Journal of Theoretical and Applied Information Technology
30th September 2025. Vol.103. No.18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# ADDRESSING KEY MANAGEMENT AND DATA INTEGRITY IN IIOT BASED HEALTHCARE: A BLOCKCHAIN APPROACH USING FERNET ENCRYPTION AND MERKLE ROOT PROOF OF WORK

**KUMAR M P[1], AKILA A[2]**

[1]Department of Computer Science and Information Technology, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, India
[2]Department of Computer Science and Information Technology, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, India
E-mail: [1] Kumarmp.mca@gmail.com, [2] akila.scs@velsuniv.ac.in

**ABSTRACT**

A blockchain based healthcare system in the Industrial Internet of Things (IIoT) improves transparency and interoperability by decentralizing patient data access and storage. It ensures tamper-proof records by enabling secure and seamless sharing of healthcare information among stakeholders and connected devices. However, IIoT devices are vulnerable to security issues like unauthorized attacks due to improper key management, which makes it easy for attackers to steal data. To overcome this issue, the Fernet Encryption Algorithm with Merkle Root Proof of Work (FEA-MRPoW) is proposed in blockchain-based healthcare systems for IIoT to increase security by generating strong data encryption which prevents unauthorized access and data confidentiality. The structure of Merkle root provides integrity of healthcare records whereas PoW protect against tampering for block validation. Therefore, this integration provides robust performance and ensures the safety of healthcare data in IIoT environments. The proposed FEA-MRPoW achieves a less encryption time of 0.298s when the number of attributes is 10 compared to existing methods like the Diagonal Digital Signature Algorithm (DDSA) with Merkle Patricia Hash Trie (MPHT).

**Keywords:** *Blockchain, Fernet Encryption Algorithm with Merkle Root Proof of Work, Healthcare, Industrial Internet of Things, Unauthorized Access.*

## 1. INTRODUCTION

The Industrial Internet of Things (IIoT) has accompanied a new era in the industrial sector, which is noticeable by the extensive incorporation of interconnected systems and devices. This revolution is redefining the standards of industry via real-time data collection, decision-making abilities, and processing [1]. The IIoT application involves Machine-to-Machine (M2M), Cyber-Physical Systems (CPS), translation and data exchange, and so on, which are determined as Industry 5.0 [2] [3]. Moreover, IoT's rapid extension network presents significant difficulties, especially in realms of integrity, data security, and privacy, which are vital in industrial settings [4]. Effectively analyzing and processing such large-scale data needs specialised analysis tools and robust computational abilities [5] [6]. In this context, blockchain technology is prominent for decentralized ledger systems, which act as an effective solution to address these difficulties. It can ensure transparency, data integrity, and trustworthiness positions for securing sensitive industrial data [7]. Therefore, a cyber safeguard system based on blockchain technology is established for offering highly secured health ledger data to healthcare providers in combined domain environments. The existing systems in maintaining healthcare records struggle with asset theft, transfer delay, eavesdropping, record duplication, etc. [8]. Also, stored data in an exterior server are sensitive for security and accessing data to healthcare management. Therefore, a new method for patient care is required to be established with the combination of numerous diagnostic data and patient data into blockchain-enabled decentralized trust system in healthcare. By utilizing blockchain in IIoT based healthcare systems has the probability to enhance security, privacy, and transparency, as well as minimise costs.

Blockchain based healthcare manages the entity's trust in the healthcare system by enabling it to handle

the data. It assists all healthcare users in verifying healthcare document authenticity which prevents fraud. Blockchain stores healthcare information like certification, unique identification number, and so on in the form of blockchain structure [9]. It minimises the losses from counterfeit or gray market trading and enhances the healthcare system. Without scalable, trusted, and effective secure architecture, the invention of communication systems in the industrial sector becomes ineffective and challenging [10] [11]. Attackers reveal the sensor data, user's privacy, and operating system program and later attain malicious actions by maintaining machines remotely, which causes serious illegal actions by deploying sensitive shared data [12]. Besides, the smart contract function is applied as an agreement among stockholders for automatically executing terms while conditions are satisfied on both sides [13]. Moreover, smart contract function implementation enhances the security of healthcare documents [14]. Accordingly, integrating the healthcare system and blockchain automates the creation and verifies a healthcare record. Hence, the benefits of blockchain technology offer trust and transparency in the healthcare system [15] [16]. Therefore, it enhances security with the management of masquerade, counterfeiting, and determining theft attacks [17] [18]. However, IIoT devices are vulnerable to security issues like unauthorized attacks due to improper key management, which makes it easy for attackers to steal data. Hence, there is a need for secure and efficient key management mechanism in IIoT environments to avoid unauthorized data access. Without proper key management, even advanced encryption method become ineffective. Therefore, this research proposes a Fernet Encryption Algorithm with Merkle Root Proof of Work (FEA-MRPoW) to address key management vulnerabilities by ensuring secure data encryption in blockchain based healthcare systems within the IIoT environment. This prevents unauthorized data interception and ensures trustworthy and secure communication in IIoT.

The major contribution of this work is determined as,

- Fernet encryption is used to ensure secure and authenticated data transmission among blockchain nodes and IIoT device. It makes end-end confidentiality of patient records, protect against unauthorized access, and supports rapid encryption and decryption with less complexity compared to Diagonal Digital Signature Algorithm (DDSA) with Merkle Patricia Hash Trie (MPHT) which enhance data integrity and effectiveness of healthcare data management system.
- Merkle tree ensures data integrity through organizing healthcare records into hierarchical hash-based structure where any tampering with individual records is rapidly identified by hash mismatches. It enable IIoT devices and users for validating huge volumes of healthcare data with less complexity.
- PoW creates trust in decentralized manner through allowing nodes to independently verify transactions without depending on central authority. Moreover, PoW involves an extra layer of protection and authenticity which prevents unauthorized modification and reinforcing the immutability of healthcare records in IIoT.

This research paper is given as follows: Section 2 denotes the literature survey and Section 3 explains the proposed methodology. Section 4 analyzes experimental results, and the conclusion of this research paper is given in Section 5

## 2. LITERATURE SURVEY

A. Divya Preetha and T.S. Pradeep Kumar [19] developed a Diagonal Digital Signature Algorithm (DDSA) with Merkle Patricia Hash Trie (MPHT) that exploits blockchain for securing medical record sharing among surgeons and dissimilar patients. The data-sharing model was integrated with smart contract technology which prevents illegal participants from determining medical records and minimizes decryption overhead. File loss rate and transmission delay were minimized greatly by utilizing a data-sharing scheme in healthcare. However, as the number of records grows managing MPHT increases retrieval and storage complexity which affects efficiency and system performance.

G. M. Karthik et al. [20] established a hybrid Elman Neural-based Blowfish blockchain for securing healthcare data. Elman network represented continuous monitoring to predict malicious actions in multimedia data. An established approach contains two significant stages: crypto analysis and monitoring stage. A system eliminates the attacks in the monitoring stage whereas crypto analysis encrypts data with the generated key. Crypto analysis was applied, which increased the confidentiality rate by hiding data from third parties. Nevertheless, the hybrid method demands extensive processing power,

which increases latency in securing healthcare multimedia data on the blockchain.

S. Vidhya and V. Kalaivani [21] presented a Blockchain-based Access Control Scheme (BACS) with Multiple Party Authority (MPA), proxy re-encryption, and smart contracts for securing Electronic Health Record (EHR). The data was encrypted using Lightweight Fused Cryptographic (LFC) with doctor and patient signatures to ensure both integrity and confidentiality. Later, encrypted EHR was stored on Interplanetary File Systems (IPFS) was decentralized file storage platform. Smart contracts verify the user's authenticity which increases security from external and internal attacks. However, managing cryptographic keys in a multi-party authority system with re-encryption was challenging which increased the mismanagement and key exposure risk.

Pratima Sharma et al. [22] suggested an Identity based Encryption (IBE) based blockchain to offer security in healthcare data. Smart contracts were utilized to attain various healthcare system functionalities such as access control, security, and integrity checking which was beneficial to each stakeholder. In the suggested scheme, a swarm was employed for storing healthcare data which allows the users to easily validate the data integrity. Nevertheless, IBE needs a trusted authority to generate private keys which creates a single failure point and comprises security in healthcare data whether authority was breached.

Ashish Tomar et al. [23] introduced a Blockchain-based Internet of Medical Things (IoMT) Authenticated Key Exchange (BIoMTAKE) by utilizing hyperledger fabric. This protocol removes the requirement for a single trusted authority and makes secure access to data produced by IoMT devices. Before accessing or sharing data from a distributed healthcare system, BIoMTAKE provides a secured shared session to avoid unauthorised access from authenticated devices. However, the introduced approach increased encryption and decryption time due to the computational overhead of managing complex cryptographic methods which results in slower transaction processing.

P. Vinayasree and A. Mallikarjuna reddy [24] established a scalable and secure blockchain based healthcare system to handle extensive patient data which provides high security. The Compact Patricia Tries (CPTs) and Adaptive Partitioned Filters (APTs) were used to enable effective data access and management whereas Go concurrency model and Sharded Byzantine Optimized Consensus (SBOC) provide parallel transaction processing. Moreover, security was provided via Patricia tries, bloom filters enhanced by Immutable blockchain ledger protected by Practical Byzantine Fault Tolerance (PBFT).

Murari Kumar Singh [25] developed a ligtweight proof of hybrid security system to enhance trust in distributed computing environment. The hybrization of Proof of Stake (PoS) and Proof of Work (PoW) were hybrid system which provide decentralized and robust blockchain ecosystem. Moreover, the combination of trust factor computation provide significant solution for the problem faced by blockchain network. However, hybrid security system lack robustness against intricate and evolving threats due to simplified crytographic assumptions.

The existing method had limitations like high latency, lack of robustness, vulnerable to unauthorized access, enhanced encryption and decryption time due to inefficient encryption methods. Hence, growing need for secure and verifiable method is required to enhance data integrity without increasing complexity. Therefore, FEA-MRPoW is proposed by integrating secure, symmetric Fernet encryption and verifiable MRPoW that ensures data integrity. The MRPoW minimize the risk of unauthorized attacks whereas Fernet ensures rapid and authenticated encryption and decryption which minimize time. The significance of proposed method enable rapid and secure encryption of patient data gathered from IIoT devices supports time sensitive healthcare application.

## 3. PROPOSED METHODOLOGY

In this research, users (patients and doctors), IIoT devices, admin, swarm storage, and smart contract are the primary entities considered which are connected as a Peer-to-Peer (P2P) network. Initially, the admin transmits key generation requests to smart contracts to generate public and private key and global parameters for the admin. Next, the blockchain performs the contract's registration function. Hence, credentials are produced to share with the admin. For login purposes, the admin employs shared credentials and healthcare services are accessed. The user transfers the registration request to the admin with email ID, user name, hospital, etc. Moreover, the admin stores the user's information, whereas the registration process is executed to generate login credentials like password and user ID. Admin generates these credentials for users and by utilizing these, users log into the system. Subsequently, users log in to the proposed

architecture by employing shared information and the service is accessed such as downloading, uploading, and sharing EHRs with registered users. Users transfer healthcare data to the blockchain for uploading EHR by utilizing the file upload option. Furthermore, every registered IIoT device gathers data in EHR form and links the proposed method employing Wi-Fi for uploading the gathered user's healthcare data. Then, the blockchain performs the associated smart contract function for encrypting data utilizing Fernet by storing it in a distributed manner. The smart contract returns a unique file hash once the EHR is successfully stored. At last, the generated file hash is transmitted to the user to obtain the associated EHR. Figure 1 depicts a workflow of blockchain-based architecture using healthcare data.

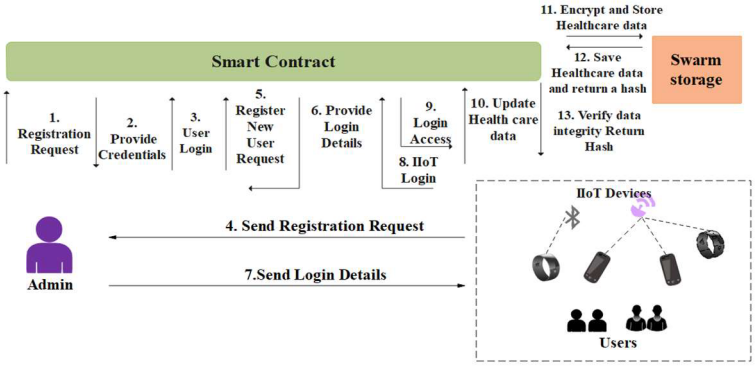


*Figure 1: Workflow of block chain based proposed architecture using healthcare*

### 3.1 System Model

All the entities utilized in this research are explained in detail below

Admin: It is a special user who acts as a Certificate Authority (CA) to generate valid digital identities and other kinds of credentials for members to join the network. Admin provides a unique identity to register patients, doctors, and IIoT devices. Once registration is completed, patients and doctors download and upload EHR from the established system. Before uploading documents, the smart contract provides EHR's confidentiality on decentralized storage utilizing fernet encryption. The smart contract authenticates the file's integrity by recomputing its hash and comparing it with the stored hash. If both hashes match, access is granted; otherwise, it is denied.

IIoT devices: These are sensors or IIoT devices to gather EHR data directly from patients. IIoT gadgets are beneficial for maintaining health factors like body temperature, weight, sugar levels, calories consumed, and so on. It gathers healthcare data for users and contains limited processing, low power, and storage capacity.

User: The users in the architecture consist of patients and doctors who register on the portal by providing valid personal information. Each user is permitted to upload EHRs by utilizing a portal and each data is stored on a swarm in encrypted form. Also, doctors and patients are enabled to access information gathered from IIoT devices and subsequently healthcare data is shared with registered users.

Swarm: In the proposed scheme, users' and physicians' encrypted data are stored in a distributed manner across storage nodes. These storage nodes rely on a swarm while the blockchain network manages the entire framework. Swarm employs a technique of solving content in that location is extracted from the document's content.

Smart Contract: It is a function set that shows core functionality and only registered users perform it for submitting requests in the blockchain.

### 3.2 System Setup

This section defines certain pre-requisite functions to establish the variables for the proposed method. A detailed description of each function is presented below.

#### 3.2.1 Global setup

It performs the global method and considers the global parameter as input and the admin's Master Key $MK$ and Public Key $PK$ as output. Admin chooses a bilinear group $G$ of generator $g$ and prime number $p$ and involves two random numbers $a, b \in Z_p$ where $Z_p$ represents prime order. Assume $G$, $G_r$ are group of multiplicative cyclic and map $G \times G \rightarrow G_r$ satisfying subsequent properties known as bilinear pairing or map $(p, G, g, e, G_r, H_1, H_2)$.

1. $e(u^a, v^b) = e(u, v)^{ab}, \forall u, v \epsilon G, a, b \epsilon Z_p$

2. If g is a generator of $G$, the later $e(g,g)$ is a generator of $G_r$
3. $e(u,v)$ is effectively calculated for each $u,v \epsilon G$
4. Assume $H_1: \{0,1\}^* \rightarrow G, H_2: G_r \rightarrow \{0,1\}'$ represents 2 hash functions which are attribute to random component of $G_r$ and $G$.
5. $PK$ is denoted as $\{G, g, g^a, g^b, e(g,g)^b, H_1\}$, where $(a,b) \epsilon Z_p$
6. $MK$ is illustrated as $\alpha$

### 3.2.2 Key generation

Admin employs $MK$ and $PK$ utilises key generation which considers global parameters as input, as well as public and secret keys, are output. A mathematical description for key generation is explained as follows,

1. Consider the Global parameters as $(p, G, g, e, G_r, H_1, H_2)$
2. All users' IIoT devices and unique IDs are used for generating the user's public key and IIoT devices which are denoted as $ID_u$ where $ID_u \epsilon \{0,1\}^*$
3. Subsequently, parameter params as $(p, g, Q, H_1, H_2]$, where $\alpha^R \leftarrow Z_p, Q = G^a$
4. Each user's secret key is employed $SK_u = H_1(ID_u)^a$, where $ID_u \epsilon \{0,1\}^*$.

### 3.2.3 Encryption

Before the IIoT device or user uploads the file to storage, key generation is performed, followed by fernet encryption to ensure data confidentiality and prevent unauthorized access. It provides easy-to-use symmetric encryption with key generation makes effective to secure sensitive data. Moreover, the encryption process involves a timestamp which allows expiration-based security to prevent replay attacks. Fernet encryption is similar to Advanced Encryption Standard (AES) which is employed to encrypt healthcare data by utilizing symmetric key cryptography. Fernet offers key rotations that are produced via "MultiFernet" during encrypting plain or ciphering. Moreover, fernet performs an inverse function to convert cipher text to plain text for decrypting encoded text and output is denoted as "string" values from bytes. Fernet encryption and decryption primarily involves three steps: key generation, assigning the key value to a chosen variable, and converting plain text into ciphered text. Compared to traditional methods like AES, fernet offers users with highly secured key and involves built-in authentication which prevents data tampering and ensures message integrity. Moreover, fernet encryption provides strong encryption to prevent data from being eavesdropped and private communications without a key such as time-stamping, sign-stamping, random allocation for security, key generation via secure mechanism and adopting secure methods towards encrypting messages. Fernet provides confidentiality by encrypting sensitive information like patient records, which helps to prevent unauthorized access. This method is rapid and effective by ensuring minimal delay while accessing healthcare data. Figure 2 represents the Fernet encryption method which increases security and ensures that sensitive healthcare information is protected from unauthorized access.

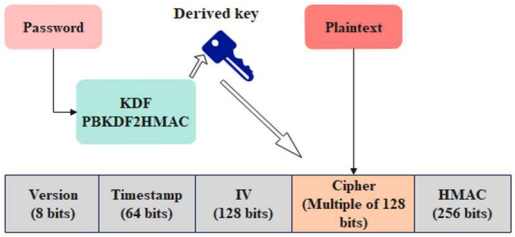


*Figure 2: Architecture of Fernet encryption*

### 3.3 Smart Contract

After encryption and decryption, smart contract primarily performs all significant tasks depending on received data. In blockchain networks, every communication is accomplished through digitally signed messages. Moreover, IIoT devices are linked to blockchain networks by utilizing Wi-Fi. Therefore, all the network entities obtain an authentication trace intimation of the smart contract process. It involves different functions like IIoT/user registration, access control function, data outsourcing function, and integrity checking function. A detailed description of the process is illustrated as follows:

### 3.3.1. Registration

Admin accomplishes key generation model for generating master and public keys. Once, the master key is generated, the admin utilizes fernet encryption to produce a secret key for IIoT devices and users. Initially, users transmit a registration request to the admin by utilizing a unique identity and later store that information on the blockchain by executing key generation. Finally, the admin shares the produced

credential share with a user after the key generation process is performed.

### 3.3.2. Data Outsourcing Function

In a swarm storage system, IIoT device or user generates this function to store healthcare data and manage metadata on the blockchain. Initially, this process splits the file into various shards and employs the SHA256 hashing method for generating the hash. Every file is incorporated and then the root hash is computed. Once, the data is stored in metadata, the user makes ciphertext by performing secret key-based fernet encryption. Then, the blockchain transmits outsourced data to the swarm for storage purposes. On effective data storage, swarm transmits a confirmation to the blockchain by returning transaction ID to a user.

### 3.3.3. Access control function

It enables the admin to check an access control before permitting the user to decrypt requested data. Users are allowed to determine data kept on decentralized storage and initially, the admin checks user authorization by utilizing metadata kept on blockchain. If the user is authorized, that means the user identity matches file details; the requested file is decrypted and converted into plaintext for access; otherwise, it is denied.

### 3.3.4. Integrity Checking Function

After access control, a checking function is performed to ensure the integrity of stored healthcare data. Users request to check the integrity of the file in the blockchain, and later verification process is employed. The user recovers stored the requested file's Merkle root and recomputes the Merkle root. If both files are similar, integrity is verified; otherwise, it shows false. In the blockchain, PoW [26] ensures data integrity by validating tamper-resistant transactions. A Merkle tree structures transactions into a hierarchical hash-based format where each node's hash is based on its child nodes which ensures secure and effective verification. The root hash uniquely denotes all transactions by enabling rapid integrity checks. PoW is utilized in Bitcoin 2 to ensure that all participating nodes are on similar blockchain branches. Initially, a node determines the solution, generates a new block and transfers data to other nodes in the network. This allows the data to be included in the block for rapid verification of its accuracy. In history, a single block is altered by attackers by modifying the block hash and interpreting the whole successful blockchain as invalid. Simultaneously, while multiple users verify a block, a network divides until new blocks are determined with each node converging to the longest chain of blocks.

Moreover, transaction data collection and block header are two elements presented in blockchain block whereas every node in PoW denotes a block header hash value. A block header involves nonce, pre, Merkle tree parameters, and transaction counter. The "pre" represents the hash function of the prior block header, "nonce" denotes the PoW block's solution, "Ri" indicates the Merkle tree root which is established by the transaction counter. Block headers comprise minors and nonce that are altered regularly to make different hash values. While a node obtains the required value, the block is broadcasted to all other nodes, which is verified independently that the hash value is correct. PoW in bitcoin is denoted as mining and nodes evaluate a hash value known as miners. In blockchain, using PoW and Merkle tree for data integrity ensures that transactions remain secure, verifiable, and tamper-proof. PoW avoids malicious alterations whereas Merkle tree makes effective verification of data consistency. This integration makes immutability, unauthorized modifications which provides a trusted and decentralized ledger for secure validation and data storage.

## 4. EXPERIMENTAL RESULTS

The proposed FEA-MRPoW is simulated for 400 patients in Python 3.4 environment with 128 GB RAM, 12th Gen Intel(R) Core(TM) i7-12700K (3.60 GHz) processor, Windows 11 pro operating system, and 24H2 version. The os, cryptography, psutil, time, cryptography, render_template, request, redirect, url_are the libraries used in this research. Moreover, a total of 50 virtual IIoT devices are simulated, each generating time-stamped health data for associated virtual patients. The performance measures like encryption time, decryption time, processing overhead time, computation time, and delay are used to analyze the model performance.

### 4.1 Performance Analysis

Figure 3 determines the performance analysis of encryption time (ms) based on a number of user attributes. The x-axis indicates user attributes ranging from 1 to 9 whereas the y-axis shows encryption time. As the number of user attributes increases, encryption time also increases for all methods. However, the proposed FEA-MRPoW

consistently obtains less encryption time of 2.0 ms for 9th user attributes compared to existing methods like AES and ChaCha20. This performance enhancement is because of lightweight cryptographic operations that employs symmetric encryption with precomputed keys which minimize computational complexity. Moreover, optimized key management in Fernet makes effective key derivation that reduces processing overhead.

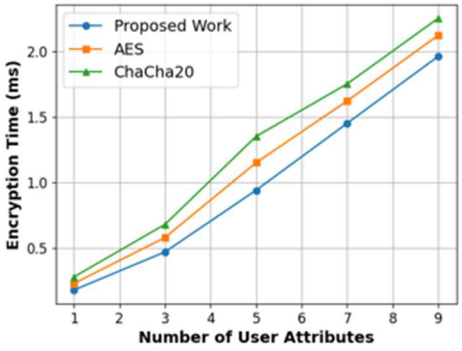


*Figure 3: Performance analysis of encryption time*

Figure 4 determines the performance evaluation of decryption time by varying the number of user attributes. The existing methods like AES and ChaCha20 are compared with the proposed FEA-MRPoW. Compared to these methods, the FEA-MRPoW obtains a less decryption time of 1.75 ms for 9th user attributes because of its effective cryptographic mechanism. Fernet provides symmetric encryption with less computational overhead, which ensures rapid key-based decryption. The combination of Merkle root minimizes verification complexity by making effective integrity checks whereas PoW ensures decryption remains lightweight. A decentralized nature of the Merkle tree structure enables rapid authentication of data blocks. Moreover, streamlined decryption and optimized key management reduce processing delays, which contribute to less decryption time.

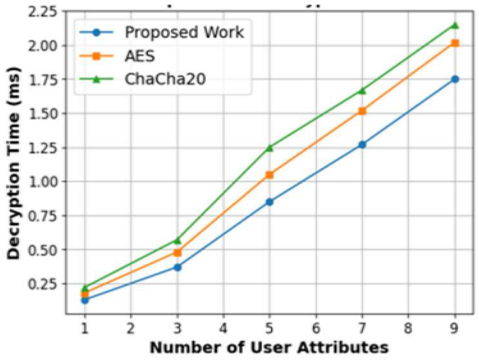


*Figure 4: Performance evaluation of decryption time*

Figure 5 represents the performance evaluation of processing overhead time (ms). Due to its effective cryptographic structure, FEA-MRPoW obtains less processing overhead time compared to existing methods like AES and ChaCha20. Fernet provides symmetric encryption with less computational complexity that minimizes decryption and encryption delays. Merkle root enables rapid data integrity verification with logarithmic time complexity whereas PoW makes effective key derivation. The combination of these methods makes a streamlined encryption process which minimizes redundant computations. Moreover, parallel processing in Merkle tree verification increases effectiveness and leads to lower processing overhead time.

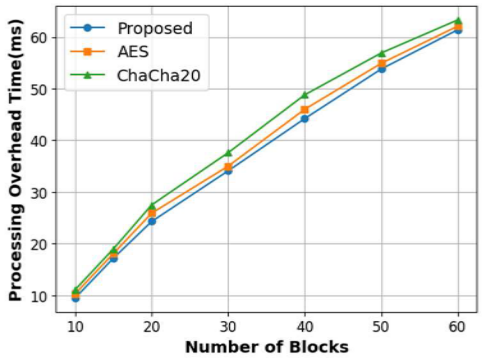


*Figure 5: Performance evaluation of processing overhead time*

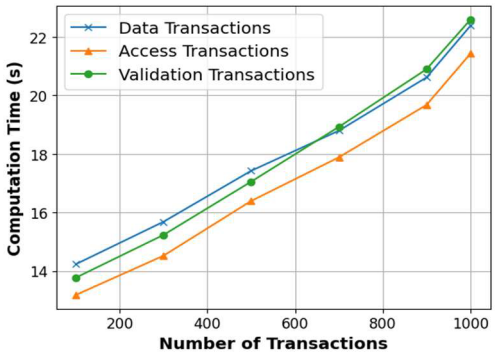


*Figure 6: Performance evaluation of computation time*

Figure 6 denotes a performance evaluation of computation time by varying number of transactions. For all three categories, as the number of transactions increases, computation time also increases, which represents a positive correlation. Among these, access transaction consistently yields the least computation time while data transaction generally takes more time to process. Validation transactions follow data transactions however, they indicate slightly lower computation times at high transaction numbers. The differences in computation time are

because of varying complexities in generating each transaction type where data transactions pertain to a more intensive process.

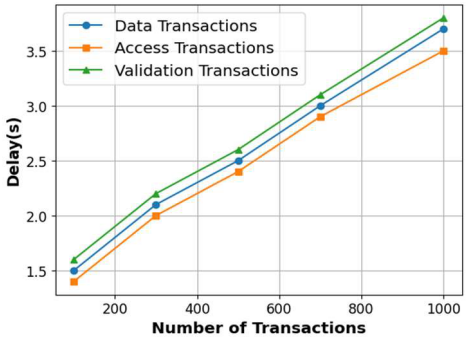


*Figure 7: Performance analysis of delay*

Figure 7 shows a performance analysis of delay (ms) with three kinds of transaction data, access, and validation. As the number of transactions increases from 200 to 1000, the delay steadily increases for all transaction types. Validation transactions show the highest delay because of additional computational overhead for verifying correctness and integrity. Data transactions nearly follow as they comprise encryption and storage processes. Access transactions suggest lease delay as they majorly focuses on retrieval with less verification. Therefore, the access transactions acquire a less delay of 3.5 ms at the 1000th number of transactions compared to data and validation transactions respectively.

### 4.2 Comparative Analysis

Tables 1 to 3 present a comparative analysis of existing methods. In this section, the proposed FEA-MRPoW method value is simulated based on existing method values. The existing methods like [19], [20], and [21] are compared with the proposed FEA-MRPoW. While compared to these methods, the FEA-MRPoW achieves a less encryption time of 0.298s at the attributes considered as 10 due to it ensuring integrity, data security, and scalability. Fernet encryption indicates a strong symmetric key encryption which helps to protect patient data from unauthorized access. Moreover, Merkle root enables effective verification which ensures medical records integrity. PoW secures the blockchain against malicious attacks and provides a consensus process. Therefore, this makes reliability and trust in healthcare by managing effective transactions in IIoT systems.

*Table 1: Comparative analysis of proposed FEA-MRPoW with DDSA-MPHT*

| Methods | Performance measures | No. of attributes | | | | |
|---|---|---|---|---|---|---|
| | | 10 | 20 | 30 | 40 | 50 |
| DDSA-MPHT [19] | Encryption time (s) | 0.334 | 0.742 | 1.129 | 1.545 | 1.896 |
| | Decryption time (s) | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 |
| | Time consumed by decrypt contract (s) | 0.267 | 0.610 | 0.98 | 1.170 | 1.506 |
| Proposed FEA-MRPoW | Encryption time (s) | 0.298 | 0.467 | 0.876 | 1.128 | 1.279 |
| | Decryption time (s) | 0.02 | 0.02 | 0.02 | 0.02 | 0.02 |
| | Time consumed by decrypt contract (s) | 0.198 | 0.472 | 0.65 | 0.873 | 0.987 |

*Table 2: Comparative analysis of proposed FEA-MRPoW with ENbBBM*

| Methods | Encryption time (ms) | Execution time (ms) | Decryption time (ms) | Confidential rate (%) | Error rate (%) |
|---|---|---|---|---|---|
| ENbBBM [20] | 4.56 | 9.68 | 3.89 | 94.6 | 0.09 |
| Proposed FEA-MRPoW | 2.39 | 6.49 | 2.98 | 97.3 | 0.05 |

*Table 3: Comparative analysis of proposed FEA-MRPoW with LFC*

| Methods | Performance measures | File Size | | | | |
|---|---|---|---|---|---|---|
| | | 25KB | 50KB | 1MB | 2MB | 2MB |
| LFC [21] | Encryption time (ms) | 100 | 200 | 220 | 250 | 220 |
| | Decryption time (ms) | 50 | 70 | 65 | 60 | 150 |
| Proposed FEA-MRPoW | Encryption time (ms) | 80 | 150 | 190 | 220 | 190 |
| | Decryption time (ms) | 30 | 55 | 40 | 45 | 110 |

### 4.3 Discussion

This section shows a discussion based on the advantages of FEA-MRPoW and the limitations of existing methods. Existing method's limitations like if the number of records grows, managing MPHT [19] increases retrieval and storage complexity which affects efficiency and system performance. The hybrid method [20] demands extensive processing power which increases latency in securing healthcare multimedia data on the blockchain. Managing cryptographic keys in a multi-party authority system with re-encryption [21] was challenging which increased the mismanagement and key exposure risk. IBE [22] needs a trusted authority to generate private keys which creates a single failure point and comprises security in healthcare data whether authority was breached. The proposed FEA-MRPoW overcomes these existing method limitations by providing data integrity and security. Fernet ensures symmetric encryption and secure data with less computational overhead. Merkle root enables effective data integrity verification whereas PoW increases security by including an additional layer of validation which increases data authenticity and prevents unauthorized access. Hence, this process supports scalability in IIoT systems with a large number of devices by maintaining trustworthiness and high system effectiveness.

### 4.4 Difference from Prior Research

The proposed FEA-MRPoW significantly differs from previous research in terms of encryption efficiency, data integrity, key management, and system scalability. Which prior methods like DDSA-MPHT rely on intricate digital signatures with enhanced storage and retrieval overhead whereas ENbBBM contained key exposure risks but proposed method simplifies encryption by utilizing Fernet which provides authentication and timestamping. This ensures secure and low-latency data encryption which is appropriate for IIoT environments. Furthermore, unlike tradition system suffer efficient integrity checks, the employment of MRPoW provides verifiable and tamper-evident data validation. PoW assist to ensure decentralized consensus and avoids unauthorized access which previous works does not emphasize. These enhancement enable proposed method more scalable, robust, and practical for securing healthcare data in IIoT environments.

## 5. CONCLUSION

This research aimed to implement secure and effective block-chain based healthcare system for IIoT by addressing challenges like unauthorized access, inefficient key management, and data integrity. To achieve these objectives, proposed FEA-MRPoW integrates Fernet encryption for authenticated data security, Merkle tree for verifying integrity, and PoW for decentralized validity. Fernet encryption secures data via symmetric key encryption which makes resistant to unauthorized access. Merkle tree provides data integrity by identifying unauthorized changes whereas PoW increases security by preventing tampering via computationally intensive validation. The experimental results show that FEA-MRPoW achieves a less encryption and decryption time of 0.298s and 0.02s at a number of attributes 10 due to rapid encryption and decryption with lower overhead which maintains high security via symmetric key encryption and hash-based verification compared to existing methods like DDSA-MPHT. These findings demonstrates the effective realization of research goals which ensures integrity and confidentiality of healthcare data in IIoT environment. By increasing key management and reducing computational complexity, the proposed FEA-MRPoW significantly minimize delay and enhances the effectiveness of healthcare data access and storage. By ensuring integrity and security, the proposed FEA-MRPoW offers an efficient and robust solution for blockchain based healthcare applications in IIoT environment. However, the use of PoW lead to block confirmation latency during network congestion and high transaction volume which affect timely access to healthcare records. In the future, adaptive consensus mechanism will be used to adjust network load and minimize delay.

## REFERENCES

[1] M. Usman, M.S. Sarfraz, M.U. Aftab, U. Habib, and S. Javed, "A blockchain based scalable domain access control framework for industrial internet of things", *IEEE Access*, Vol. 12, 2024, pp. 56554-5570.

[2] F. Khallaf, W. El-Shafai, E.S.M. El-Rabaie, F.E.A. El-Samie, "Blockchain-based color medical image cryptosystem for industrial", Internet of Healthcare Things (IoHT)", *Multimedia Tools and Applications*, Vol. 84, 2024, pp. 25749–25803.

[3] A. Sasikumar, L. Ravi, K. Kotecha, A. Abraham, M. Devarajan, and S. Vairavasundaram, "A secure big data storage framework based on blockchain consensus mechanism with flexible finality", *IEEE Access*, Vol. 11, 2023, pp. 56712-56725.

[4] Y. Bobde, G. Narayanan, M. Jati, R.S.P. Raj, I. Cvitić, and D. Peraković, "Enhancing industrial IoT network security through blockchain integration", *Electronics,* Vol. 13, No. 4, 2024, p. 687.

[5] N. Xiao, Z. Wang, X. Sun, J. Miao. "A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things", *Alexandria Engineering Journal*, Vol. 86, 2024, pp.631-643.

[6] A. Sasikumar, L. Ravi, M. Devarajan, A. Selvalakshmi, A.T. Almaktoom, A.S. Almazyad, G. Xiong, A.W. Mohamed, "Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things", *IEEE Access*, Vol. 12, 2024, pp. 12586-12601.

[7] M.S. Islam, M.A.B. Ameedeen, M.A. Rahman, H. Ajra, Z.B. Ismail, "Healthcare-chain: blockchain-enabled decentralized trustworthy system in healthcare management industry 4.0 with cyber safeguard", *Computers,* Vol. 12, No. 2, 2023, p. 46.

[8] A.I. Taloba, A. Elhadad, A. Rayan, R.M. Abd El-Aziz, M. Salem, A.A. Alzahrani, F.S. Alharithi, C. Park, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare", *Alexandria Engineering Journal*, Vol. 65, 2023, pp. 263-274.

[9] P. Sharma, S. Namasudra, R.G. Crespo, J. Parra-Fuente, M.C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain", *Information Sciences*, Vol. 629, 2023, pp. 703-718.

[10] S.M. Umran, S. Lu, Z.A. Abduljabbar, and V.O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry", *Internet of Things*, Vol. 24, 2024, p. 100969.

[11] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system", *Wireless networks*, Vol. 29, No. 3, 2023, pp. 1005-1015.

[12] P.C. Sharma, M.R. Mahmood, H. Raja, N.S. Yadav, B.B. Gupta, V. Arya, "Secure authentication and privacy-preserving block chain for industrial internet of things", *Computers and Electrical Engineering,* Vol. 108, 2023, p. 108703.

[13] R. Vatambeti, E.P. Krishna, M.G. Karthik, and V.K. Damera, "Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things", *Cluster Computing,* Vol. 27, No. 2, 2024, pp. 1625-1637.

[14] A. Lakhan, M.A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, N. Kumar, "DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system", *Scientific Reports,* Vol. 13, No. 1, 2023, p. 4124.

[15] D. Rani, R. Kumar, N. Chauhan, "A secure framework for IoT-based healthcare using blockchain and IPFS", *Security and Privacy*, Vol. 7, No. 2, 2024, p. e348.

[16] S. Abdullah, J. Arshad, M.M. Khan, M. Alazab, and K. Salah, "PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle", *Complex & Intelligent Systems*, Vol. 9, No. 3, 2023, pp. 3023-3041.

[17] A. Raj, S. Prakash, "Privacy preservation of the internet of medical things using blockchain", *Health Services and Outcomes Research Methodology*, Vol. 24, No. 1, 2024, pp.112-139.

[18] S. Alsubai, A. Alqahtani, H. Garg, M. Sha, A. Gumaei, "A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records", *Complex & Intelligent Systems*, Vol. 10, No. 5, 2024, pp. 6117-6141.

[19] A.D. Preetha, T.P. Kumar, "Securing IoT-based healthcare systems from counterfeit medicine penetration using Blockchain", *Applied Nanoscience*, Vol. 13, No. 2, 2023, pp. 1263-1275.

[20] G.M. Karthik, A.S. Kalyana Kumar, A.B. Karri, N.P. Jagini, "Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data", *Wireless Networks*, Vol. 29, No. 6, 2023, pp. 2481-2493.

[21] S. Vidhya, V. Kalaivani, "A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme", *Peer-to-Peer Networking and Applications*, Vol. 16, No. 2, 2023, pp.900-913.

[22] P. Sharma, N.R. Moparthi, S. Namasudra, V. Shanmuganathan, C. H. Hsu, Blockchain-based

IoT architecture to secure healthcare system using identity-based encryption", *Expert Systems*, Vol. 39, No. 10, 2022, p. e12915.

[23] A. Tomar, N. Gupta, D. Rani, S. Tripathi, "Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system", *Internet of Things*, Vol. 23, 2023, p. 100849.

[24] P. Vinayasree, A.M. Reddy, "A Scalable and Secure Blockchain-Based Healthcare System: Optimizing Performance, Security, and Privacy with Adaptive Technologies", *Journal of Theoretical and Applied Information Technology,* Vol. 102, No. 22, 2024, pp. 8084-8103.

[25] M.K. Singh, S.K. Pippal, V. Sharma, "Lightweight blockchain mechanism for secure data transmission in healthcare system", *Biomedical Signal Processing and Control,* Vol. 102, 2025, p. 107411.

[26] M. Rukhiran, S. Boonsong, P. Netinant, "Sustainable optimizing performance and energy efficiency in proof of work block chain: A multilinear regression approach", *Sustainability,* Vol. 16, No. 4, 2024, p. 1519.