c (F_{BP}) by creating a hiding sequence where x3 = λ2 – Ex1 – Ex2, Ey3 = λ (Ex1 – Ex3) – y1, and λ = (Ey2 – Ey1) / (Ex2 – Ex1),

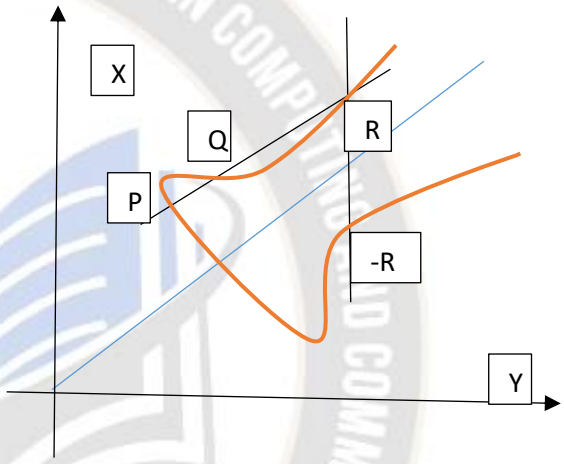

Figure 2. Addition of 2 points P and Q on the curve $y^2 = Ex^3 – 3Ex + 3$

To create multiplicative point block level encryption using doubling point elliptic curve encryption pointed at tangent slope P$\rightarrow$ $2(Ex_n, Ey_n)$) $\in$ E_c (F_{BP}) at random 'n' level blocks Ex1 = λ2 – 2Ex, E y1 = λ (Ex – Ex1) – y, where λ = (3Ex2 + a) / 2Ey. In addition, E_c $2(F_{BP})^T$ inversion-based double squaring and 4*2 addition shifting was carried from 256-bit block-level encryption.

The dynamic block-level ECC creates doubling state E_c $2(F_{BP})$$\rightarrow$ R = P + Q under block level closure, associative level block encryption with identity key element for Hash pointing with inverse transformation.

The block level closure in tangent slope is formulated as,

$\forall$EP, EQ $\in$ E(F)P, if ER = BlockLevel (P) + asciative level (EQ), then ER $\in$ E(Fp), (1)

The associative level block encryption in Elliptic point $EP + (EQ + ER) = (EP + EQ) +$ ER, $\forall$EP, EQ, ER $\in$ E(Fp), the represented key element is $IDE \rightarrow \exists EO \in E(Fp), such\ that\ \forall EP \in E(Fp), EP + EO = EO + EP = EP,$ (2)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

To hide the non-nature of data encryption based on an inverse definition.

$$\forall \mathrm{EP} \in \mathrm{E(Fp)}, \exists - \mathrm{EP} \in \mathrm{E(Fp)} \longrightarrow IDE^{T}$$

The block is a non-sequentially identity to maintain the hash pointer to improve the security in blockchain principle. This supports block-level information associatively to generate the key based on the relational block one over the other sequence to enhance the ECC in dynamic block level to protect the data.

B. Hash coded Starvation Blockchain security (HCSBC)

The starvation creates cross-matrix endpoint blocks in which the encrypted content is routinely hash-coded into random blocks. These blocks are pointed only by endpoint conjunction end with mutual points. This contains the information but the previous block information and following coordination block information which is not unique to identify the originality of the encrypted content sequence. Bu the identity was not intended to collaborate with other blocks to maintain the series through hash codes secretly.

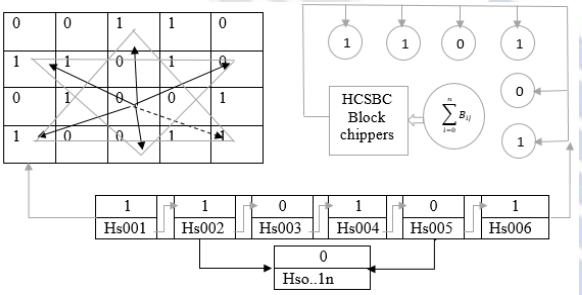

Figure 3. Hash-coded Starvatio Blockchain security

Creating Random blocks by attaining $Bc \leftarrow \{0,1\}. If\ Bc = 0, it\ turns\ \ (Hs, M_0 Z) \leftarrow M(\lambda)$ to generate the key.

The Finite automated key searching principle maintains the uniform sequence to create a cluster node set. $If\ b = 1, it\ chooses\ \ M_1$. Where 'M ' is the primary node,

For each $Bc \leftarrow \{0,1\}$, $E_c\,(F_{BP}\,)$ from each block $i\epsilon\ [1,n]$, hash code $i\epsilon\ [1,n]\ Hc$,

$\sum_{i=0}^{n} B_{ij}\ E_c\,(F_{BP}\,)$ →connected edge block E_c

Create block keys $k_i \leftarrow B - key\ Gen\ (M[i,j])$ the encryption block connects nodes define $C[i] \leftarrow B \rightarrow Enc\big(k_i, (\,M[i])\big)$, with master aggregation for chipper text is referred as

$k_i : C[n+1] \| \ldots . \| C[n'] \leftarrow BK - Enc(k_1, \ldots k_n)$ And $C = C[1] \| \ldots \| C[n] \| C[n+1] \| \ldots . \| C[n']$.

Create hashtags for all starvation blocks,

$tagT_0 \leftarrow M - TagGen(C[i]) and\ blocktagsT_i \leftarrow B - TagGen(C[i])$, to attend random starvation point

$For\ each\ i\epsilon\ [1,n]. set\ T = \{T_0, T_1, \ldots T_{n'}\}$

In this step, we will develop an advanced collaborative change policy for encrypted block content to protect the ciphertext without persistent knowledge of the block information. Blocks are maintained in a hash code table maintained by the shift encoder hash key policy during each change.

C. Provable Partition Chain Link (P^2CL)

The Security proofing dependability's starvation chain link to verify the data by Assuming that data be partitioned into block cyphers randomly and controlled to verify the data from peer to peer to prove the acknowledgement transaction policy to keep the information secure in transaction nodes. Each node is confirmed by a provable aggregator through key validation to partition the block level to ensure the safety of authentication keys.

The bloc is generated by authenticity aggregated by Creating a polynomial ECC to generate public and private keys.

Step 1: compute the Hash-coded blocks to validate access to Va

Attain block cypher with a hash key transaction to verify public and private keys

Create the chain link for partition block order. Cl continues block aggregation during the transaction.

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

Step2: By chose partition block L at split proofing

Split the data hash code verification and transaction to link the authentication

Verify the starvation endpoint key

Sk→$[1,n]. set\ T$

$$\mathrm{SK} = \int Br(Ud)$$

Step 3: Create Hash for all starvation Shk.

$$\mathrm{Sk} = \sum (Shk\ (Key \in K \longrightarrow starvation\ point\ s) \cup Ekey$$

Step 4: return the partition to create Sk

Usr→ return chain link proofing key (Sk)

End

Based on identifying the critical scenario, the block is slit with a key to a partitioned hash key. The cypher block is tightly coupled to safely hold the key without knowing the sequence of another block key. This partition block level improves the trust to validate the transaction to enhance the chain link security policy.

D. Hash-indexed block with chain ring policy

In this stage, a shifting chain ring policy was applied to form Blockchain to link the blocks. This chooses circular shifting form's matrix codded block to ensure the chain links. The SHA- encryption shifting depends on connections between public key Q and private key d to $create\ a\ bock\ level$ is referred to as,

$$tagT_0 \leftarrow M - TagGen(C[i]) and\ blocktagsT_i \leftarrow B - TagGen(C[i]) \qquad (3)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

Creating matrix shifting policy for random block k ∈ [1, n – 1]→ $Bc \leftarrow \{0,1\}\ E_c\ (F_{BP}\ )$ for generating shuffle key,

kG = (x, y) and r = x mod n, if r = n at each round hash index created

Generate session time,

For each block, t = k^{-1} mod n $E_c\ (F_{BP}\ )$ (4)

Attain exponential finite sets keys kG = SHA-1(m (Q, d)), 256 hash key

For each shifting round 'r' Calculate s = k^{-1} (e + d_a*r) mod n, if s = 0, the signature of the block pair is,

$Bc \rightarrow$ m (r, s) (5)

The primary node aggregation 'm' verifies the key at the peer end to prove the pairs to authenticate based on the request principle. The chain ring principle has the hash signature to generate a block sequence index to improve security.

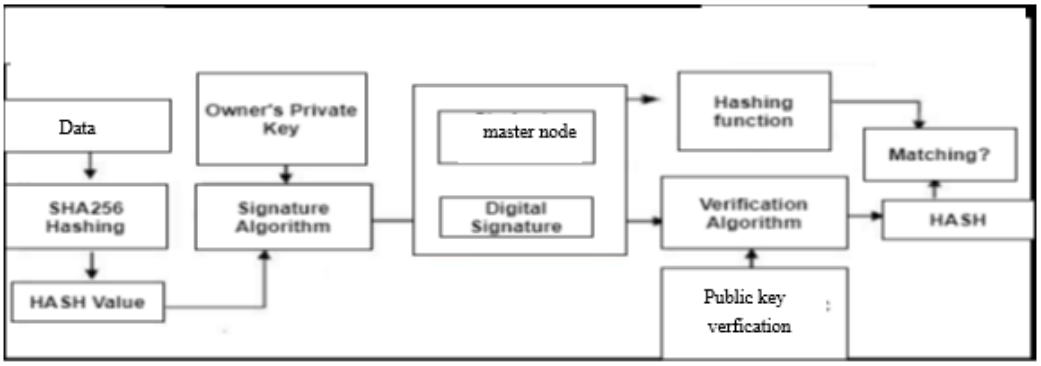

Figure 4. Master node Authentication

i) Proof of Authenticity (PoA)

The Proof of validation and verification was carried out after verifying the secret key. Such validity authentication is proven to allow data access at the peer end. Fig 4 shows the Master node Authentication.

The request Key at the peer end,

'$P_B \rightarrow$ Valid user V_u (6)

If check validated key on partial coordinated master key verification

R→ At $P_B(V_u)$← F_q (7)

At the finite set of blocks, proceed to the peer end by elliptic essential formulation.

$$P_B(V_u) \leftarrow F_q(Encrypted\ block)$$

$$Verify\ the\ hash\ index\ sequence\ to\ reorder\ chain\ link\ H_B \rightarrow P_B(V_u) \quad (8)$$

Compute the user key $K_B = H_B \rightarrow P_B(V_u)$, check Block hash key proofing

Verify machine address peer block at the session time't'

t = Mac_k (Clair text) (9)

Allow decrypt Computes D = t→Block content B_C

Return the validated progress content to secure transactions only at the peer end to deliver the data efficiently.

3.5 Principle of primary node aggregation

The security ends at peer-end verification based on the primary node policy; this verifies the transaction principle through Proof of authenticity, validity, and Proof of work to ensure the security, the public keys, and private keys are progressed through a blockchain transaction. The nodes contain the blocks and hash keys during the transaction to acknowledge the ledger data transmission. Each node authentication in the primary node is a news aggregator that maintains the sequence of blocks and keys to verify the verification and validation to deliver the data safely.

ii) Proof of Validity (PoV)

The validity proof is based on the signing verification using session standards. This proofing assigns the key at the specified time to ensure the transaction with public and private keys. The decentralization verifies the validation by considering the Proof with validation keys from peer to peer. The ECC enhances the hash index policy to encrypt the data to verify the digital signature.

$$sign\ [(\mathcal{H}: (\mathcal{k}, msg_1) \rightarrow \{\widetilde{0,1}\}^{\gamma}, \widetilde{s_{\mathcal{k}}})] \rightarrow \sigma_m \quad (10)$$

where s he denotes the secret key and σ_m represents the encrypted Hash

a value is known as a digital signature.

verification can be defined as

$$Verify\ session\ (n, \sigma_m, \mathcal{p}_{\mathcal{k}}\ ) \rightarrow \{0,1\}$$

$$where\ \mathcal{p}_{\mathcal{k}}\ denotes\ the\ public\ key \quad (11)$$

$$Verf(n, \sigma_m, \mathcal{p}_{\mathcal{k}}\ ) = \begin{cases} 1\ if\ \sigma_m\ is\ valid\ signature\ msg_1\ of\ under\ verification\ key\ SK \\ 0 \qquad\qquad if\ not\ valid \end{cases} \quad (12)$$

Informally, the digital information is verified by signature scheme = $\{\mathcal{K}, Sign, Verf\}$ owns the existential enforceability in contradiction chooses the session time to validate the public and private key to ensure the digital signature

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

C) Proof of Work (E-PoW)

The Proof of work validates the data and transaction based on the time stamp verification D_k *and* H_k in the blockchain mining network. The timestamp be worked under the transaction verification at peer reviewer policy,

t=0 at t0 ≤ t1 ≤ t2 ≤ · · ·tn

The continuity of the hash code block be verified Tk = to − tk − 1 be represented with the time of blockB_k. The sequence of the league based on the time window verified by,

$$T_k = \frac{D_k}{h_k} + t_k^p = \frac{D_k}{H_k} \quad (13)$$

Verbalizing the actual Proof depends on a secret key with a hash rate to verify the block of the propagation delay by time round Proof of validation. The exponential values distributed by the delays are eventually rejected. The hash block is confirmed by the representation equation as,

$$H_k = \frac{\sum_{i=1}^{W} D_{k-W+i}}{\sum_{i=1}^{W} T_{k-W+i}} \quad (13)$$

The nominal hash rate is verified $by\ H_K$ having the peer conversation authenticated to accept the valid Proof. This proves each code block level hash information by dividing the session time of representation during the regular interval time window. The PoW retrieves the validated key at peer-end authentication and only knows the secret key to ensure the Proof receives the data. This blockchain principle enhances the Proof of work consensus-based validity authenticity and proofing to improve security.

IV. EXPERIMENT RESULT ANALYSIS

In this phase, we assess the performance of the proposed experimental scheme. We first developed an experimental simulation platform to compare the different methods further. In particular, we run tests on block epoch time on Windows 10 with Intel Core i5-2120 CPU @ 3.30GHz with 8GB RAM.

TABLE 1. DEPLOYMENT OF SIMULATION PARAMETERS

Parameters	Values
Simulator tool	Visual Studio
Simulation language	C#
Dataset name	Medical Personal Healthcare Records (MPHR)
No of users	100
File size (in MB)	15, 30, 45, 60, 75, 90 and 100

The simulated blockchain environment parameters and values are defined in table I to show the data set with testing and validation. The performance testing was conducted to analyze the security performance, encryption-decryption time, and average latency, comparing the proposed technique with the previous algorithms.

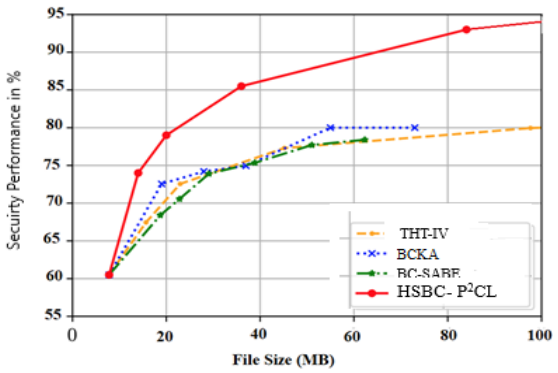

Figure 5: Result of classification performance

Fig. 5 describes the patients' sensitive information classification results compared with previous schemes. The proposed HSBC- P2CL method attains 93% classification performance for a 100MB file size. The proposed HSBC-P2CL algorithm achieves high performance than THT-IV, BSPEFB, and BC-SABE techniques.

TABLE 2: IMPACT OF SECURITY PERFORMANCE

Security performance in %				
File size (MB)	***THT-IV***	***BSPEFB***	***BC-SABE***	***HSBC-P2CL***
20	58	64	68	72
40	63	67	71	76
60	69	71	75	81
80	74	77	82	87
100	79	81	86	93

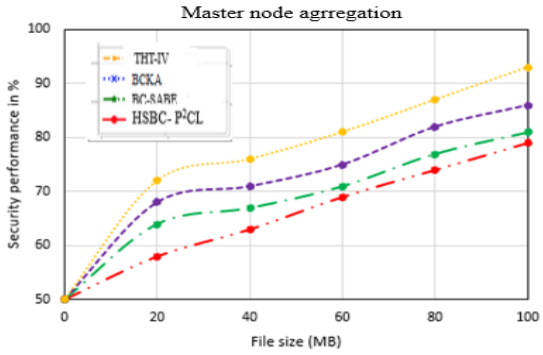

Figure 6. Security performance

Fig. 6 and Table 2 define the proposed MPHR security performance result with different file sizes like 20, 40, 60, 80, and 100 MB. The proposed HSBC- P2CL scheme attained 93% security performance for a 100MB file size. Also, the existing method is the THT-IV technique has 79% security performance, the BSPEFB approach has 81% security performance, and the BC-SABE technique has 86% security performance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

TABLE 3: IMPACT OF PRECISION AND RECALL PERFORMANCE

Comparison methods	*Verification (%)*	*Authenticity (%)*
THT-IV	68	67
BSPEFB	74	73
BC-SABE	80	78
HSBC- P2CL	91	89

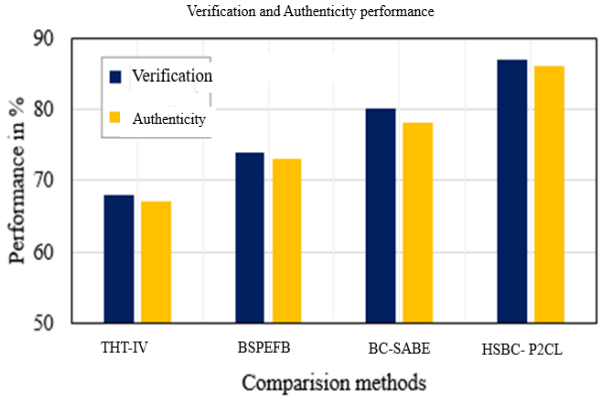

Figure 7. Result of Verification and Authenticity performance

Fig. 7 and Table 3 describe the Verification and Authenticity performance with existing methods. In the fig, the X-axis denotes the proposed method with different approaches, and the Y-axis represents each method's performance gradually increasing. The proposed HSBC-P2CL method's precision and recall performance is 91% and 89%, respectively. Similarly, the existing method result is that the THT-IV technique has a precision of 68% and recall of 67%; the MEdge-chain approach has an accuracy of 74% and recall of 73%. BC-SABE technique has a precision is 80% and recall is 78%.

TABLE 4: IMPACT OF F-MEASURE PERFORMANCE

F-measure performance in %				
File size (MB)	***THT-IV***	***BSPEFB***	***BC-SABE***	***HSBC-P2CL***
20	65	69	73	76
40	69	74	77	80
60	73	78	80	84
80	77	81	85	89
100	80	84	87	91

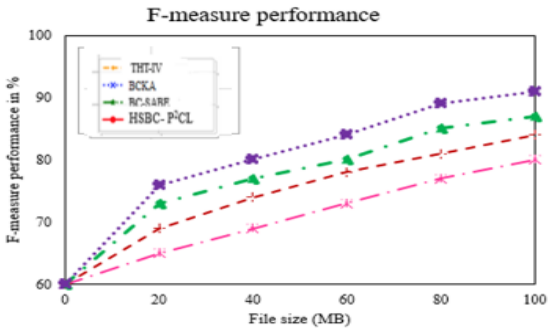

Figure 8: Result of F-measure performance

Fig. 8 and Table 4 illustrate the result of F-measure performance with different file sizes like 20, 40, 60, 80, and 100 MB. The proposed method produces 91% of F-measure performance; the THT-IV process yields 80% of F-measure performance, BSPEFB produces 84% of F-measure, and the BC-SABE method produces 87% of F-measure performance. However, the proposed method has high F-measure result than previous methods.

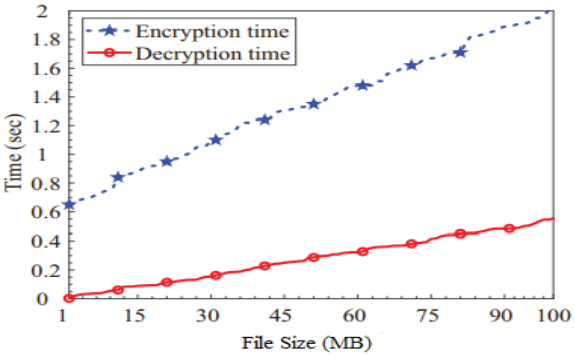

Figure 9. Result of encryption and decryption time

This value is calculated by averaging each User's 100 MB file size. Assuming each User has a 1MB MPHR file, 10 new users will join the proposed plan monthly. As shown in Fig 9, the response time delay gradually rises with the number of users. Thus the proposed HSBC- P2CL scheme encryption time is 2 sec, and the decryption time is 0.5 sec.

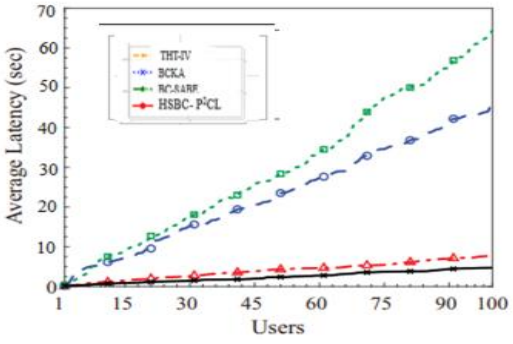

Figure 10. Result of average time complexity

Fig 10 shows the average time complexity performance result compared with previous methods. The X-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

axis presents the number of users like 15, 30, 45, 60, 75, 90, and 100. The proposed HSBC- P2CL scheme latency has 6 sec for response time during healthcare data sharing. The proposed HSBC- P2CL technique provides less time complexity performance than other methods.

V. CONCLUSION

To conclude, this proposed system achieves high performance to improve security. The information proactively enhances safety as well as privacy to identify sensitive records. The proposed secure data Transactions are based on Hash-coded Starvation Blockchain security. The cryptography adaption using Padded Ring signature-ECC for Network of Things proves the authenticity in IoT data transmission as a safeguard to make the transmission. This makes the encrypted block's provable partition chain Link (P^2CL). The encrypted blocks are transmitted into the nodes monitored by NoT security to create Proof of authentication. The proposed system proves high performance in the experimental result is security has 93%, verification and validation commission is 93%, F-measure has 91%, precision is 91%, recall is 89%, and overall time complexity is 6sec than other existing systems.

REFERENCES

[1]. A. gbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. (2019) "Blockchain technology in healthcare: a systematic review." In Healthcare, Multidisciplinary Digital Publishing Institute, vol. 7, 56, pp. 1-30.

[2]. M. Qiu, H. Qiu, H. Zhao, M. Liu and B. Thuraisingham, "Secure Data Sharing Through Untrusted Clouds with Blockchain-enhanced Key Management," 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 11-16, DOI: 10.1109/SmartBlock52591.2020

[3]. D. Tosh, S. Shetty, P. Foytik, C. Kamhoua and L. Njilla, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 302-309, DOI: 10.1109/CLOUD.2018

[4]. S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," in IEEE Access, vol. 8, pp. 192177-192191, 2020, DOI: 10.1109/ACCESS.2020.3032680.

[5]. B. Chen, L. Wu, H. Wang, L. Zhou and D. He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5813-5825, June 2020, DOI: 10.1109/TVT.2019.2959383.

[6]. Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng, and Z. Liu, "Blockchain-Based Verifiable Multi-Keyword Ranked Search on Encrypted Cloud With Fair Payment," in IEEE Access, vol. 7, pp. 140818-140832, 2019, DOI: 10.1109/ACCESS.2019.2943356.

[7]. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, DOI: 10.1109/ACCESS.2021.3054129

[8]. S. Wang, X. Wang, and Y. Zhang, "A Secure Cloud Storage Framework with Access Control Based on Blockchain," in IEEE Access, vol. 7, pp. 112713-112725, 2019, DOI: 10.1109/ACCESS.2019.2929205.

[9]. S. Wang, Y. Wang and Y. Zhang, "Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System," in IEEE Access, vol. 7, pp. 127652-127668, 2019, DOI: 10.1109/ACCESS.2019.2939492.

[10]. X. Yang, G. Chen, M. Wang, T. Li, and C. Wang, "Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on Blockchain," in IEEE Access, vol. 8, pp. 158765-158777, 2020, DOI: 10.1109/ACCESS.2020.3020841.

[11]. H. Cui, Z. Wan, X. Wei, S. Nepal, and X. Yi, "Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3227-3238, 2020, DOI: 10.1109/TIFS.2020.2973864.

[12]. Bahga, Arshdeep, and Vijay K. Madisetti. (2016) "Blockchain platform for the industrial internet of things." Journal of Software Engineering and Applications 9, no. 10, pp. 533-546

[13]. Y. Wang and M. He, "CPDS: A Cross-Blockchain Based Privacy-Preserving Data Sharing for Electronic Health Records," 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), 2021, pp. 90-99, doi: 10.1109/ICCCBDA51879.2021.

[14]. S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7851-7867, Sept. 2020, DOI: 10.1109/JIOT.2020.2993231.

[15]. K. Lee, "Comments on “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption”," in IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1299-1300, 1 Oct.-Dec. 2020, DOI: 10.1109/TCC.2020.2973623.

[16]. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, DOI: 10.1109/ACCESS.2021.3073203

[17]. M. Thangavel and P. Varalakshmi, "Enabling Ternary Hash Tree Based Integrity Verification for Secure Cloud Data Storage," in IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 12, pp. 2351-2362, 1 Dec. 2020, DOI: 10.1109/TKDE.2019.2922357.

[18]. Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 793-806, 1 April-June 2021, DOI: 10.1109/TCC.2018.2883063.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
DOI: https://doi.org/10.17762/ijritcc.v11i1.5986
***Article Received**: 14 November 2022 **Revised**: 16 December 2022 **Accepted**: 05 January 2023*

[19]. J. Zhang, R. Lu, B. Wang and X. A. Wang, "Comments on “Privacy-Preserving Public Auditing Protocol for Regenerating-Code-Based Cloud Storage”," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1288-1289, 2021, DOI: 10.1109/TIFS.2020.3032283.

[20]. G. Sciumè, E. J. Palacios-García, P. Gallo, E. R. Sanseverino, J. C. Vasquez and J. M. Guerrero, "Demand Response Service Certification and Customer Baseline Evaluation Using Blockchain Technology," in IEEE Access, vol. 8, pp. 139313-139331, 2020, doi: 10.1109/ACCESS.2020.3012781.