TPM Vol. 32, No. S4, 2025
ISSN: 1972-6325
https://www.tpmap.org/

ENHANCED MED-CHAIN SECURITY FOR PROTECTING DIABETIC HEALTHCARE DATA IN DECENTRALIZED HEALTHCARE ENVIRONMENT BASED ON ADVANCED CRYPTO AUTHENTICATION POLICY

[1]M. WASIM RAJA, [2]DR.M. PUSHPAVALLI, [3]DR.M. BALAMURUGAN, [4]K. SARANYA,

[1]DEPARTMENT OF COMPUTER SCIENCE, JAMAL MOHAMED COLLEGE (AUTONOMOUS), (AFFILIATED TO BHARATHIDASAN UNIVERSITY), TIRUCHIRAPPALLI, TAMILNADU, INDIA
mail: mwr@jmc.edu

[2]ASSOCIATE PROFESSOR, DEPARTMENT OF ECE,
BANNARI AMMAN INSTITUTE OF TECHNOLOGY, SATHYAMANGALAM.
pushpavallim@bitsathy.ac.in

[3]HEAD OF THE DEPARTMENT & ASSOCIATE PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, THE KAVERY ENGINEERING COLLEGE, SALEM, TAMIL NADU, INDIA
Hodcse@kavery.org.in

[4]ASSOCIATE PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, BANNARI AMMAN INSTITUTE OF TECHNOLOGY, SATHYAMANGALAM, ERODE, TAMILNADU, INDIA
Email: ksaranyacse@gmail.com

Abstract

Security is the important aspect in healthcare environment based on data analysis and blockchain security in the context of IoT. By harnessing the power of these technologies, healthcare administrations can recover patient care, privacy data preservation and ensure the integrity of their data. The optimized deep learning model proposed in this paper serves as a valuable tool for healthcare organizations looking to leverage AI and blockchain technology for data analysis and security in the digital age. Due to leveraging the security breaches, key leakages, the healthcare data contains more sensitive information and patient treatment data are personalized to key safely. So, the prevailing security system doesn't pose to attain integrity, confidentiality, trust to reliable the protection. To address this problem, To propose an Enhanced Proof of Work-Based Block Chain Security (EPoW-BC) system for improving healthcare data transmission security to handover the authorized person. To implement an Advanced Shuffle Padding Folding Encryption (ASPFE) algorithm to improve the security. Shift Matrix Code Block Chaining Key (SMCB-CK) is used to create the secret key grounded the block level and chain level which is used for secret key verification to access the data. Creating verification and validation model based on Master Node Authentication Policy (MNAP) to improve the secure data handover. The proposed system produces high performance as well in higher security by validating the key parameters, encryption and security parameter by compared with exits system which proves high confidentiality, trust, and reliability.

Keywords: Artificial Intelligence, Blockchain, Healthcare Data Analysis, Internet of Things, Enhanced Proof of Work, Encryption, Security, Data Integrity, Confidentiality, Master Node Authentication.

1.INTRODUCTION

The development of Artificial Intelligence (AI) in pricay data protection for heathcare has transformed the landscape of medical data management [1, 2], enabling more efficient patient care and operational functionalities [2]. Yet, as healthcare organizations pivot towards increasingly digitized environments, the challenges surrounding data integrity, security, and patient confidentiality have become more pronounced [3, 4].

Given the sensitive nature of healthcare data, which includes personalized treatment plans and sensitive patient information, existing security frameworks often fall short of providing comprehensive protection [5, 6]. This paper highlights a proposed Enhanced Proof of Work-Based Blockchain Security (EPoW-BC) system that not only aims to safeguard healthcare data during transmission but also to enhance the analytical capabilities through a robust partnership with advanced algorithms.

The healthcare sector is witnessing an exponential increase in cyber threats, including data breaches and key leakages [7]. Traditional security systems often rely on outdated mechanisms that do not adequately protect sensitive data from unauthorized access or manipulation [8]. This forms the backbone of the problem; hospitals and healthcare providers need a security model that ensures integrity, confidentiality, and trustworthiness. Current mechanisms lack the capabilities to achieve these benchmarks, which are critical in an era where healthcare data are being increasingly digitized and shared across interconnected networks [9]. By integrating AI with blockchain technology within the Internet of Things (IoT) architecture, healthcare organizations can leverage both preventive and analytical advantages. AI algorithms provide powerful data analysis capabilities, from trend identification to predictive analytics, while blockchain offers decentralized security through immutable ledgers that ensure data integrity [10]. Collectively, these technologies offer a transformative potential, promising to elevate patient care and operational efficacy while intensifying security protocols.

Enhanced Proof of Work-Based Blockchain Security (EPoW-BC) system to bolster the security of healthcare data transmission, ensuring that access is granted only to authorized personnel. Additionally, we implement an Advanced Shuffle Padding Folding Encryption (ASPFE) algorithm to enhance data protection. The Shift Matrix Code Block Chaining Key (SMCB-CK) is introduced to generate secret keys at both block and chain levels, facilitating secure key verification for data access. Moreover, we establish a verification and validation model based on the Master Node Authentication Policy (MNAP) to enhance secure data handover procedures. Our proposed system demonstrates superior performance and elevated security metrics, outmatching existing systems through improved verification of key parameters, encryption techniques, and overall security, thereby fostering increased confidentiality, trust, and reliability in healthcare data management.

2.LITERATURE SURVEY

In this chapter, discussed the existing methodologies of Blockchain (BC) methodologies based on verification security. The author discussed about the communication of satellites, capacities of processing and power of satellite was so restricted. To resolve the issue, mechanism of ground equipment and satellite composite was deployed. Through the strong data processing volume, the collected data forwards the data to a ground station. Yet, the channels of the satellite communications enormously susceptible to the user so it remains big encounter [11].

By continuing, the author carried out merkle tree methodology to progress the effectiveness of authentication. The deployed methodology maintains a consistent and set authentication time for each transaction. However, the suggested solution necessitates frequent testing in IoT systems featuring diverse components [12]. The author discussed about how to certify a cloud data integrity through the large scale systems. To resolve the issue, a lattice signature mechanism was deployed [13].

To resolve the following restrictions, a Multi-Layer BC Security (ML-BCS) methodology was deployed. The deployed method assumed global BC mechanism to securely communicate through each other. But the communication among the such nodes remains the security drawbacks [14]. In IoT systems security is the main drawback when the data was exchange. To resolve the issue, the author deployed a enhance authentication & authorization methodology. The disadvantages of this approach are theft of identities, improper access, and data breaches [15].

The author discussed the possible security hazards of digitizing medical certificates and documents, including the possibility of certificate forgeries endangering patient privacy. To resolve the issue. a privacy-preserving methodology was deployed. The deployed methodology offers a way for patients and medical facilities to communicate for the purpose of creating and managing medical records. But documents can also result in security threats. For example, forged certifications put patient privacy in jeopardy [16]. The author's primary objective is to enhance the security of the suggested approach by guaranteeing confidentiality and implementing a verification mechanism during authentication. To attain the objective, a light cryptography methodology was

deployed. The new recommended matching process compares password properties with database records for the purpose of verifying the legitimacy of the proposed technique [17].

The network's security and dependability can easily be challenged due to the author's implementation of an inadequate data protection strategy. The shown methodology improves the consortium BC, which lowers processing latency and boosts efficient throughput, eliminating the need for the long-standing certificate authority. The suggested approach has raised serious concerns about security alternatives because of the current increase in cyberattacks, which primarily target vital infrastructure [18].

However, the issue of fraudulent credentials is concerning and worrisome. To resolve the issue, an overlay methodology on the basis of BC mechanisms was deployed. It keeps authentic certificates digitally and quickly and firmly authenticates those while required [19]. Yet, these are distributed in groups via standard passwords and users, leaving those open to intrusions. To resolve the issue, a distributed identity-based authentication methodology was used. By acting as a distributed PKG, BC solves the key escrow issue and single point of failure associated with PKGs [20].

The author discussed that the medical industry depends heavily on IoT-based healthcare technology, which is driving the creation of more efficient and individualized treatment. Data standards and protocols are still lacking in a number of IoT devices. To resolve the issue, a Lamport Merkle Digital Signature Generation (LMDSG) methodology was deployed. Sensitive patient data is protected from nefarious users by the suggested verification technique. But decision-making is hampered by the massive volume of data, and privacy is a major concern with IoT [21]. In order to solve these issues, BC mechanism was created because of its end-to-end verification capabilities. To solve the aforementioned issues, the suggested approach is a dependable one. The primary challenge is in the ease with which any malware can be introduced into the device to cause interference affecting the server [12].

The author explained how different security and privacy issues arise on public channels as a result of insecure communication. To resolve the issue, a Public BC-envisioned Secure Communication Framework (PBCSCF) was deployed. A variety of network-related performance metrics, including the quantity of mined blocks and transactions per block, were examined in relation to the suggested technique. There may be some possibility of biassing to enable the suggested approach [23].

The author discussed how WSNs are highly susceptible to network attacks and how adequate safety precautions are needed. To resolve the issue, an efficient authentication methodology was deployed. The base station creates the WSN nodes, which are via the IoT. Nevertheless, the suggested approach is highly vulnerable to frequent node failures [24]. Nevertheless, it's necessary to effectively administer with the value a framework and ensure the confidentiality and safety of machines. To resolve the issue, a secure and lightweight authentication scheme on the basis of BC was deployed. To accomplish an efficient authentication procedure, the modular square root technique and the BC approach are combined in the suggested approach. However, ensuring the authenticity of devices has become increasingly problematic for linked devices in the IoT security system [25].

The author discussed about how distributive BC technology can be applied to problems with user authorization and authentication. Because it requires piracy data protection, the Role-Based Access Control (RBAC) is most case used in the way for organizations to meet security requirements. Yet, administrators of systems now face a big difficulty when it comes to safeguarding data [26]. The reliability of the decryption and verification of access rights to shared data are either disregarded or carried out by an unreliable third-party. To resolved the issue, a Ciphertext Policy Attribute-Based Encryption (CP-ABE) techniques is most cases used public clouds with numerous accounts accessed by complex access structures, nevertheless, due to its low granularity of policy masking and less expressive access structures [27].

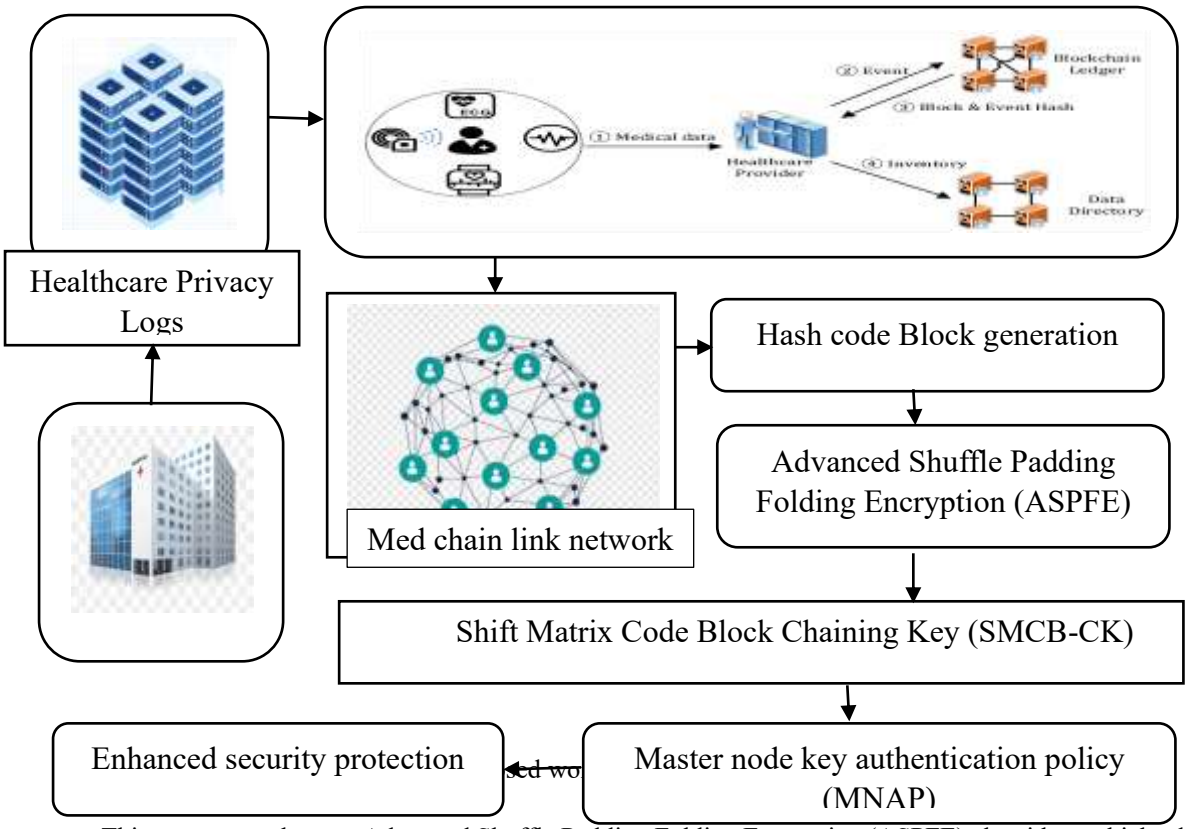
The author's goal was to finish the medical data security architecture so that data owners may safely and conveniently communicate private medical records with healthcare providers. To resolve the issue, a Secured Encrypted Medical Record (SEMRES) methodology was deployed. The suggested solution assures data accuracy using a BC open ledger's non-repudiation characteristic and comprehensive, integrated information security protection. Nonetheless, the primary issues are data safety, precision, and confidentiality [28].

The author discussed the need for more methods to solve privacy and trust issues in IoT applications. To resolve the issue, a novel BC- built authentication framework was deployed. The majority of applications that use BC technology can be solved by the deployed methodology, particularly those that need help with scalability and optimized storage. However, the deployed methodology are the complexity and storage overhead [29]. Accordingly, a safe and effective authentication system must be designed to protect sensitive data in the IoT. To

resolve the issue, a privacy-preserving authentication management mechanism was deployed. The deployed mechanism visible that the optimized storage is safe. Still, it could be vulnerable to a number of security flaws and assaults via an unreliable broadcast connection [30].

3.PROPOSED EPOW-BC SYSTEM OVERVIEW

The crux of the proposed solution lies in the Enhanced Proof of Work-Based Blockchain Security (EPoW-BC) system. This novel framework aims to recover the general security of medical data during transmission in a manner that ensures only authorized personnel access sensitive information. Unlike conventional blockchain models, the EPoW-BC introduces several innovative components that fortify security and validate access through a multi-layered approach. The proposed Enhanced Proof of Work-Based Blockchain Security (EPoW-BC) system aims to significantly strengthen the security of healthcare data transmission by ensuring that access is exclusively granted to authorized personnel.



This system employs an Advanced Shuffle Padding Folding Encryption (ASPFE) algorithm, which adds an additional layer of protection for sensitive data. To further augment security, the Shift Matrix Code Block Chaining Key (SMCB-CK) mechanism is introduced to generate secret keys at both the block and chain levels, facilitating effective key verification for secure data access. Figure 1 explains the Proposed work flow architecture ASPEE -MNAP. Furthermore, we establish a robust verification and validation model guided by the Master Node Authentication Policy (MNAP), which enhances secure data handover procedures. This comprehensive approach combines blockchain technology with advanced encryption and authentication methods, offering a resilient framework for safeguarding healthcare data in transmission against unauthorized access and tampering.

A) Advanced Shuffle Padding Folding Encryption (ASPFE) Algorithm:

At the heart of the EPoW-BC system is the ASPFE algorithm, designed to enhance data security through a sophisticated encryption mechanism. This approach not only obscures data but also limits vulnerabilities during data transmission, deterring potential interception and unauthorized retrieval.

An encryption technique that is frequently used and renowned for its power, effectiveness, and resilience is the AES technique. To sum up, storing and safeguarding large amounts of sensitive data securely and effectively can be achieved through the use of the AES algorithm on a permissioned blockchain. The encryption used by the AES algorithm is block cypher. The encryption procedure is more sophisticated and secure with AES because of its bigger block size of 128 bits. The high level of security that the AES algorithm offers is applied to the shard data before it is stored in the blockchain that various cloud providers offer.

A predefined set of S-Boxes, each with 256 entries, are used by the AES algorithm. The algorithm makes use of ten S-Boxes, one for every round of encryption. An 8-bit value is used to represent each item in an S-Box, and this value is used to replace the corresponding 8 bits in the input data. A fixed set of input values is subjected to a combination of substitution and permutation procedures in order to construct the S-Boxes.

Algorithm : Block Level AES

Input:

Initialize O for encryption

Initialize D_1, D_2, set of sub keys, S-boxes for decryption

Output:

256-byte initialized S-box is the outcome of encryption

The plaintext is the outcome of the decryption

Set the S-box, an empty 256-byte array, to its initial value.

0x00 through 0x0F should be the values that fill the first 16 bytes of the S-box.

for $x \rightarrow 255$

do

Using the Extended Euclidean Algorithm, find the multiplicative inverse of x in the finite field GF (2^8).

Utilizing the inverse function of Galois field multiplication and a bitwise XOR via a fixed constant, an affine transformation is applied to the outcome.

The resultant byte should be placed in the appropriate S-box location.

end for

The finished S-box was return.

First, the plain text is split into 128-bit blocks for the AES encryption procedure. A substitution-permutation network (SPN) structure is used by the AES algorithm. The cypher text is the block that remains after the last round. The round keys are utilised in reverse order during the access the original data tor decrypt with key, which is the opposite of the encryption procedure. The procedure for AES encryption is explained in Algorithm 2. The process for decrypting AES is shown in Algorithm 3.

Algorithm 2:

Start

Input:

Plain text

Output:

Cipher text

Phase 1: There are four 32-bit sections that make up the 128-bit Plain Text.

Phase 2: The first round key is used to perform the AddRoundKey operation on the input data.

Phase 3: The S-box is used to transmit the data via the SubBytes transformation.

Phase 4: The ShiftRows transformation then shifts the data row-wise.

Phase 5: The MixColumns transformation is applied on the shifted data.

Phase 6: Up until the last round, phases 2 through 5 are repeated for every round key.

Phase 7: The SubBytes transformation and the ShiftRows transformation are used in the last round.

Phase 8: The output data is subjected to the AddRoundKey operation using the final round key.

Phase 9: The Cypher text is found in the generated 128-bit data.

End

Algorithm 3:

Start

Input:

The file is a text file with cypher characters.

Output:

It is changed to plain text E.

Phase 1: The same set of keys are used in reverse order for the decryption procedure, which is analogous to the encryption process.

Phase 2: The key schedule methodology generates the subkeys in reverse order, beginning with the final subkey.

Phase 3: There are 128-bit chunks in the cypher text.

Phase 4: The final subkey and the first block are XORed.

Phase 5: After that, the block does the inverse rounds of shifting, mixing, and substituting using the inverse S-box, inverse mix columns, and inverse shift rows operations.

Phase 6: The output is XORed with the second last subkey once the inverse rounds are finished.

Phase 7: Until the first subkey is utilised, this procedure keeps on.

Phase 8: The final block is the plain text.

End

In order to provide secure data storage, the developed model suggests integrating blockchain technology with a serverless framework. This allows organisations to assign tasks related to architecture, such as provisioning, scaling, and maintenance. The model uses encryption because it offers high security, quick data storage transactions, and a variable key size that can be adjusted based on the sensitivity of the data.

B) Shift Matrix Code Block Chaining Key (SMCB-CK)

The SMCB-CK acts as a critical instrument in generating secret keys based on both block and chain levels. This enhanced key-generation mechanism ensures that access keys remain unique and specific to data segments, providing an additional layer of validation and security. It promotes secret key verification processes that are essential for accessing sensitive healthcare data. A hash code is produced by the Shuffle standard padding encryption password policy using a string of significant characters that is chosen at random. The message price will not stop consuming extra value right away.

Every new message needs a unique is periodic key that is a part of that matrix as every is period adds rows to it. Start with the smallest behemoth in each row of the data by replacement. Uses a collection of altered round key values to compute an initialization key value.

$dk_{\propto}, dk_{\beta}, dk_{\rho}, h_{key}$ be appropriate end key

Checkeed set of key $dk_{\propto}, dk_{\beta}, dk_{\rho} \in \{0,1,3 \ldots . 3^{10} - 1\}$

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

The sorting block are connected with hash code , data block link code represented as α, ρ, and β that are proportional to the block size key length h.

$d_{\propto}, d_{\beta}, d_{\rho}\ h_{key}$creates block connecting link on chain link hash code.

Th block and key index are generated and connected by loop-dependent calculation parameters.

Row $\propto = ax + d_{\propto} \times 10^{-3}$

Data Column block $\beta = by + (d_{\beta} \times 10\ block^{-3})$

Representing the block connecting edge to chain link $\rho = cz + (d_{\rho} \times 10^{\ block-3})$

The padding values for each computation continue to contain Key+1 and the first W f.

(S) ∈ {random,..,∞}.

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

The indexing character is represented by Wf. Because every cell in each matrix block has a prime value, data block is represented as w (i).

For every value in the index, generate

$wi_i = (10^2 \times \sum a_{s+i} + b_{s+i} + c_{s+i})\ mod\ 2^8 \qquad \forall_i = \ 1,2, \ldots \ldots N^2$

To reorganize the column and row indexes, use circular shifting on N index terms. Wf into an N-square matrix W.

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

$$Wi = \begin{bmatrix} wi_1 & wi_2 & \ldots & wi_N \\ wi_{N+1} & wi_{N+2} & \ldots & wi_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ wi_{N^2-N+1} & wi_{N^2-N+2} & \ldots & wi_{N^2} \end{bmatrix}$$

Key values that are theorem-transferred matrix stored and replaced by random ().

Use h_{key} - The block data contain each hash index value W in each block's top row, as well as the complement of all rows, are XOR.

At the conclusion of the hash key substitution, calculate the padding scheme so that the XOR is proportionate to each block that follows.

If padding is started with +1 in the row matrix

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

For every row that follows in padding row,$wi_{row(i)} = w_{irow(i)} \oplus wi_{row(i-1)}$

$Wx(i) \longrightarrow \forall_i = 0,1,2, \ldots N$

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

Compute to produce a N * N representation ob block matric with a distinct representation block denoted by ϕ.

$$\phi = \{wi_1, wi_2, \dots wi_i, \dots wi_{L-1}, wi_L\}$$

After scrolling the selected calculated column along each block hash code is connected with other code block,

$$\overbrace{IN \to [wi_1] \to [wi_2] \to \cdots \to [wi_L]}^{enc\ code \to a\ time}$$

$$Is = \begin{bmatrix} \to 3 & \downarrow 2 & \downarrow 1 \\ \uparrow 6 & \downarrow 4 & \downarrow 5 \\ \uparrow 9 & \leftarrow 7 & \leftarrow 8 \end{bmatrix}$$

The appropriate faeces matrices are produced by the code using the pad keys.

$$\overline{Is} = \begin{bmatrix} 4 \to & 5 \to & 9 \to \\ 6 \to & 7 \to & 5 \to \\ 1 \to & 2 \to & 5 \to \end{bmatrix}$$

Insert every block's hash connecting with private key →CT (Pki) before sending it to form chain link with random circulation.

Return block Ct (Pk)

End

End.

The random chain link creates serial representation of block position maintained in chain link to identify the block sequence during the key validation time This is due to the fact that long strings in regular printing create circular and keystroke-like chunks.

C) Master Node Authentication Policy (MNAP)

The proposed solution includes a robust verification and validation model predicated on Master Node Authentication Policy. MNAP serves as a governance framework that enhances secure data handover processes. By ensuring that only authorized users can authenticate transactions, the MNAP fortifies security protocols while enhancing data accessibility.

A blockchain-based authentication verification algorithm presents a novel approach to safe identity management and verification. This method reduces the hazards associated with centralised data storage and improves user privacy by utilising blockchain's distributed ledger and cryptography concepts. Every attempt at authentication is maintained block level transaction, guaranteeing the process's transparency and auditability. Some of the fundamental equations that could be included in such an algorithm are listed below along with their definitions:

$$Z(a) = E\ (z)$$

In equation , Z is known for hash function, a is known for fixed size string of bites, and z is known for input data. In blockchain, D is used to produce unique characteristics for blocks and contacts as well as to guarantee data integrity. In equation 9 we compute the digital signature,

$$P = P_{Sv_m}\big(Z(O)\big)$$

The hash key formalized with private key to sign the message's hash, a digital signature P is produced. By doing this, the message's integrity and authenticity are guaranteed. By secret key with validation master ode allows the user to attain the signature. With public key encryption to verify the key,

$$D = G_{Sw_m}(H)$$

here, D is known for ciphertext, and H is known for plaintext message. Public key encryption converts plaintext messages into ciphertext by using a public key. The ciphertext can only be decrypted back into the original plaintext with the matching private key.

$$L = L_{Sw_m}\big(U, Z(O)\big)$$

the verification procedure determines whether the signature L is legitimate. The signature is regarded as legitimate if the values match. The consensus mechanism is illustrating in equation 12,

$$Z\big(n||Z(Y)\big) < R$$

here, R is meant for target, Y is meant for block, and n is known as nonce. By determining a nonce such that its hash when combined with the block's hash is smaller than a predefined objective, miners can solve a cryptographic problem and arrive at a consensus method. On the blockchain, new blocks are created and transactions are validated using this procedure. In equation 13 we illustrate the merkle tree root computation,

$$C = Z\left(Z(E_1)||Z(E_2)|| \dots ||Z(E_n)\right)$$

here, C is meant for merkle tree root, and the leaf nodes is determined as E. The C value is calculated by iteratively hashing pairs of leaf nodes maintain hask hey. The C delivers a secure and efficient technique for determining the honesty of all transactions within a block. In equation 14 we illustrate how the verify the block in hash function,

$$L(Y_x) = \big(Z(Y_{i-1}), R_x, C_x, n_x, Z(Y_x)\big)$$

in this equation, block verification validates the correctness of a block by inspecting its components, which include the preceding block's hash, the transaction list, the Merkle root, and the nonce. The hash of the current block is computed and compared to these components. In equation 15 we verify the blockchain,

$$\forall_x L(Y_x)\ \&\ Z(Y_x) = Z(Y_{x+1})$$

in this equation, blockchain verification entails ensuring that each block on the blockchain has been correctly authenticated and hash key matches the reference in the next block. This protects the blockchain's integrity and continuity after verification done to decrypt the data securely.

The ciphertext must first be converted from its encrypted format into plaintext in order to be decrypted.

Employ the same subkey and S-box combinations as for encryption, but in the opposite sequence.

Beginning with the final subkey, decryption proceeds backwards to the first subkey.

Proceed with the decryption procedure by employing every subkey in turn.

After all, subkeys have been used in reverse order, return the plaintext.

The application of a med chain intent with med chain authentication verification methodology marks a big step forward in secure identity management systems, providing a scalable and trustworthy solution that can be applied to improv the security.

4.RESULTS AND PERFORMANCE EVALUATION

One of the most significant features of the EPoW-BC system is its demonstrable efficacy in terms of both performance and security. Preliminary evaluations, conducted comparative to existing systems, indicate that the EPoW-BC solution significantly outperforms traditional models in computational efficiency and data protection. Key parameters, such as encryption strength, authentication speed, and reliability of data transfer, are markedly enhanced, proving that the proposed system fulfills the core objectives of security, confidentiality, and trust.

The following section carries out a simulation result comparison of the proposed algorithm with traditional methods. Furthermore, experiment settings for secure data sharing illustrated in table 1.

Table 1: Simulation settings for sensitive data sharing

Parameters name	Data
Development tool	Visual studio
Language used	C#.net
Dataset processed	Pregnancy dataset
Number of records	3000
Training and testing ratio	7:3

The evaluation criteria include sensitivity, specificity, security, F1-score, and classification performance results as outlined below. **Performance with S2AES under HC-MNKA.**

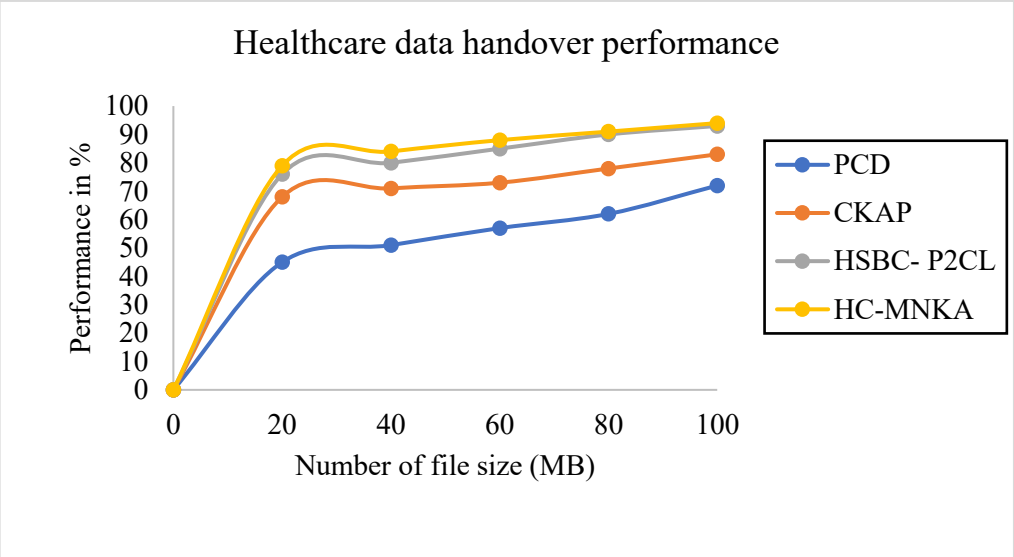


Figure 2 Impact of Healthcare data handover performance

The healthcare data handover performance is explained in Figure 2 through an analysis of medical records with varying file sizes. For 100MB files, the suggested method's categorization performance is 94%. Comparably, the security performance of the Patient-centric Design (PCD) technique is 79%, and the Construction of Key Agreement Protocol (CKAP) method has an 84% security performance.

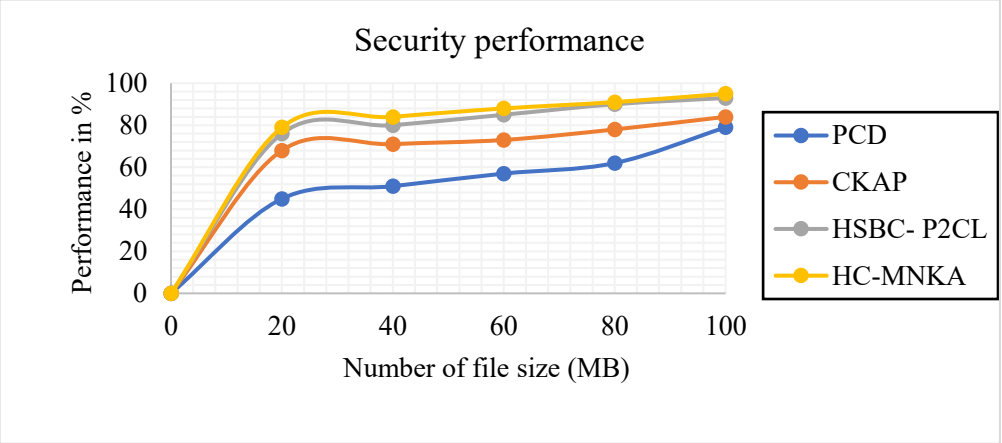


Figure 3 Impact of Security Performance

The security performance for healthcare records is explained in Figure 3. Safely share and save data in cloud settings. For 100MB files, the suggested method's security performance is 95%. Comparably, the security performance of the PCD technique is 79%, and the CKAP method has an 84% security performance.

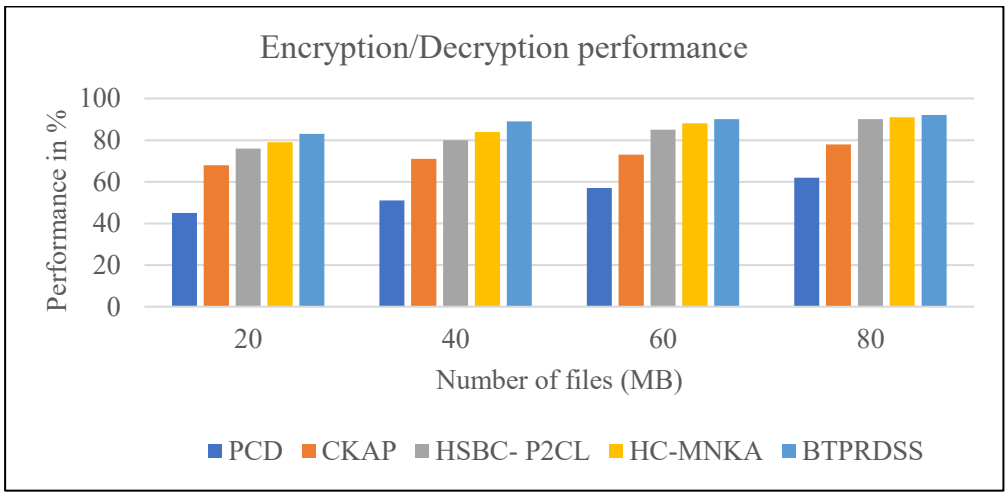


Figure 4 Encryption and decryption Performance

The encryption and decryption performance for cloud-based secure data sharing of medical records is described in Figure 4. For 100MB files, the performance of the suggested technique is 95%. Comparably, the performance of the current techniques is 79% for PCD and 84% for CKAP.

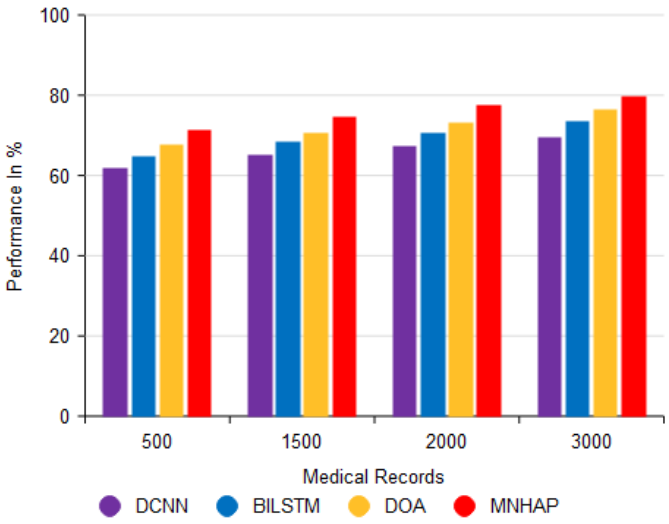


Figure 5. Analysis of Sensitivity Performance

As depicted in Figure 5, various methods can be determined to forecast accuracy values through sensitivity performance analysis. Additionally, the suggested implementation attains sensitivity performance compared to other methods. Hence, the comparison of blockchain-based IoT devices in the healthcare sector offers numerous advantages, including secure data storage and transmission, real-time patient monitoring, automated medication management, and enhanced supply chain efficiency. Furthermore, the forecast accuracy of the MNHAP proposed sensitivity performance analysis method has been enhanced to 79.64%. Similarly, its accuracy is 62% lower when compared to methods outlined in the literature such as DOA, BiLSTM, and DCNN.

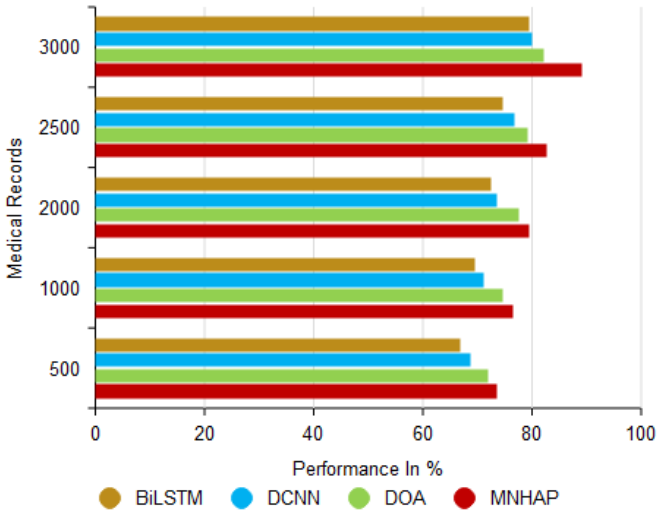


Figure 6. Analysis of Specificity Performance

In figure 6 illustrates the analysis of various methods used to predict accuracy values through specificity performance analysis. The proposed implementation demonstrated superior performance in comparison to alternative approaches. Accordingly, the prediction accuracy of the MHAP proposed sensitivity performance analysis method exhibited a remarkable improvement, reaching 89.24%. However, it is worth noticing that the accuracy of the proposed method fell short in comparison to established methods such as DOA, BiLSTM, and DCNN, with a difference of approximately 66.72%. Despite this, there are several benefits to integrating Blockchain technology with IoT devices in the healthcare industry, such as safe data transfer and storage, automated medication management, real-time patient monitoring, and improved supply chain effectiveness.

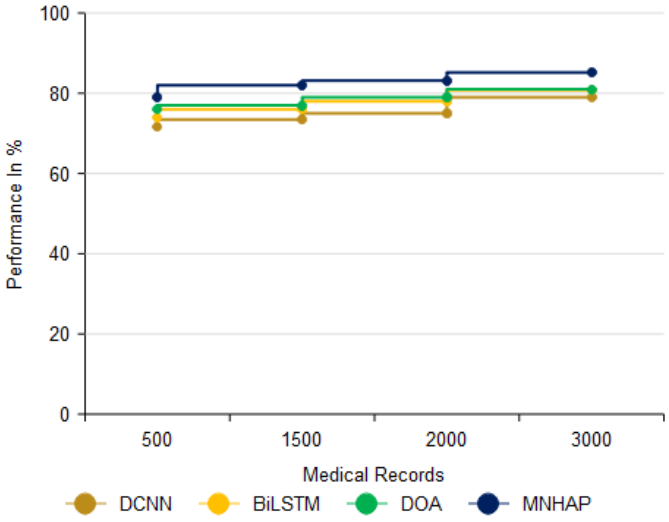


Figure 7. Analysis of False Detection Performance

In Figure 7, various methods has been compared for analyzing prediction accuracy values using F1-Score performance. Furthermore, the proposed implementation outperforms other methods. When examining F1-Score performance using methods outlined in the literature like DOA, BiLSTM, and DCNN, their accuracy is as low as 69.2%. Moreover, the MNHAP proposed F1-Score performance analysis method enhances prediction accuracy to 83%. As a result, the healthcare industry may benefit greatly from the integration of blockchain-based IoT devices. These benefits include safe data transfer and storage, automated medication management, real-time patient monitoring, and increased supply chain efficiency.

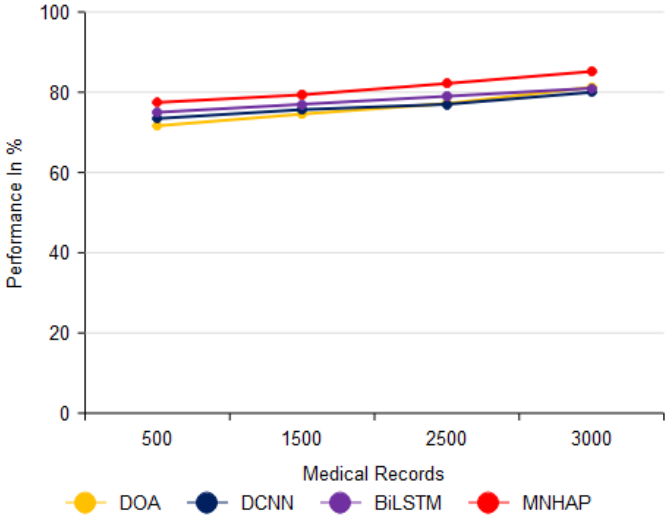


Figure 8. Analysis of Security Performance

Therefore, the integration of blockchain-based IoT devices in the healthcare sector brings many benefits such as secure data storage and transmission, real-time patient monitoring, automated medication management, and improved supply chain efficiency. As demonstrated in Fig. 9, different methods can be compared to analyze the prediction accuracy values using security performance. Furthermore, the proposed implementation achieves higher performance than other methods. Similarly, when analyzing the security performance with methods described in the literature such as DOA, BiLSTM and DCNN, their estimate is as low as 71.63%. Moreover, the safety performance analysis accuracy of the proposed MNHAP method is improved to 85.18%.

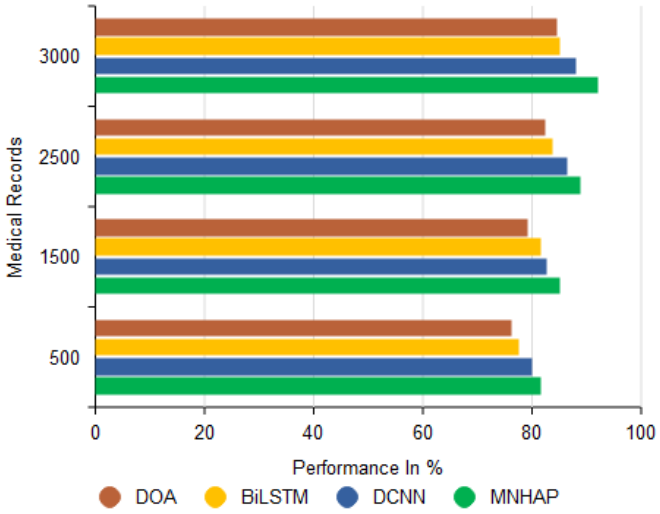


Figure 9. Analysis of classification Detection Accuracy

Figure 6 illustrates a comparison of various methodologies for assessing prediction accuracy within the realm of classification performance. The integration of blockchain-based Internet of Things (IoT) devices in the healthcare sector presents numerous advantages, such as secure data storage and transmission, real-time patient monitoring, automated medication management, and enhanced supply chain efficiency. Notably, the proposed implementation yields superior classification detection performance relative to alternative methods.

5.CONCLUSION

The perpetual evolution of healthcare technology mandates an equally dynamic approach to data security and analysis. The proposed Enhanced Proof of Work-Based Blockchain Security (EPoW-BC) system represents a pioneering advancement in safeguarding healthcare data within IoT frameworks. By intertwining AI capabilities

with innovative blockchain methodologies, this system seeks not only to bolster security but also to enhance operational performance in healthcare settings. As organizations continue to navigate the complexities of digital health management, the EPoW-BC system offers a pathway toward a future where data integrity and patient care coexist seamlessly, sustaining the trust that is paramount in healthcare relationships. In conclusion, embracing such advanced technologies is not merely an option but a necessity in ensuring that sensitive healthcare information is shielded from the evolving landscape of cybersecurity threats.

REFERENCES

[1]. E. R. D. Villarreal, J. García-Alonso, E. Moguel and J. A. H. Alegría, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," in IEEE Access, vol. 11, pp. 5629-5652, 2023, doi: 10.1109/ACCESS.2023.3236505.

[2]. Suruchi Singh, Bhatt Pankaj, K. Nagarajan, Neha P. Singh, Veer Bala, Blockchain with cloud for handling healthcare data: A privacy-friendly platform, Materials Today: Proceedings, Volume 62, Part 7, 2022, Pages 5021-5026, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2022.04.910.

[3]. Noshina Tariq, Ayesha Qamar, Muhammad Asim, Farrukh Aslam Khan, "Blockchain and Smart Healthcare Security: A Survey, Procedia Computer Science," Volume 175, 2020, Pages 615-620, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.07.089.

[4]. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. IEEE Trans. Eng. Manag. 2020, 1–16

[5]. P V, Gopirajan & Mani, Kanchana. (2022). Secure Multi-Authentication using BlockchainTechnology in Cloud based Internet of Things. 21. 6640-6650.

[6]. Vahiny Sharma, Ankur Gupta, Najam Ul Hasan, "Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions," Volume 2022, Article ID 9697545, https://doi.org/10.1155/2022/9697545.

[7]. Liang Huang and Hyung-Hyo Lee, "A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing," Volume 2020, Article ID 8859961, https://doi.org/10.1155/2020/8859961.

[8]. Ma, Ruonan & Zhang, Leyou & Wu, Qing & Mu, Yi & Rezaeibagha, Fatemeh. (2023). BE-TRDSS: Blockchain-Enabled Secure and Efficient Traceable-Revocable Data-Sharing Scheme in Industrial Internet of Things. IEEE Transactions on Industrial Informatics. PP. 1-10. 10.1109/TII.2023.3241618.

[9]. Rani, Deepti & Gill, Nasib & Gulia, Preeti. (2022). Design of a Cloud-Blockchain-based Secure Internet of Things Architecture. International Journal of Advanced Computer Science and Applications. 13. 10.14569/IJACSA.2022.0130851.

[10]. Sadrishojaei, Mahyar & Kazemian, Faeze. (2023). Development of an Enhanced Blockchain Mechanism for Internet of Things Authentication. Wireless Personal Communications. 132. 1-19. 10.1007/s11277-023-10731-7.

[11]. C. Li, X. Sun and Z. Zhang, "Effective Methods and Performance Analysis of a Satellite Network Security Mechanism Based on Blockchain Technology," in IEEE Access, vol. 9, pp. 113558-113565, 2021, doi: 10.1109/ACCESS.2021.3104875.

[12]. Wang, J., Wei, B., Zhang, J., Yu, X., & Sharma, P. K. (2021). An optimized transaction verification method for trustworthy blockchain-enabled IIoT. Ad Hoc Networks, 119, 102526. https://doi.org/10.1016/j.adhoc.2021.102526

[13]. Xie, G., Liu, Y., Xin, G., & Yang, Q. (2020). Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency. Security and Communication Networks, 2021(1), 9921209. https://doi.org/10.1155/2021/9921209

[14]. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2020). Multi-Layer Blockchain-Based Security Architecture for Internet of Things. Sensors, 21(3), 772. https://doi.org/10.3390/s21030772

[15]. Zhong, Y., Zhou, M., Li, J., Chen, J., Liu, Y., Zhao, Y., & Hu, M. (2020). Distributed Blockchain-Based Authentication and Authorization Protocol for Smart Grid. Wireless Communications and Mobile Computing, 2021(1), 5560621. https://doi.org/10.1155/2021/5560621

[16]. S. Namasudra, P. Sharma, R. G. Crespo and V. Shanmuganathan, "Blockchain-Based Medical Certificate Generation and Verification for IoT-Based Healthcare Systems," in IEEE Consumer Electronics Magazine, vol. 12, no. 2, pp. 83-93, 1 March 2023, doi: 10.1109/MCE.2021.3140048.

[17]. Hagui, I., Msolli, A., ben Henda, N. et al. A blockchain-based security system with light cryptography for user authentication security. Multimed Tools Appl 83, 52451–52480 (2024). https://doi.org/10.1007/s11042-023-17643-5

[18]. Z. Rahman, I. Khalil, X. Yi and M. Atiquzzaman, "Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System," in IEEE Communications Magazine, vol. 59, no. 5, pp. 128-134, May 2021, doi: 10.1109/MCOM.001.2000679.

[19]. Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R. et al. Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP J. on Info. Security 2021, 7 (2021). https://doi.org/10.1186/s13635-021-00122-5

[20]. Babu, E. S., Dadi, A. K., Singh, K. K., Nayak, S. R., Bhoi, A. K., & Singh, A. (2022). A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system. Expert Systems, 39(10), e12941. https://doi.org/10.1111/exsy.12941

[21]. Alzubi, J. A. (2021). Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. Computer Communications, 170, 200-208. https://doi.org/10.1016/j.comcom.2021.02.002

[22]. Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Journal of King Saud University - Computer and Information Sciences, 34(9), 6855-6871. https://doi.org/10.1016/j.jksuci.2022.06.014

[23]. M. Wazid, B. Bera, A. K. Das, S. P. Mohanty and M. Jo, "Fortifying Smart Transportation Security Through Public Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 17, pp. 16532-16545, 1 Sept.1, 2022, doi: 10.1109/JIOT.2022.3150842.

[24]. Mubarakali, A. An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. Wireless Pers Commun 127, 255–269 (2022). https://doi.org/10.1007/s11277-021-08212-w

[25]. X. Yang et al., "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3321-3332, 1 March1, 2022, doi: 10.1109/JIOT.2021.

[26]. Kamboj, P., Khare, S. & Pal, S. User authentication using Blockchain based smart contract in role-based access control. Peer-to-Peer Netw. Appl. 14, 2961–2976 (2021). https://doi.org/10.1007/s12083-021-01150-1

[27]. Z. Zhang, J. Zhang, Y. Yuan and Z. Li, "An Expressive Fully Policy-Hidden Ciphertext Policy Attribute-Based Encryption Scheme With Credible Verification Based on Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8681-8692, 1 June1, 2022, doi: 10.1109/JIOT.2021.3117378.

[28]. Lee, Y., Lee, H., Hsu, C., Kung, H., & Chiu, H. (2022). SEMRES - A Triple Security Protected Blockchain Based Medical Record Exchange Structure. Computer Methods and Programs in Biomedicine, 215, 106595. https://doi.org/10.1016/j.cmpb.2021.106595

[29]. Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Shishakly, R., Lutfi, A., & Alrawad, M. (2022). A New Blockchain-Based Authentication Framework for Secure IoT Networks. Electronics, 12(17), 3618. https://doi.org/10.3390/electronics12173618

[30]. Miao, J., Wang, Z., Wu, Z., Ning, X., & Tiwari, P. (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems With Applications, 237, 121329. https://doi.org/10.1016/j.eswa.2023.121329