# A Novel and Secure Machine Learning-based Hyperledger Blockchain for IoT Healthcare

Sidra Aslam, Saba Aslam, Taotao Wang, *Member, IEEE*,
Daquan Feng, *Member, IEEE*, and Shengli Zhang, *Senior Member, IEEE*

***Abstract*—Data privacy protection and secure sharing are the main issues faced by smart healthcare IoT systems. In medical uses, patient health information is frequently kept in the cloud, which limits the user's ability to entirely control their data. Additionally, standard encryption keys do not sufficiently mitigate the risks posed by malicious entities like compromised cloud service providers. To address these issues, blockchain technology, combined with Internet of Medical Things (IoMT) can securely safeguard patient medical records through a peer-to-peer, secure, and collective ledger. Therefore, we propose a novel IoT-driven architecture that leverages blockchain technology to protect patient medical files from tampering and unauthorized access. This architecture integrates patient medical files with blockchain and is enhanced by a combination of Bidirectional Long Short-Term Memory (BiLSTM) networks and Convolutional Neural Networks (CNN). Utilizing blockchain for the transmission of encrypted data significantly strengthens data security and minimizes the risk of data breaches. The process of generating encryption and decryption keys through a coupled CNN and BiLSTM ensures the robustness and uniqueness of these keys. Additionally, the selection of the best key is performed using the Gradient Descent Optimization Algorithm (GDOA), which demonstrates the effectiveness and efficiency of the encryption and decryption process. We also compare the implementation of our model with existing technologies, assessing its performance based on various metrics, including restoration efficiency, response time, record time, key generation time, encryption time, decryption time, turnaround time, and overall running time. Our proposed method is confirmed to be more effective than current techniques in terms of these performance metrics.**

***Index Terms*—Blockchain, Hyperledger Fabric, IoMT, AES + Twofish, BiLSTM, GDOA.**

## I. Introduction

AFTER decades of development, healthcare management systems have leveraged the rapid advancement of Internet technologies to achieve remarkable progress in various areas, including both front-end and back-end systems [1]. This evolution has streamlined traditional record-keeping systems designed for diagnosis, patient management, equipment management, treatment, and so on [2], [3]. Meanwhile, maintaining personal healthcare data or patient medical files remains a crucial responsibility for hospitals.

Data confidentiality must be carefully protected, whether during personal use by patients or in academic exchanges between hospitals. Ultimately, the beneficiaries of these data movements are the patients themselves. Therefore, it is imperative to address the challenges associated with patient file storage systems as a critical issue to ensure accurate diagnoses, high-quality services, and effective treatments for patients [4], [5], [6].

The healthcare industry is undergoing a major transformation due to the integration of Internet of Things (IoT) technologies. This development facilitates the use of connected IoT devices that can collect, process, and exchange healthcare data across various operational tasks [7]. The IoT offers significant potential for improving healthcare outcomes, enhancing care quality, and increasing operational efficiency while reducing costs through the continuous collection, analysis, and sharing of data. Modern medical remote monitoring tools, sensors, wearable devices, and mobile applications are fundamental in this specific field [8]. Compared to outdated healthcare infrastructures, the IoT integrates these technologies to enable constant data gathering, transmission, and analysis, creating new avenues for medical record monitoring and exchange. The implementation of IoT in healthcare has already shown promise in reducing hospital visits, shortening patient stays, and cutting associated healthcare costs [9]. Additionally, IoT technology addresses multiple challenges in traditional healthcare systems by providing real-time access to patient information, empowering patients, enhancing telemedicine capabilities, predicting disease outbreaks, improving operational workflows, and optimizing resource distribution [10].

IoT is a persuasively growing communication technology that aims to dominate the conventional concepts of network communication. It is significantly expanding to assist every aspect of our lives through its applications, such as smart homes, smart agriculture, smart transportation, and smart health care [2], [3]. The applications of IoT in the industrial sector are also grabbing considerable attention in the present era and are intensively acknowledged as industrial IoT. While IoT has great potential to transform healthcare, several significant challenges still impede its widespread adoption. Data security, privacy, transparency, interoperability, reliability, and scalability concerns are among the most critical issues. Additionally, problems such as data manipulation, risk of single points of failure and data overload should be considered to confirm the safe use of IoT devices in healthcare [11]. Protecting

This work is supported in part by the Guangdong Basic and Applied Basic Research Foundation (2024A1515012407), and in part by the Shenzhen Science and Technology Program (JCYJ20220531101015033). (Corresponding author: Taotao Wang).

S. Aslam, T. Wang, D. Feng, and S. Zhang are with the College of Electronics and Information Engineering (CEIE), Shenzhen University, Shenzhen, Guangdong Province, e-mail: sidra@szu.edu.cn, ttwang@szu.edu.cn, fdquan@szu.edu.cn, zsl@szu.edu.cn

S. Aslam is with the Accounting and Finance Department, Strathclyde Business School, University of Strathclyde, United Kingdom e-mail: saba.aslam@strath.ac.uk

sensitive patient data requires the implementation of robust strategies to mitigate vulnerabilities within medical IoT devices. The diversity of IoT healthcare devices from different manufacturers often creates challenges with interoperability, both between the devices and with existing healthcare systems. This underscores the urgent need for effective solutions to ensure seamless interoperability. Additionally, scalability is a significant concern, especially as healthcare systems increasingly adopt IoT devices and encounter growing demands for infrastructure and data management [12], [13]. Many healthcare IoT systems depend on centralized platforms, which can present significant vulnerabilities and potentially result in single points of failure. Moreover, ensuring reliable, low-latency and stable connectivity for Internet of Medical-Things devices within smart hospitals is still a considerable challenge for research scholars [14], [15].

The application of blockchain technology to healthcare holds significant promise in solving various problems. However, several critical challenges remain for blockchain-based healthcare, particularly in enhancing security protocols to protect against attacks that target trust-building consensus mechanisms [16]. Research of healthcare blockchain should address scalability concerns, minimize computational requirements, establish robust regulatory frameworks to protect privacy, and foster confidence among shareholders involved in patient medical file sharing [17]. Future advancements should focus on enhancing blockchain interoperability in improving IoT healthcare techniques for larger ability, optimizing consensus algorithms and pharmacological supply chains, and assimilating blockchain technology with cloud setup to minimize storage overhead and streamline control [17]. Also, research should focus on enhancing usability through improved user interfaces, the implementation of incentive systems, the validation of personal health records, and biometric authentication regarding cost-effectiveness and security [18], [19].

Blockchain applications in the healthcare sector are diverse, including patient data management, supply chain management, clinical trials, medicine traceability, invoicing, and claims adjudication [20]. Supply chain management is a particularly interesting area for blockchain integration. Healthcare organizations face increasing pressure due to rising patient dissatisfaction, escalating healthcare costs, and decreasing reimbursements for services [21]. These demands have prompted healthcare providers to seek solutions capable of tackling such difficulties while accommodating technology improvements and growing expenses [22], [23]. Supply chain management is essential for minimizing costs and achieving organizational goals. It involves overseeing the movement of products, information, and finances among supply chain participants to effectively meet customer demand. However, healthcare supply chain management faces unique challenges, as any disruptions in this system can jeopardize patient safety and potentially lead to tampering or breaches of medical information [24], [25].

*1) Research gaps:* In the medical field, there are many benefits of IoT sensors to collect patient data, which has led to the creation of enormous quantities of health information that must be securely transmitted and stored. However, this poses a substantial issue as the data can be intercepted by unauthorized entities, theoretically leading to confidentiality breaches. Therefore, the absence of collective safety measures across many Internet of Medical Things (IoMT) platforms presents a severe difficulty in protecting the security and privacy of IoMT data.

To address these issues, this work proposes the development of a patient medical file and supply chain management model that integrates the Hyperledger Fabric blockchain with an IoT-based architecture [17], [26]. Therefore, the envisioned method increases privacy and security in terms of access control. Access control policies are well-defined to confirm that only the consumers who have the authorization can access the patient's medical file, whereas contracts are stored inside the blockchain [27]. These rules, describing distinct user roles, are recorded in X.509 digital certificates [28]. The suggested IoT-based blockchain approach tackles scalability and interoperability difficulties typical in smart health applications. A personalized consensus code will be created to address the special requirements of blockchain-based IoT hospital applications [29], [30]. This protocol enables consensus via data transaction validation, as opposed to concentrating exclusively on transaction syntax. Given the dense topologies characteristic of healthcare facilities, such as hospitals, creating data-centric consensus methods is vital for efficient IoT integration [31]. The ability estimation stage will focus on the computational resources and time required for tasks such as creating, reading, updating, and retrieving asset history, which are commonly associated with blockchain applications, to assess the viability of the proposed system [32]. By integrating blockchain technology with a comprehensive access control management system that governs resource sharing, the main goal is to mitigate risks to data security and integrity.

To improve security and avoid privacy violations, remote patient and other healthcare institutions often set up their wellness programs in safe settings, such as private networks with firewalls [33]. This makes it difficult to conduct collaborative medical research and provide services since many healthcare organizations have disjointed medical data silos [34]. Therefore, maintaining patient confidentiality, avoiding data breaches, and guaranteeing the safe delivery of healthcare via cloud-based platforms all depend on securing the privacy and security of IoT-based medical data [35]. To safeguard IoT medical data, strong security mechanisms like access restriction and encryption must be put in place. Also, privacy and security can be improved by examining intricate patterns in the data, assisting in the creation of robust encryption keys, enabling proactive threat mitigation and enhancing anomaly detection via deep learning techniques and real-time monitoring [28].

*2) Main contribution:* The novelty and contribution of this work is summarized as follows.

(a) We propose a novel deep learning-based encryption and decryption key generation model that combines a Bi-directional Long Short-Term Memory (BiLSTM) neural network model with Convolutional Neural Networks (CNN). This model ensures the safe transmission of medical data that is collected from IoT sensors.

(b) We further optimize the encryption and decryption process by selecting the most appropriate cryptographic key through the Gradient Descent Optimization Algorithm (GDOA). This optimization approach enhances the system's efficiency and robustness, ensuring that the key selection process contributes to the overall performance of the encryption framework.
(c) We enhance symmetric searchable encryption with a Bloom filter, keywords within medical data that are hashed and mapped to the filter, enabling secure and efficient searches on the encrypted data. This approach ensures that patient privacy is protected during data sharing while meeting the need for safe data access.
(d) We evaluate performance of the proposed solution and discuss the comparative analysis of the experiments. The proposed solution is a reliable way to protect patient medical files through a peer-to-peer distributed, secure, and shared ledger. Experimental results prove the efficiency of the proposed scheme over the existing schemes.

This paper is organized as follows. Section II reviews the existing solutions that use blockchain technology for managing patient medical files. Section III provides an overview of Hyperledger Fabric as a blockchain platform. Section IV discusses the system model and method of the proposed system. Section V shows the experimental results, performance evaluation, and comparative analysis of the proposed solution. Finally, Section VI concludes this paper and suggests future work.Table I presents the notations and symbols used in this paper.

TABLE I: LIST OF NOTATIONS

| Symbols | Description |
|---|---|
| $E$ | Encryption function |
| $D$ | Decryption function |
| AES | Advanced Encryption Standard |
| CDOA | Detailed Descent Optimization Algorithm |
| CNN | Convolutional Neural Network |
| BiLSTM | Bidirectional Long Short-Term Memory |
| $R^2$ | Coefficient of determination (accuracy metric) |
| MAE | Mean Absolute Error |
| RMSE | Root Mean Square Error |
| IoMT | Intranet of Medical Things |
| ZKP | Zero-Knowledge Proof |
| KK | Cryptographic key |
| $T_{enc}$ | Encryption time |
| $T_{dec}$ | Decryption time |
| $T_{resp}$ | Response time |
| CRL | Certificate Revocation List |
| $\Theta$ | Sigmoid functions |
| $b$ | Bias vectors |
| $W$ | Weight matrices |
| $y_t$ | Input vector |
| $q_{t-1}$ | Memory cell state |
| $\acute{R}$ | Self-attention layer |
| $p_t$ | Stored cell |

## II. Related Work

The security of patient medical files presents critical challenges in healthcare systems. These records contain comprehensive patient data vital for treatment and diagnosis, necessitating robust protection to ensure patient privacy [26], [36]. Real-time monitoring, improved patient experiences, and improved treatment results are just a few of the notable advancements brought about through the IoMT's quick development in the healthcare industry [37]. Patient data is usually sent to cloud servers and edge devices in an IoMT environment for processing and analysis. IoMT equipment, such as biosensors and smart wearables, is used by healthcare practitioners to remotely monitor patients and make data-driven choices in real-time. However, there are several difficulties in using these devices because of their sensitive nature and the amount of data they produce. The IoMT ecosystem's cybersecurity flaws and experts' growing knowledge of these threats have been the subject of in-depth research [38].

Cloud-based solutions are frequently used to manage the substantial data produced by IoMT devices, given their scalability, privacy, safety, remote accessibility, and cost-effectiveness [39]. Despite these advantages, cloud environments introduce several security concerns. Several recent data breaches have exposed the risks associated with cloud-hosted data, highlighting the potential for unauthorized access to sensitive information [40]. Data created by IoMT that includes private and sensitive information shouldn't be made public [41]. There are serious privacy and integrity issues when this data is stored in external cloud services. Because cloud operations are opaque, cloud service providers (CSPs) may employ backup copies to keep access to stored data. Although encryption provides some security, it may ultimately be broken by advances in computing power, giving hackers access to private data. CSPs may nevertheless have administrative access to the data without user authorization, even though access control systems are intended to prevent unwanted access [42]. As a result, cloud-based IoMT data is still susceptible to external attackers as well as malevolent CSPs, highlighting the need for stronger security protocols and more openness.

Several research initiatives have concentrated on improving security and privacy to solve the issues surrounding the sharing of personal health data. For example, Kabra et al. [43] suggested a new frontier blockchain to secure patient data, which effectively detects cyberattacks by combining cloud computing with a unique BiLSTM network. Rehman et al. [44] created a more effective and reversible blockchain-based hybrid technique for IoMT-based systems in response to concerns about data confidentiality. Additionally, Ramani et al. [45] used a federated learning method by combining key blinding, proxy re-encryption, and the Ciphertext-based Encryption algorithm to define a new fine-grained data-sharing system. In cloud-assisted IoMT systems, this technique provides flexible modifications to user access rights. Table II shows overview of existing solutions over different features like scalability, privacy, storage, CIA (Confidentiality, Integrity, Availability), and consensus. The table demonstrates that some existing solutions use Hyperledger Fabric blockchain, and Kafka consensus

TABLE II: Our proposed solution comparison with existing work

| Solutions | Blockchain | Scalability | Privacy | Storage | CIA | Consensus |
|---|---|---|---|---|---|---|
| [48] | Dual-channel | No | No | Decentralized | Partial | PBAS |
| [46] | Hyperledger Fabric | Yes | Yes | Decentralized | Full | Kafka |
| [47] | Hyperledger Fabric | Yes | Yes | Hybrid | Partial | PBFT |
| [49] | Hyperledger Besu | Yes | No | Decentralized | Full | IBFT |
| [50] | Ethereum | Yes | No | Decentralized | Partial | PBAS |
| [43] | Ethereum | No | No | Cloud | Partial | BFT |
| **Our solution** | Hyperledger Fabric | Yes | Yes | Decentralized | Full | Kafka |

mechanism[46], [47]. However, some solutions did not ensure scalability and privacy[43], [48], [49]. Also, some solutions are not fully decentralized and did not address CIA [43], [48], [50].

## III. Overview of Hyperledger Fabric

Hyperledger Fabric is a modular, enterprise-grade consortium blockchain platform that supports the development of scalable and secure distributed applications [36]. Unlike public, permissionless blockchains such as Ethereum or Bitcoin, Fabric provides fine-grained access control and customizable consensus mechanisms, making it ideal for scenarios where privacy and trust are critical—such as medical data management [29]. In Hyperledger Fabric based medical data systems, only registered and authorized individuals can access sensitive medical information, ensuring data confidentiality. By leveraging smart contracts, Fabric offers an immutable and secure transaction history accessible to all relevant parties, guaranteeing data provenance and eliminating the need for intermediaries. Hyperledger Fabric has the following features.

- Architecture and Transaction Flow: The platform follows an execute-order-validate model, dividing transaction processing into three distinct phases: execution, ordering, and validation. These steps are handled by separate components, allowing for greater flexibility and scalability. Fabric's network components operate within Docker containers, ensuring resource isolation and deployment consistency.
- Consensus and Privacy: Hyperledger Fabric supports pluggable consensus protocols, including Kafka with Zookeeper and Practical Byzantine Fault Tolerance (PBFT), which enhance efficiency and reduce energy consumption compared to traditional proof-of-work systems. Its permissioned architecture, combined with private data collections, ensures confidentiality and controlled data sharing between organizations.
- Network Organization and Governance: Participants in Fabric are grouped into organizations, each representing a real-world entity. Transactions are governed at the organizational level, enabling entities that may not fully trust each other to collaborate under shared governance models, supported by legal agreements or dispute resolution processes.
- Smart Contracts and Chaincode: Smart contracts, known as chaincode in Fabric, define the business logic and are implemented using general-purpose programming languages such as Java, Go, and Node.js. Chaincode packages one or more smart contracts and is deployed across the network. The ledger consists of a blockchain for transaction records and a world state database for current data, both of which smart contracts can interact with. Endorsement policies specify which organizations must approve transactions before they are committed to the ledger.
- Identity and Security: Identity management in Fabric relies on X.509 digital certificates, issued by trusted Certificate Authorities (CAs). These certificates use public-private key pairs and digital signatures to authenticate participants and secure communications, ensuring data integrity and trust across the network.

## IV. System Model and Method

This section presents the system model of the proposed Hyperledger fabric based IoMT system, and the proposed method of machine learning-based encryption and decryption.

### A. System Model

Fig. 1 illustrates the system model of the proposed Hyperledger fabric based IoMT system. Blockchain technology is utilized to store and protect hashes of patient' medical files and their associated access control policies. Access to users' data is governed by these predefined policies. The proposed Hyperledger fabric based IoMT system consists of the follownning four components: 1) IoT Health Manager, 2) Patients' bodies equipped with sensors, 3) Blockchain network, and 4) Cloud technology. We explain them in detail as follows.

*1) IoT Health Manager:* IoT-enabled devices have revolutionized patient monitoring in healthcare, offering opportunities to enhance patient security and well-being while enabling healthcare professionals to provide high-quality care. The adoption of these technologies has also led to improved patient engagement and satisfaction, facilitated by effective communication between healthcare providers and patients. Far-flung patient checking helps reduce the likelihood of readmissions and reduces hospital stays. IoT is reshaping healthcare delivery by transforming the interaction between medical devices

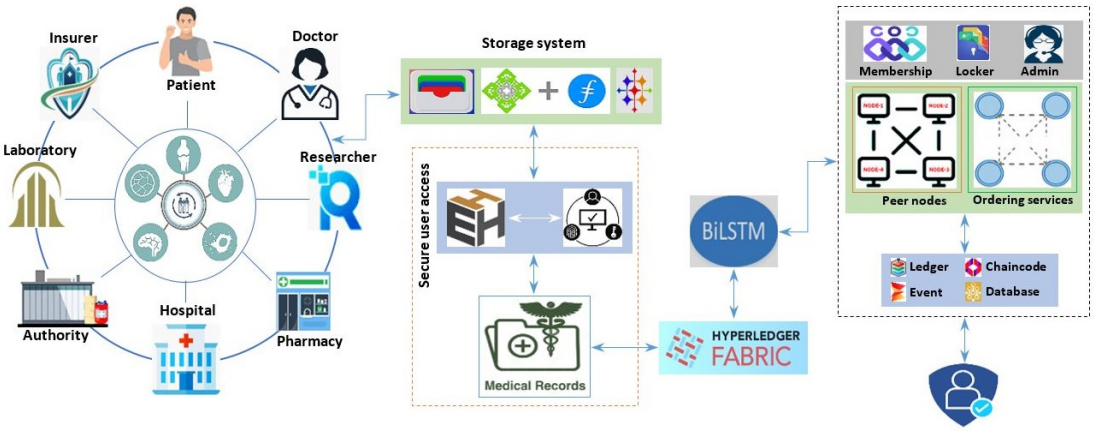


Fig. 1: The system model of the proposed Hyperledger fabric based IoMT system.

and healthcare professionals. Wearable medical tools, like wearable belts, fitness trackers and health monitors, provide patients with personalized care and real-time health updates. These tools could be programmed to remind customers to monitor vital signs like heart rate and to alert healthcare professionals and family members to any significant changes. IoT technology has particularly benefited elderly patients, enabling continuous monitoring of their health conditions and offering timely alerts for necessary interventions. Beyond monitoring patient health, IoT devices serve various critical functions in hospital settings. Sensors attached to medical equipment allow for real-time tracking of their location, and the positioning of healthcare staff can be monitored as well. Infection control is another vital application of IoT, as hygiene monitoring devices can help reduce the spread of illnesses. Additionally, IoT devices support asset management tasks, including managing pharmacy inventories and monitoring patients' body temperatures.

*2) Patient's Bodies Equipped with Sensors:* The healthcare industry presents opportunities for the application of wearable medical devices. These technologies can greatly enhance patient care by enabling the continuous monitoring of individual health metrics and preventing certain medical conditions. Wearable devices, such as those used to monitor vital signs, are integrated with health apps that help track various health parameters. The usage of wearable devices such as brain-computer interfaces, blood pressure monitors, healing chips, fitness trackers, cyber pills, and similar tools is increasing in the healthcare sector worldwide. When coupled with mobile technology, these devices can effectively monitor and potentially prevent various health issues, including chronic conditions like diabetes and respiratory diseases.

*3) Blockchain Network:* A distributed ledger is maintained by a multitude of linked systems that make up a blockchain network. This ledger is made up of several coupled blocks. Each successive block refers to the hash of its predecessor. Additionally, each block also carries a timestamp element and the preceding block's cryptographic hash and node. In the network, each node has a copy of a ledger and verifies the contacts in its logs. In the field of information security, blockchain has emerged as a key tool for guaranteeing tamper-proof data and strong data integrity. Blockchain functions as a decentralized network where information is stored across multiple nodes. This network offers an ideal solution for securing sensitive data, enabling the secure and private exchange of information. It serves as an efficient mechanism for the centralized, yet secure, storage of critical records. In addition, blockchain aids in expediting the identification of candidates who meet specific clinical trial criteria by utilizing individual patient records. Blockchain represents a distributed peer-to-peer framework containing nodes that store, track, and display transaction data. When leveraged properly, this technology facilitates the integration of different networks, highlighting the value of personalized care. The key advantages of blockchain lie in its immutability and robust security. Its foundational elements include blocks, nodes, and miners.

*4) Cloud Technology:* Integrating cloud computing technology into healthcare services can lead to simplified data sharing, significant cost savings, telehealth applications, personalized medicine and other benefits. Many healthcare providers utilize cloud-based systems for secure data storage, backup, and easy access to digital records. The detail of cloud technology in the healthcare sector is presented in Tang et al. [51]. We explain the process as follows: The major goal is to secure the transfer of patient medical files acquired by sensors implanted in the patient to the personal arithmetical assistant for analysis. The acquired files are secured by utilizing a coupled encryption technique (AES + Twofish) to confirm privacy during transformation. The encoded medical files are subsequently kept in the cloud location, which is secured by strict access restrictions and additional encryption measures to ensure safe retrieval. Blockchain is used to transport encrypted files, increasing the security of file exchanges and lowering the risk of file breaches. A coupled BiLSTM and CNN are used to create encryption and decryption keys, which confirms their rareness and resilience. A Gradient Descent Optimization Algorithm (GDOA) is applied to pick the best encryption key and increase the efficiency of the decryption and encryption operations.

Cloud-based healthcare solutions enhance various aspects of the healthcare sector, including improved monitoring of patient health data, vast storage capacity for hospital records, access to

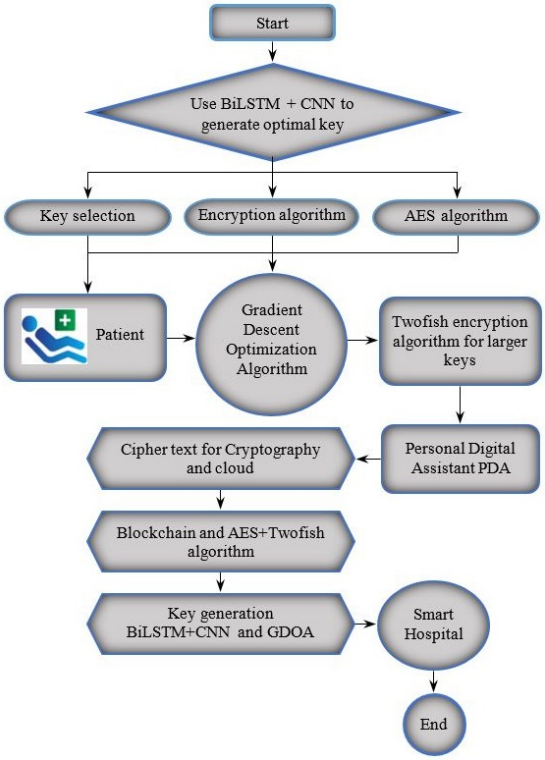


Fig. 2: The flowchart diagram of the proposed methodology.

computing resources, and more precise data analysis. Overall, these solutions ensure that medical data is securely transmitted and stored, prevent unauthorized access, and maintain the security and privacy of patient information.

### B. Methodology

The flowchart of the proposed deep learning-based encryption and decryption method as depicted in Fig. 2. The proposed method consists of three main parts, which are: 1) data encryption, 2) key generation, and 3) optimal key selection. We present the design details of them in the following.

*1) Data Encryption:* In this paper, we use AES + Twofish algorithm for data encryption. The medical record is first encrypted with AES using the initialization vector. Data encryption secures a message, ensuring that only the sender and recipient can understand it. In our work, we use encryption algorithm (AES + Twofish) to scramble the collected medical data, safeguarding it during transmission. Advanced Encryption Standard (AES + Twofish) is an extensively adopted and strong symmetric encryption algorithm that provides record safety for apps, networks, and other systems. This standard considers special ciphers with manifold substitution sequences, mixing, and shifting to encode data securely using 128-256 bit keys [52], [53]. The Twofish algorithm is a symmetric block cipher with a variable length of 128, 192, or 256 bits and a block of 128 bits. This encoding method is enhanced for 32-bit processing units and is perfect for software [54], [55]. Here, an AES algorithm coupled with the Twofish encryption method is used to encode the acquired medical file in the manner described below:

First, the unencrypted data is separated carefully into blocks of a predetermined size. Then, with the help of a randomly generated key, an AES encryption algorithm is used on each block to create the ciphertext. Finally, an encrypted block is obtained by further encoding the ciphertext block using the Twofish approach with an additional randomly generated key.

We denote the randomly generated keys for AES and Twofish by $\hat{A}_1$ and $\hat{A}_2$, respectively, denote the plaintext data by $p$, and denote the ciphertext data by $\hat{c}$. Here, $p$ is divided into fixed-size blocks: $p_1$, $p_2$, $p_n$. For each block, $p_i$ AES encryption is applied with $\hat{A}_1$: $\text{AES}(\hat{A}_1, p_i) = \hat{c}_i$. Each $\hat{c}_i$ is further encrypted using Twofish with $\hat{A}_2$: $\text{Twofish}(\hat{A}_2, \hat{c}_i)\hat{c}'_i$. The final encrypted data is $D = (D_1, D_2, D_n)$.

The encrypted data (including two randomly generated initialization vectors and the ciphertext) is inserted into a block structure. A simple hash of the block's contents is computed using SHA-256 to serve as the block's identifier. In a full blockchain system, additional steps, such as proof-of-work, distributed consensus, and linking to previous blocks, are applied using the AES algorithm.

*2) Key Generation:* After defining the ciphertext, a coupled machine learning method (BiLSTM and CNN) is used to create encryption and decryption keys. This hybrid method is prepared by using a kernel value as an input parameter. The model uses BiLSTM to create a series of important candidates. Then, the CNN evaluates the set of key candidates and picks the optimal key with the help of a fitness function. A coupled BiLSTM and CNN machine learning model is used to confirm the uniqueness and robustness of the optimal keys during the encryption and decryption process. The details of BiLSTM are given below.

**BiLSTM network**: The BiLSTM framework is a particular form of Recurrent Neural Network (RNN) that is developed to reduce threatened and exploding gradients that often arise during training [56]. The important feature of a BiLSTM network is its capacity to manage the flow of information through a memory control mechanism, which modifies the cell state via three distinct gates: input, output, and forget gates. These gates provide the network with the capability to selectively retain or discard information. The network contains the smooth layer, which turns the multi-size output of a self-attention layer into a smooth vector, as illustrated in Fig. 3. This selective memory mechanism significantly enhances the LSTM's capacity to filter out noise and recognize temporal patterns over varying time scales, as noted in recent work [57]. However, the traditional LSTM network is limited in its capability to process medical records in both directions at the same time. To address this limitation, a BiLSTM network integrates both forward and backward layers into a single architecture, enabling the system to consider both past and future contexts effectively.

Integrating the current input vector $y_t$, the previous hidden state $g_{t-1}$, and the memory cell state $q_{t-1}$, the following equations describe the mathematical formulation of an LSTM

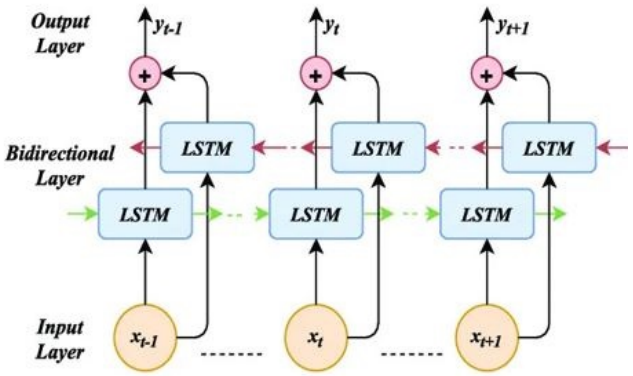


Fig. 3: The BiLSTM network model.

model:

$$i_t = \Theta(W_{xi}y_t + W_{hi}h_{t-1} + W_{ci}q_{t-1} + b_i) \quad (1)$$
$$f_t = \Theta(W_{xf}y_t + W_{hf}h_{t-1} + W_{cf}q_{t-1} + b_f) \quad (2)$$
$$q_t = f_t q_{t-1} + i_t \tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c) \quad (3)$$
$$p_t = \Theta(W_{xo}h_t + W_{ho}g_{t-1} + W_{co}q_{t-1} + b_o) \quad (4)$$
$$g_t = o_t tang(c_t) \quad (5)$$

where $i$, $q$, $f$, and $p$ represent the input gate, memory cell state, forget gate, and output gate at time $t$, respectively. $\Theta$, $b$, and $W$ are sigmoid functions, bias vectors, and weight matrices, respectively. BiLSTM model proves to be particularly effective in blockchain technology for the retention of information in both forward and backward directions, as shown in Fig. 3.

The forward hidden layer ($h_m^f$) and the backward hidden layer ($h_m^b$) are two distinct hidden layers in the BiLSTM mathematical model. Layer $h_a^f$ takes input vector $y_t$ in the forward direction as $m = 1, 2, 3, \ldots, M$, and layer $h_m^b$ in the backward direction as $m = M, M-1, M-2, \ldots, 1$. Finally, the output $o_t$ is created by merging the outcomes of $h_m^f$ and $h_m^b$ as:

$$h_m^f = \tanh(W_{xh}^f x_m + W_{hh}^f h_m^f - 1 + b_h^f) \quad (6)$$
$$h_m^b = \tanh(W_{mh}^b x_m + W_{hh}^b h_m^b - 1 + b_h^b) \quad (7)$$
$$o_m = \tanh(W_{hy}^f h_m^f + W_{hh}^b h_m^b + b_y) \quad (8)$$

To minimize the range of production vectors in regression or classification tasks, fully connected layers often follow BiLSTM layers, as shown in Fig. 3. The output of a BiLSTM algorithm, in this case, is a combination of $\tilde{I}$ and $\bar{I}$, represented as $I = [\tilde{I}; \bar{I}_T]$, signifying that the data for each time step has been consolidated into two vectors. This strategy complicates the effective use of critical time intervals, leading to a definite amount of data loss. This problem is resolved by the concept of self-attention [58], which posits that when the self-attention layer is implemented after the BiLSTM layer, the output layer is preserved as a matrix $\ddot{U}T \times L$, where $L$ signifies the dimension of the input vector and $T$ indicates the time steps. The procedure in a self-attention layer starts by multiplying the layer's input by three distinct weight matrices.

The matrices, representing the Key ($K$), Query ($Q$), and Value ($V$), are produced as the following:

$$\begin{cases} K = \acute{R}W_K \\ Q = \acute{R}W_Q \\ V = \acute{R}W_V \end{cases} \quad (9)$$

where the input of a self-attention layer is indicated by $\mathcal{R}$ parameters. The weight matrices, designated $W_K$, $W_Q$, and $W_V$ are applied to turn $\acute{R}$ into the Key ($K$), Query ($Q$), and Value ($V$) components, respectively. The dot-product attention approach is the most often used scoring function for this purpose, and its calculation is given by

$$s(Q, K) = \frac{QK^T}{\sqrt{D_k}} \quad (10)$$

where $s(Q, K)$ denotes the attention of dot-product and $D_k$ shows the dimension of $K$. Third, in the following, the softmax function normalizes the attention score before multiplying by value to get the result:

$$context = soft_{max}(s(Q, K))V \quad (11)$$

where $soft_{max}$ shows the softmax function and $context$ is an output of a self-attention layer.

**CNN**: A Convolutional Neural Network (CNN) is used here to automatically and adaptively learn the order of longitudinal features from patient medical records. CNNs' main innovation is the introduction of convolutional layers, which allow for more efficient image and spatial data processing. The yield of the convolutional layer is governed by feature maps, which are created by applying a set of spatial filters to the input. These feature maps capture the activations of the filters throughout the input data.

**Architecture of BiLSTM + CNN**: Both BiLSTM and CNN models utilize an observation window to process data in real-time [59]. In contrast, models such as Genetic Algorithm (GA), Ant Colony Algorithm (ACA), and Particle Swarm Algorithm (PSA), which do not natively support two-dimensional data inputs, require preprocessing of the input data. For these models, statistical metrics, including standard deviation and mean deviation, are generated for all features. In the case of GA, patient health was combined with other input features, resulting in a feature set of 317. On the other hand, the Particle Swarm Algorithm (PSA) can directly handle categorical features, eliminating the need for one-hot encoding and reducing the total number of input features to 308. The methodology proposed by Alkhammash [59] was applied here to capture the performance of the BiLSTM model considering the Convolutional layer, Max pooling layer and fully connected layer.

The dimensionality of the datasets is typically reduced through the pooling layer. Max pooling, one of the most common pooling techniques, outputs the maximum value found within a given 2×2 pooling filter. Other pooling techniques include averaging and summation. Max pooling is particularly effective as it significantly reduces the input size, often by as much as 75%, while preserving the most important features. On the other hand, in a CNN framework, the flattening layer

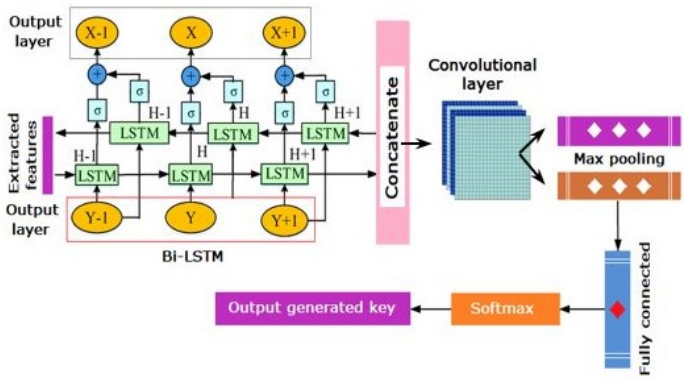


Fig. 4: The architectural diagram of BiLSTM+CNN.

converts the output of the CNN into a one-dimensional array via a neural network, as illustrated in Fig. 4. Two-dimensional arrays created with the help of the combined feature contours are flattened into a continuous, single and long vector. This flattened vector is then sent as an input dataset to the fully connected layer for further classification.

Neural networks may enhance historical data by using a chain-like neural network architecture. When the space between two time steps increases, typical neural networks diminish their capacity to separate long-term dependencies. To tackle this problem, BiLSTM was first established as a very effective architecture that generates excellent outcomes in numerical machine learning. The output of a module is directed through several gates in $R^{dimens}$ at each time interval. Here, $hidden_{t1}$, $m_t$ and $forget_t$, $in_t$, and $output_t$ are the preceding hidden layer, present input, forget gate, input gate and the output gate, respectively. In addition, the term dim $ens$ is utilized to show the capacity of the memory in the BiLSTM network. The BiLSTM transition processes are given by

$$Int = \sigma(C_{in} \cdot [hidden_{t-1}, m_t] + V_{in}) \quad (12)$$

$$forget_t = \sigma(C_{forget} \cdot [hidden_{t-1}, m_t] + V_{forget}) \quad (13)$$

$$s_t = \tanh hidden(C_s.[hidden_{t-1}, m_t] + V_s) \quad (14)$$

$$output_t = \sigma(C_{output} \cdot [hidden_{t-1}, m_t] + V_{output}) \quad (15)$$

$$P_t = forget_t \Theta p_{t-1} + in_t \Theta s_t \quad (16)$$

$$hidden_t = output_t \Theta(p_t) \quad (17)$$

where $\Theta$ represents the sigmoid feature. Tanh is the hyperbolic tangent function. To understand the architecture's system, consider $forget_t$ as the capacity to control the amount of dataset in the memory cell is discarded, and $p_t$ is the stored cell. Because BiLSTM is specially designed for learning dependency, therefore, it must be applied after the CNN layer.

By combining BiLSTM and CNN, the hybrid machine learning model leverages the strengths of both architectures. BiLSTM can sequentially process relevant features, capturing temporal context and relationships, and CNN can then extract these features. Fig.5 illustrates the workflow of key generation process using a hybrid BiLSTM and CNN approach. BiLSTM first generates multiple cryptographic key candidates by learning temporal dependencies from patient data features. These candidates are then evaluated by the CNN, which assigns a

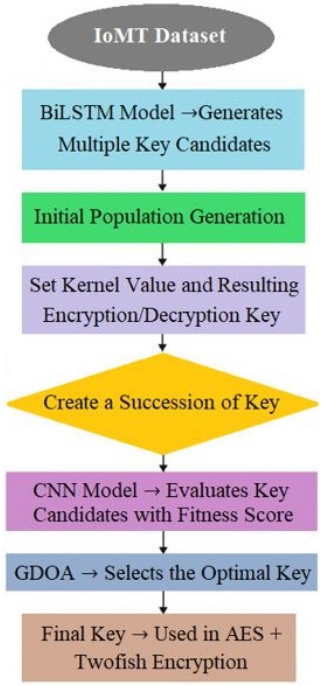


Fig. 5: The workflow of key generation process using a hybrid BiLSTM+CNN.

robustness score to each based on structural characteristics. Finally, the Gradient Descent Optimization Algorithm (GDOA) selects the optimal key from the pool, which is used for encryption and decryption. This layered process ensures high entropy and uniqueness in key generation, improving resistance to brute-force or pattern-based attacks. Since BiLSTM + CNN is specifically made for learning dependencies that last from time-series data, it should be used after the convolution layer for what is required in the progression of higher-level factors.

*3) Optimal Key Selection:* Finally, a Gradient Descent Optimization Algorithm (GDOA) is applied to pick the optimal key. The fitness function of the GDOA is evaluated using the candidate key and the efficiency of the encoding processes. The GDOA optimization algorithm frequently improves the primary population of candidate keys that the algorithm begins with. In the final population, the key that performs the best is chosen as the ideal key for optimization. Gradient Descent is an optimization algorithm used for minimizing the cost function in machine learning, deep learning, and other optimization problems. It is an iterative method for finding the minimum of a function by moving in the direction of the steepest descent, i.e., the negative of the gradient of the function.

The key objective of gradient descent is to find the optimal parameters (weights) that minimize a cost or loss function $J(\theta)$. In addition, gradient descent aims to minimize this function by adjusting the parameters $\theta$:

$$\theta := \theta - \alpha \nabla J(\theta) \quad (18)$$

where $\theta$ is the weight parameter to be optimized, and $\alpha$ is the learning rate or a hyperparameter that controls the step size.

$\nabla J(\theta)$ is the gradient (the vector of partial derivatives) of the cost function concerning $\theta$.

The gradient of the cost function $J(\theta)$ at any given point $\theta$ is calculated. The gradient tells you about the direction in which the function increases the fastest. After calculating the gradient, the parameters are updated by subtracting a fraction of the gradient. This fraction is controlled by the learning rate $\alpha$. This process is repeated iteratively until convergence, meaning the parameters stop changing significantly or reach a predefined stopping criterion (e.g., number of iterations, or the change in cost function is small).

The gradient $\nabla J(\theta)$ is the vector of partial derivatives of the cost function concerning each parameter:

$$\nabla J(\theta) = \left[\frac{\partial J(\theta)}{\partial \theta_1}, \frac{\partial J(\theta)}{\partial \theta_2}, \cdots, \frac{\partial J(\theta)}{\partial \theta_n}\right] \tag{19}$$

where $n$ is the number of parameters (dimensions). For example, in linear regression, the cost function $J(\theta)$ is typically the Mean Squared Error (MSE), which is given by:

$$J(\theta) = \frac{1}{m}\sum_{i=1}^{m}\left(h\theta(x^{(i)}) - y^{(i)}\right)^2 \tag{20}$$

where $m$ is the number of training examples.

To update the weights, we compute the gradient of the MSE concerning $\theta$:

$$\nabla J(\theta) = \frac{1}{m}\sum_{l=1}^{m}\left(h_\phi(x^{(l)}) - y^{(l)}\right)x^{(l)} \tag{21}$$

The update rule then becomes:

$$\theta := \theta - \alpha \cdot \nabla J(\theta) \tag{22}$$

where $\alpha$ is the learning rate.

The gradient of the cost function is computed using the entire dataset. Pseudocode 1 demonstrates the process of data encryption and key generation using a hybrid approach.

Pseudocode 1: Data Encryption and Key Generation Pseudocode

**Apply** AES + Twofish for Data Encryption.

Divided $p$ into fixed-size blocks as $p_1, p_2, \ldots, p_n$

Do encryption for $p_i$ AES for $\hat{A}_1 : (\hat{A}_1, P_i) = \hat{c}_1$

Further encrypt $\hat{c}_i$ by using Twofish with $\hat{A}_2$: Twofish$(\hat{A}_2, \hat{c}_i) = \hat{c}_i'$

Obtain results for encrypted data as $D = (D_1, D_2, \ldots, D_n)$

Save the record and update the AES + Twofish model

**end** for

**Apply** BiLSTM + CNN for Key Generation

Set the **Kernel** value and the resulting encryption/decryption key as $\breve{S}$ and $R$, respectively

**Use** BiLSTM to create a succession of key candidates: $[R_1, R_2, \ldots, R_n]$

**Find** optimal key $R$ using CNN based on a fitness function: $R = \text{CNN}([R_1, R_2, \ldots, R_n], \breve{S})$

**Apply** a BiLSTM classifier as a fitness function

end for

**Use** the GDOA Algorithm for the Best Key Selection

**Define** the encryption/decryption key as $R$ and the fitness value $\gamma(R)$

**Apply** GDOA with an initial candidate key: $\hat{H}[R_1, R_2, \ldots, R_n]$

**Assess** the performance of the encryption/decryption procedure: $\gamma(R) = \ell(\text{Encrypt}(\dot{P}, R), \text{Decrypt}(\dot{C}, R))$

**Improve** population using mutation, selection, and crossover operators with the help of the Gradient Descent Optimization Algorithm

**Pick** the best key for the final population as $R* = \arg\max(\gamma(\dot{P}))$

**end** for

The proposed GDOA provides an accurate estimate of the gradient. This technique converges to the minimum more smoothly for convex functions. However, GDOA is slow, especially with large datasets and requires holding the entire dataset in memory.

### C. System Layers of the Proposed Method

The proposed method is based on Hyperledger Fabric and features an architecture that can be divided into three distinct layers: the IoMT Layer, the Blockchain Layer, and the Storage Layer. The IoMT Layer is made up of smart devices that communicate with Hyperledger Fabric, using the blockchain's capabilities and services. The Blockchain Layer performs two functions: it works as a system for ownership and managing metadata for patient files saved in a decentralized data storage system, as well as regulating permission management. This enables secure data transfer among possibly untrustworthy parties. The storage layer delivers an off-chain scattered file scheme that securely stores encoded patient files, which are structured and identifiable using appropriate cryptographic hashes.

## V. Evaluation and Discussion

In this section, we present the experimental evaluation of our proposed method along with the associated discussion. We used Python 3.10 to implement our proposed method. We conducted all experiments on a system with the following specifications:

- Processor: Intel Core i7-12700H
- RAM: 16 GB DDR4
- Operating System: Windows 10 (64-bit)
- Dataset size: 2 GB (UCI Heart Disease Dataset used for testing IoMT performance)
- Blockchain platform: Hyperledger Fabric v2.3 running on Docker

We conducted experiments to evaluate performance using several metrics, including Encryption Time Evaluation, Decryption Time Evaluation, Record Time Evaluation, Restoration Efficiency Evaluation, Key Generation Time Evaluation, Turnaround Time Evaluation, and Running Time Evaluation. We compare these metrics with other optimization algorithms, such as the Genetic Algorithm (GA), Ant Colony Algorithm (ACA), and Particle Swarm Algorithm (PSA). Additional criteria for comparison included Delivery Ratio, Security,

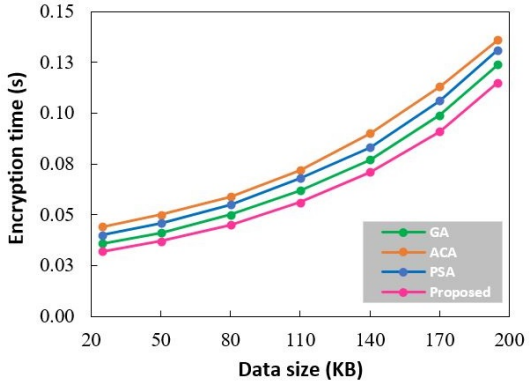


Fig. 6: The performance evaluation of encryption time.

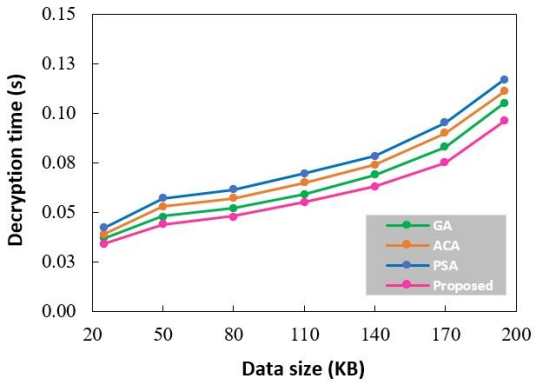


Fig. 7: The performance evaluation of decryption time.

Trust Score, and Throughput. We also present the training of machine learning models for the proposed solution and discuss the comparative analysis of the experiments. In the following sections, we will discuss these aspects in detail.

### A. Encryption Time Evaluation

Encryption is a procedure by which readable text is transformed into an unreadable form to prevent unauthorized parties from reading it. Encryption time is an important measure for encryption algorithms since it represents the time necessary to safeguard data. Encryption time is the total amount of time that is required for an encryption algorithm to turn plaintext into ciphertext. This feature indicates the algorithm's efficiency. Fig. 6 depicts the encryption times for GA, ACA, PSA, and the proposed method. The encryption time increased slowly as the data size or file size increased, as can be observed in Fig. 6. The suggested approach has the shortest encryption time, measured at 0.32 seconds for a file size of 25 kB, making it the quickest of the techniques studied. Shorter encryption times improve system efficiency by allowing quicker data processing, resulting in better overall system performance.

### B. Decryption Time Evaluation

Decryption is the process of converting an encrypted message to its original (readable) format. The original message is called the plaintext message. Decryption time is an important feature for encoding algorithms, as it estimates the duration required to decrypt encrypted data. Fig. 7 shows the decryption time of GA, ACA, PSA, and the proposed technique. As we can see from Fig. 7, the decryption time of the proposed method is the smallest as compared to other methods. A lower decryption time enhances system performance, ensuring that data can be quickly restored to its original form for further use or analysis.

### C. Record Time Evaluation

Record time refers to the time taken to log, capture, or document a specific event, transaction, or activity. In medical, data processing, and computing contexts, it indicates how long it takes to input or store information into a system. Record time is an important statistic that measures the time needed

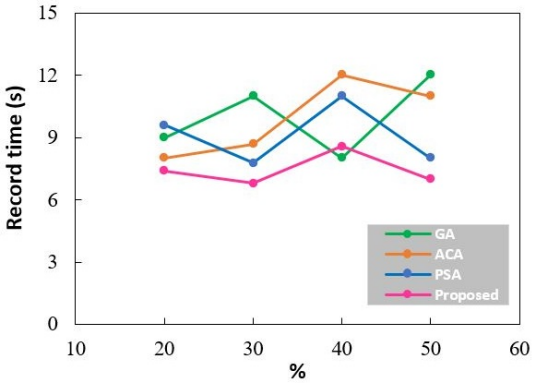


Fig. 8: The performance evaluation of record time.

to write and read medical records from the storage tool. This statistic is particularly essential for encoding techniques that need numerous write and read tasks, such as those used in big data management schemes, where rapid data processing is critical to good performance. The time required to store and retrieve medical records from the blockchain or cloud, including transaction finalization [60]. A faster record time is essential in healthcare to reduce clinician workload and increase efficiency. However, speed should not compromise the accuracy and completeness of the information being recorded. Fig. 8 presents the record times for GA, ACA, PSA, and the proposed method. We observe that the record time of the proposed solution take 7 seconds, emphasizing the algorithm's ability to perform tasks quickly as compared to other algorithms.

### D. Restoration Efficiency Evaluation

Restoration efficiency refers to the effectiveness of a process designed to restore data, systems, or services to their original or optimal state. This term measures how effectively the system recovers encrypted data without errors after storage or transmission disruptions [61]. It is calculated as the ratio of successfully recovered data to total encrypted data. This term can be applied in various contexts, but generally, it measures how effectively the restoration process recovers the intended data or service with minimal loss or delay [60]. In addition, the restoration efficiency shows the algorithm's capacity to maintain the integrity and security of encrypted data. Fig. 9

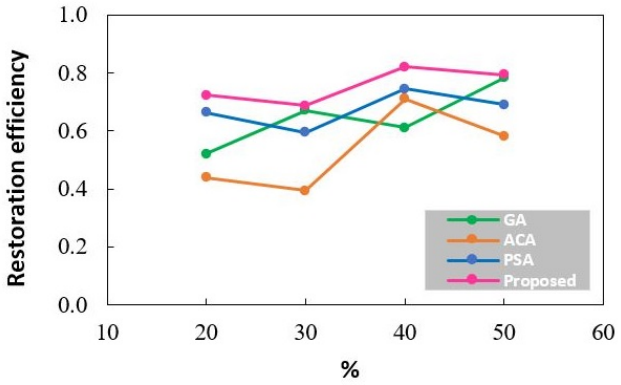


Fig. 9: The performance evaluation of restoration efficiency.

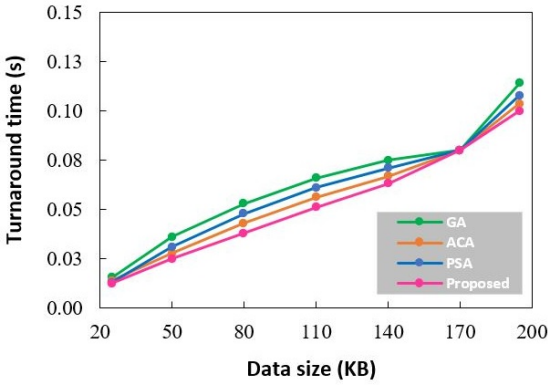


Fig. 11: The performance evaluation of turnaround time.

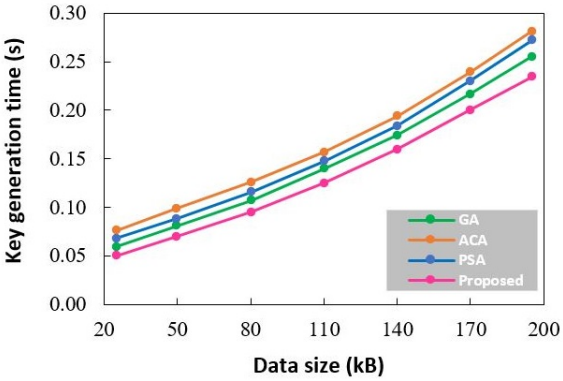


Fig. 10: The performance analysis of key generation time.

depicts the restoration efficiency of the GA, ACA, PSA and proposed solution. As we can see from Fig. 9, the proposed solution has a maximum restoration efficiency of 0.814648 seconds, demonstrating its exceptional capacity to restore the system after damage or security breaches.

### *E. Key Generation Time Evaluation*

Key generation time is the amount of time that is necessary to produce a cryptographic key for secure communication. Key generation time is an essential parameter in encryption algorithms since it counts the time required to produce cryptographic keys used in both encryption and decryption procedures. Fig. 10 depicts the key generation times for GA, ACA, PSA and the proposed method. Key generation time increased slowly as the data size or file size increased, as shown in Fig. 10. The key generation time might vary based on the algorithm's complexity, available computer resources, and the degree of security needed. As we can observe from Fig. 10, the proposed algorithm has the smallest duration of 0.05 seconds as data size increases. Our proposed solution generates cryptographic keys faster as compared to other algorithms. The smallest key generation time enhances the algorithm's overall efficiency, resulting in quicker data processing and system performance.

### *F. Turnaround Time Evaluation*

Turnaround time is the total time that is necessary to complete a particular task from begining to final, including all phases of data processing and data transformation. It represents the elapsed time from when a job or task is initiated until it is completed and ready for the next step or delivery [62]. Turnaround time is a remarkable metric for assessing the overall efficiency and responsiveness of an algorithm in completing its designated tasks. Fig. 11 demonstrates the turnaround time of GA, ACA, PSA, and the proposed methond. We observe that, the turnaround time of the proposed solution is less as compared to the other three algorithms. It shows that the proposed solution has better performance than existing methods.

### *G. Running Time Evaluation*

Running time is used to measure the total running period required by the algorithm to execute or register users. Fig. 12 presents the running time for query execution and user's registration. Fig. 12 shows the time required to extract information from the blockchain for datasets ranging from 500 to 5000 entries. We observe that, in the case of query execution time, the running time increased from 103 milliseconds to 632 milliseconds as the number of register devices increased from 500 to 5000 when the proposed method was used. The running time increased from 1055 milliseconds to 3258 milliseconds, in case of user registration time, as the number of registered devices increased from 500 to 5000 when the proposed method was used. The data show a significant rise in running time as the number of register devices increases. However, the response curve increases slowly, indicating consistent performance and allowing for the calculation of transaction running efficiency, particularly in the absence of system cramming. These findings illustrate the effect of device size on running time, however, stressing the stability of transaction reactions under changing circumstances. The Fig. 12 clearly shows that the number of data records has a substantial influence on latency, with larger datasets resulting in longer delays.

### *H. Machine Learning Model Training Evaluation*

We utilize neural networks as the machine learning model, leveraging the advantages of the graphics processing unit and the rapid development of computational power. To ensure high accuracy and avoid underfitting or overfitting models, we implemented three approaches by adding a dropout layer,

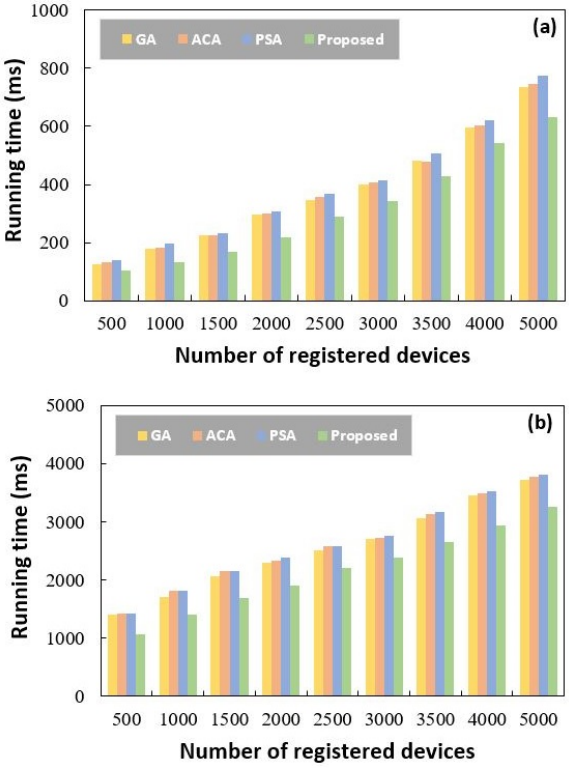


Fig. 12: The performance evaluation of running time: (a) query execution time, and (b) user's registration execution time.

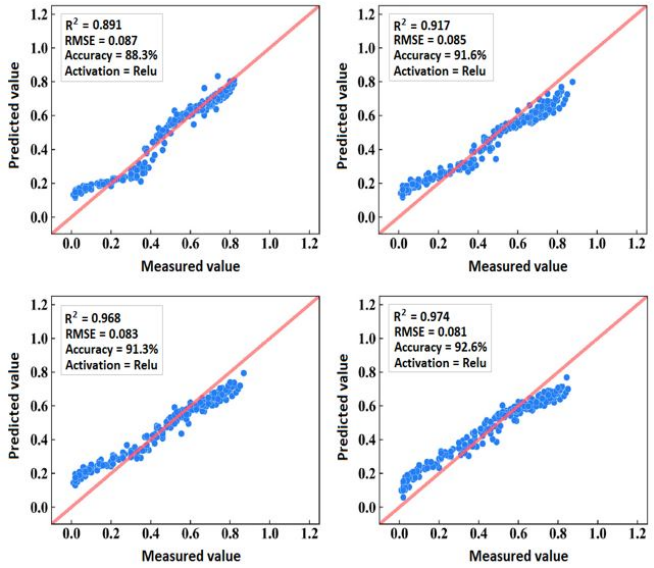


Fig. 13: The prediction accuracy of the proposed method based on deep neural networks with different hyper parameters.

cross-validation, and a batch normalization layer. Furthermore, a set of suitable hyper parameters is important for finding operative network models, which usually contain the optimization algorithm, the activation function, the number of hidden layers, the initialization of biases and weights, and the number of nodes in each hidden layer. To assess the accuracy of the proposed method, we typically use the determination coefficient ($R^2$), and root mean squared error (RMSE). The $R^2$ value indicates the goodness of fit for the method, serving as a statistical measure of how well the technique predicts real data sets. The RMSE is also employed to evaluate the model's performance; a RMSE of zero signifies excellent performance. If there is any discrepancy between the predicted and observed values, the RMSE will exceed zero. Smaller values of RMSE, along with a larger $R^2$, suggest high forecasting precision of the method.

Fig. 13 shows the prediction accuracy of the proposed method based on deep neural networks with different hyper parameters. The ReLU activation function was utilized here. We widely observed the impacts of various hyper parameters on the accuracy and convergence of deep learning models.

### *I. Comparative Analysis of Experiments*

In the process of using the Paillier cryptosystem for data encryption and decryption, the size of the public key plays a significant role in determining the complexity of the key and impacts the time required for both encryption and decryption operations. In this paper, we generate different lengths of keys, including 500 bits, 1000 bits, 1500 bits, 2000 bits, 2500 bits, 3000 bits, 3500 bits, 4000 bits, 4500 bits, and 5000 bits. We conduct a series of experiments using randomly generated data of consistent length, and the results were analyzed and organized accordingly. From the results shown in Fig.14(a), it is evident that the time required for encryption and decryption increases as the key size increase.

Typically, larger key sizes ensure better theoretical security, however, they suffer increased computational and communication overhead. In this paper, we choose a key size of 2500 bits, because it meets the security requirements of the system while maintaining relatively fast encryption and decryption speeds. The Fig. 14 further highlights that the encryption time in the proposed scheme is lower than the latest scheme [60], while the decryption time remains comparable. Overall, the proposed scheme demonstrates superior efficiency compared to the original algorithm, primarily due to the optimization of encryption and decryption processes through the use of the fast exponentiation algorithm, which reduces time consumption.

Furthermore, we analyze the efficiency of ciphertext retrieval in an encrypted state and conduct tests at different ciphertext data volumes. We compared results to other recent schemes, as presented in Fig. 14(b). As shown in Fig. 14(b), the time overhead for ciphertext retrieval in the scheme increases as the volume of ciphertext data increases, with a more significant increase observed for larger datasets [1]. In contrast, the proposed scheme maintains a nearly constant time overhead, which is also substantially smaller. This improvement is attributed to the use of a Bloom filter in the proposed scheme, which maps query keywords to integer IDs and significantly enhances search efficiency. The Bloom filter, employing multiple hash functions, can determine whether an element is present in the dataset in constant time, meaning that its query speed is independent of the dataset size, thus keeping the time overhead nearly constant.

From Fig. 15, it is evident that as the size of the encrypted files increases, both the encryption time of the scheme in

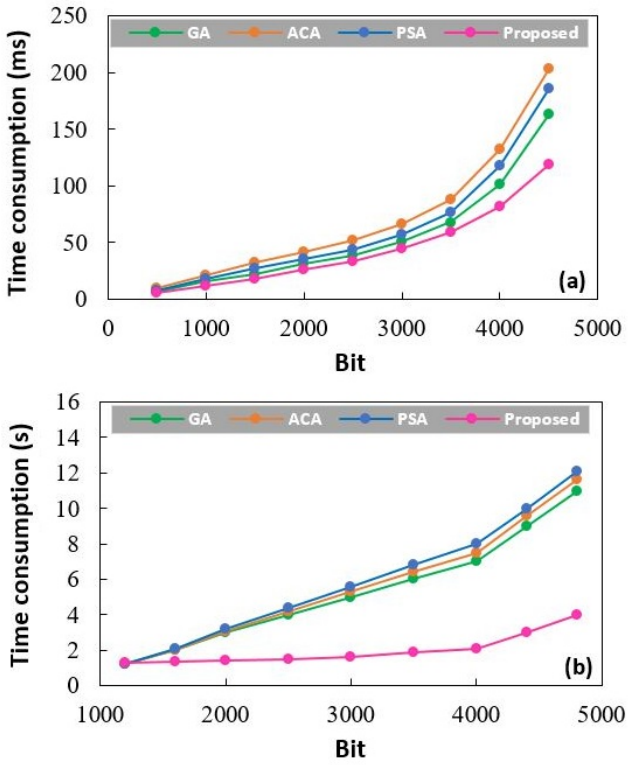


Fig. 14: (a) Time consumption of encryption and decryption for different key sizes. (b) Ciphertext retrieval time for different medical record sizes.

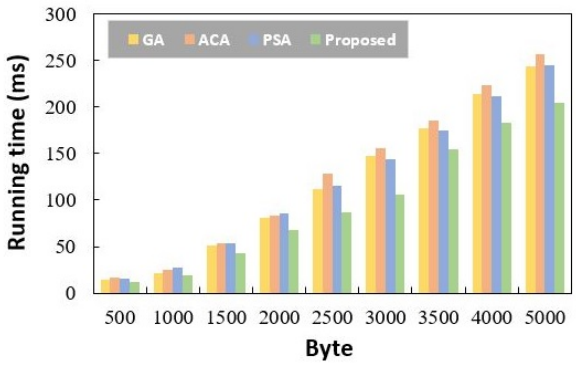


Fig. 15: Time consumption of encryption and decryption for different file sizes.

TABLE III: Comparative Analysis of Encryption Methods

| **Algorithm** | Speed | Key Size (bits) | Security Level | IoMT Suitability |
|---|---|---|---|---|
| **AES + Twofish** | High | 128–256 | Strong | Excellent |
| **RSA** | Low | 1024–4096 | Strong | Poor |
| **ECC** | Medium | 160–512 | Strong | Good |
| **Blowfish** | High | 128 | Moderate | Acceptable |

Sutradhar et al. [29] and the proposed scheme rise gradually, while the decryption time remains relatively constant. This is because encryption operations in homomorphic encryption exhibit higher computational complexity, involving numerous mathematical calculations. The complexity of these operations is influenced by the amount of input data, meaning that as the size of the encrypted files grows, the encryption time tends to increase linearly. On the other hand, the time required for decryption operations remains relatively small and stable. In homomorphic encryption schemes, the decryption time is typically less sensitive to the size of the encrypted data, which results in a consistent decryption time despite the increase in the size of the files being processed.

In this paper, the use of the fast exponentiation algorithm significantly reduces the time complexity of modular exponentiation operations. Traditional homomorphic encryption typically requires multiple computational steps for modular exponentiation, but the time complexity of fast exponentiation is reduced from O($n$) to O(log$n$), leading to a reduction in time consumption for both encryption and decryption when handling large-scale medical files. Experimental results demonstrate that, compared to the non-optimized scheme, the optimized encryption and decryption times are reduced by an average of 28%. This improvement boosts the efficiency of processing encrypted data while retaining the security benefits of homomorphic encryption, making the scheme more practical and effective in applications such as wearable medical devices and IoMT systems.

Overall, the proposed algorithm excels in encryption and decryption speed, key generation, system recovery, and task completion, outperforming the other algorithms across several performance metrics. However, it is crucial to note that these findings are based on specific patient medical records and may differ depending on the data collection, system configuration, and hardware and software configurations utilized throughout the encryption process.

We selected AES + Twofish as our encryption scheme due to its balance of high performance and strong cryptographic resistance. As seen in Table III, the Rivest Shamir Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC) offer strong security but suffer from slower performance, making them less ideal for latency-sensitive IoMT scenarios. Twofish complements AES by strengthening key expansion and substitution operations, ensuring efficient encryption even in resource-constrained environments. This combination proved most efficient in our experimental setup.

## VI. Conclusion

Medical file management has become an important focus of research recently. Since patient data is highly valuable, maintaining patient privacy can be challenging. Healthcare applications often store patient data in the cloud, which limits users' ability to have full control over their information. This paper proposed a new Hyperledger Fabric based IoMT architecture that leverages a coupled algorithm for protecting patients' records from external adversaries and illegal cloud service providers. For this purpose, IoMT sensors were installed in patients to collect medical data, which was then processed by a personal assistant. The collected medical data

are transmitted securely by a hybrid encryption algorithm. We used the cloud to store encrypted data for later retrieval, with the proper encryption and access controls in place. The use of blockchain to store encrypted data further improves data security and lowers the possibility of data breaches. The robustness and uniqueness of the encryption and decryption keys were guaranteed by using a hybrid deep learning model integrating Bidirectional Long Short-Term Memory (BiLSTM) and Convolutional Neural Networks (CNN). The Gradient Descent Optimization Algorithm (GDOA) was used to pick the best key, guaranteeing the speed and effectiveness of the encryption and decryption procedures. The proposed method could be guaranteed to be a more productive technique than the existing technique in terms of performance metrics because the model's performance was compared with that of the available technology. As part of our future work, we plan to integrate Zero-Knowledge Proofs (ZKPs) into the proposed architecture. ZKPs will allow verification of access rights or user identities without revealing any underlying patient data, thereby enhancing privacy and confidentiality. For instance, a hospital could confirm a doctor's authorization to view a record without exposing the record itself. This cryptographic primitive ensures stronger data minimization and compliance with privacy standards in decentralized IoMT networks.

## DATA AVAILABILITY

The UCI Heart Disease Data utilized in this paper which is publicly available and accessible via the UCI Machine Learning Repository(https://archive.ics.uci.edu/ml/datasets/Heart+Disease). This dataset provides useful insights into numerous cardiovascular parameters and has been crucial to our research on guaranteeing the privacy and security of IoT medical data.

## REFERENCES


[1] S. H. Alharbi, A. M. Alzahrani, T. A. Syed, and S. S. Alqahtany, "Integrity and privacy assurance framework for remote healthcare monitoring based on iot," *Computers*, vol. 13, no. 7, p. 164, 2024.

[2] T. Arpitha, D. Chouhan, and J. Shreyas, "A hybrid optimization approach to enhance source location privacy for iot healthcare," *IEEE Access*, 2024.

[3] S. Ma and X. Zhang, "Integrating blockchain and zk-rollup for efficient healthcare data privacy protection system via ipfs," *Scientific Reports*, vol. 14, no. 1, p. 11746, 2024.

[4] K. Pal, "Security implications of iot applications with cryptography and blockchain technology in healthcare digital twin design," in *Digital twins and healthcare: Trends, techniques, and challenges*. IGI Global, 2023, pp. 229–252.

[5] D. Kumari, S. Sharma, M. Chawla, and S. Panda, "A manifesto for healthcare based blockchain: Research directions for the future generation," *Journal of The Institution of Engineers (India): Series B*, vol. 105, no. 5, pp. 1429–1450, 2024.

[6] X. Liu, R. Shah, A. Shandilya, M. Shah, and A. Pandya, "A systematic study on integrating blockchain in healthcare for electronic health record management and tracking medical supplies," *Journal of Cleaner Production*, vol. 447, p. 141371, 2024.

[7] I. Zrelli and A. Rejeb, "A bibliometric analysis of iot applications in logistics and supply chain management," *Heliyon*, vol. 10, no. 16, 2024.

[8] S. K. Nanda, S. K. Panda, and M. Dash, "Medical supply chain integrated with blockchain and iot to track the logistics of medical products," *Multimedia Tools and Applications*, vol. 82, no. 21, pp. 32 917–32 939, 2023.

[9] D. Kumar, R. K. Singh, R. Mishra, and T. U. Daim, "Roadmap for integrating blockchain with internet of things (iot) for sustainable and secured operations in logistics and supply chains: Decision making framework with case illustration," *Technological Forecasting and Social Change*, vol. 196, p. 122837, 2023.

[10] K. Sallam, M. Mohamed, and A. W. Mohamed, "Internet of things (iot) in supply chain management: challenges, opportunities, and best practices," *Sustainable machine intelligence journal*, vol. 2, pp. 3–1, 2023.

[11] V. Hemamalini, A. K. Mishra, A. K. Tyagi, and V. Kakulapati, "Artificial intelligence–blockchain-enabled–internet of things-based cloud applications for next-generation society," *Automated secure computing for next-generation systems*, pp. 65–82, 2024.

[12] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on internet of medical things," *Personal and ubiquitous computing*, vol. 28, no. 1, pp. 59–72, 2024.

[13] B. Sarker, N. B. Sharif, M. A. Rahman, and A. Parvez, "Ai, iomt and blockchain in healthcare," *Journal of Trends in Computer Science and Smart Technology*, vol. 5, no. 1, pp. 30–50, 2023.

[14] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, 2023.

[15] S. R. Mallick and S. Sharma, "Emri: A scalable and secure blockchain-based iomt framework for healthcare data transaction," in *2021 19th OITS International Conference on Information Technology (OCIT)*. IEEE, 2021, pp. 261–266.

[16] S. R. Mallick, S. Sobhanayak, and R. K. Lenka, "Blockchain-enhanced iot ecosystem for healthcare: Transformative potentials, applications, challenges, solutions, and future perspectives," *Computers & Industrial Engineering*, vol. 197, p. 110538, 2024.

[17] A. K. Tyagi, "Blockchain-enabled internet of things (iots) platforms for iot-based healthcare and biomedical sectors," *Artificial Intelligence-Enabled Blockchain Technology and Digital Twin for Smart Hospitals*, pp. 201–217, 2024.

[18] W. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-iot healthcare applications and trends: A review," *IEEE Access*, vol. 12, pp. 4178–4212, 2024.

[19] P. Whig, R. Gera, A. B. Bhatia, R. R. Nadikattu, and Y. J. Alkali, "Convergence of blockchain and iot in healthcare: Opportunities and challenges," *Convergence of Blockchain and Internet of Things in Healthcare*, pp. 277–296, 2024.

[20] R. Lacson, Y. Yu, T.-T. Kuo, and L. Ohno-Machado, "Biomedical blockchain with practical implementations and quantitative evaluations: a systematic review," *Journal of the American Medical Informatics Association*, vol. 31, no. 6, pp. 1423–1435, 2024.

[21] Y. Ghoul and O. Naifar, "A healthcare application based on iot devices," *Wireless Networks*, vol. 30, no. 4, pp. 2541–2556, 2024.

[22] K. Li, A. R. Sai, and V. Urovi, "Do you need a blockchain in healthcare data sharing? a tertiary review," *Exploration of Digital Health Technologies*, vol. 2, no. 3, pp. 101–123, 2024.

[23] A. Haque, N. H. A. Manaf, M. N. Uddin, N. Akther, and A. Mokhtar, "Enhancing community health sustainability through the use of maqasid al-shariah theory," *International Journal of Islamic Marketing and Branding*, vol. 6, no. 2, pp. 159–179, 2024.

[24] S. Meti, S. Razauddin, R. Nallakumar, P. B. Mansingh, A. Z. Sameen, S. Pandey, S. K. Bhatt, and B. Jayabalan, "An empirical iot and cloud-based customizable healthcare surveillance system," *International journal of information technology*, vol. 16, no. 8, pp. 5317–5323, 2024.

[25] X. Shao, A. Pham, and T.-T. Kuo, "Webquorumchain: a web framework for quorum-based health care model learning," *Informatics in medicine unlocked*, vol. 50, p. 101590, 2024.

[26] M. Saad, S. A. Haidery, A. Bhandari, M. R. Bhutta, D.-J. Park, and T.-S. Chung, "An efficient privacy and anonymity setup on hyperledger fabric for blockchain-enabled internet of things (iot) devices," *Electronics*, vol. 13, no. 13, p. 2652, 2024.

[27] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based distributed application for multimedia system using hyperledger fabric," *Multimedia tools and applications*, vol. 83, no. 1, pp. 2473–2499, 2024.

[28] J. E. Abang, H. Takruri, R. Al-Zaidi, and M. Al-Khalidi, "Latency performance modelling in hyperledger fabric blockchain: Challenges and directions with an iot perspective," *Internet of Things*, p. 101217, 2024.

[29] S. Sutradhar, S. Karforma, R. Bose, S. Roy, S. Djebali, and D. Bhattacharyya, "Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security

and scalability for healthcare industry," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 49–67, 2024.
[30] S. Velmurugan, M. Prakash, S. Neelakandan, and E. O. Martinson, "An efficient secure sharing of electronic health records using iot-based hyperledger blockchain," *International Journal of Intelligent Systems*, vol. 2024, 2024.
[31] S. Arsheen and K. Ahmad, "Immunechain: A blockchain-based secure and transparent vaccine supply chain," *SN Computer Science*, vol. 6, no. 1, pp. 1–13, 2025.
[32] A. Sahoo and S. Sobhanayak, "Ebh-iot: Energy-efficient secured data collection and distribution of electronics health record for cloud assisted blockchain enabled iot based healthcare system," *Journal of Industrial Information Integration*, vol. 42, p. 100702, 2024.
[33] S. Garg, R. K. Kaushal, and N. Kumar, "A systematic approach to implement hyperledger fabric for remote patient monitoring," in *Applied Data Science and Smart Systems*. CRC Press, 2025, pp. 147–151.
[34] M. Rahaman, C. Y. Lin, I. Rachmat, R. Bansal, *et al.*, "Secure health features: Implementing hyperledger fabric in blockchain-driven healthcare management systems," in *Digital Forensics and Cyber Crime Investigation*. CRC Press, 2025, pp. 129–152.
[35] E. M. Alotaibi, H. Issa, and M. Codesso, "Blockchain-based conceptual model for enhanced transparency in government records: A design science research approach," *International Journal of Information Management Data Insights*, vol. 5, no. 1, p. 100304, 2025.
[36] S. K. Jena, B. Kumar, B. Mohanty, A. Singhal, and R. C. Barik, "An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry," *Decision Analytics Journal*, vol. 10, p. 100411, 2024.
[37] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," *Sensors*, vol. 21, no. 2, p. 359, 2021.
[38] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, p. 120235, 2021.
[39] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into internet of medical things (iomt): Data fusion, security issues and potential solutions," *Information Fusion*, vol. 102, p. 102060, 2024.
[40] T. Abbas, A. H. Khan, K. Kanwal, A. Daud, M. Irfan, A. Bukhari, and R. Alharbey, "Iomt-based healthcare systems: A review." *Computer Systems Science & Engineering*, vol. 48, no. 4, 2024.
[41] Z. Xu, E. Zheng, H. Han, X. Dong, X. Dang, and Z. Wang, "A secure healthcare data sharing scheme based on two-dimensional chaotic mapping and blockchain," *Scientific Reports*, vol. 14, no. 1, p. 23470, 2024.
[42] Y. Segal and A. Hod, "Dynamic access decision scoring: An adaptive framework for healthcare data security and privacy," 2024.
[43] S. Kabra, S. Sharma, and M. Sachdeva, "Blockchain: A new frontier in secure patient data management," *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, pp. 319–334, 2025.
[44] A. U. Rehman, N. Tariq, M. A. Jan, F. Khan, H. Song, and M. Ibrahim, "A blockchain-based hybrid model for iomt-enabled intelligent healthcare system," *IEEE Transactions on Network Science and Engineering*, 2024.
[45] R. Ramani, A. R. Mary, S. E. Raja, and D. A. Shunmugam, "Optimized data management and secured federated learning in the internet of medical things (iomt) with blockchain technology," *Biomedical Signal Processing and Control*, vol. 93, p. 106213, 2024.
[46] N. Rathore, A. Kumari, M. Patel, A. Chudasama, D. Bhalani, S. Tanwar, and A. Alabdulatif, "Synergy of ai and blockchain to secure electronic healthcare records," *Security and Privacy*, vol. 8, no. 1, p. e463, 2025.
[47] B. Jiang, C. Li, Y. Tang, and X. Xin, "Secure cross-chain transactions for medical data sharing in blockchain-based internet of medical things," *International Journal of Network Management*, vol. 35, no. 1, p. e2279, 2025.
[48] J. Kaur, R. Rani, and N. Kalra, "Healthcare data security and privacy protection framework based on dual channel blockchain," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 1, p. e70049, 2025.
[49] A. Samanipour, O. Bushehrian, and G. Robles, "Mdapw3: Mda-based development of blockchain-enabled decentralized applications," *Science of Computer Programming*, vol. 239, p. 103185, 2025.
[50] A. A. Khan, A. A. Laghari, A. M. Baqasah, R. Bacarra, R. Alroobaea, M. Alsafyani, and J. A. J. Alsayaydeh, "Bdlt-iomt—a novel architecture: Svm machine learning for robust and secure data processing in internet of medical things with blockchain cybersecurity," *The Journal of Supercomputing*, vol. 81, no. 1, pp. 1–22, 2025.
[51] Y. Tang, K. Wang, D. Niyato, J. Li, O. A. Dobre, and T. Q. Duong, "Secure data sharing and prediction with digital twin and blockchain in healthcare," *IEEE Communications Magazine*, 2025.
[52] E. I. Zafir, A. Akter, M. Islam, S. A. Hasib, T. Islam, S. K. Sarker, and S. Muyeen, "Enhancing security of internet of robotic things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques," *Internet of Things*, p. 101357, 2024.
[53] H. V. Krishna and K. R. Sekhar, "Enhancing security in iiot applications through efficient quantum key exchange and advanced encryption standard," *Soft Computing*, vol. 28, no. 3, pp. 2671–2681, 2024.
[54] S. K. Maddila and N. Vadlamani, "A novel efficient hybrid encryption algorithm based on twofish and key generation using optimization for ensuring data security in cloud," *Journal of Information & Knowledge Management*, vol. 23, no. 01, p. 2350062, 2024.
[55] K. Ramachandraiah, N. Bommagani, and P. Jayapal, "Enhancing healthcare data security in iot environments using blockchain and dcgru with twofish encryption," *Inf. Dyn. Appl*, vol. 2, no. 4, p. 173185, 2023.
[56] X. Zheng, C. Yang, L. Zeng, Y. He, Y. Tian, Y. Zhang, and J. Li, "Intensity recognition of vortex ropes in draft tube of a prototype pump turbine using an optimized cnn-bilstm framework with multi-head self-attention mechanism," *Journal of Energy Storage*, vol. 106, p. 114910, 2025.
[57] U. Saleem, W. Liu, S. Riaz, M. M. Aslam, W. Li, and K. Wang, "Enernet: Attention-based dilated cnn-bilstm for state of health prediction of cs2 prismatic cells in energy systems," *Electrochimica Acta*, vol. 512, p. 145454, 2025.
[58] V. Pandey, U. K. Lilhore, R. Walia, R. Alroobaea, M. Alsafyani, A. M. Baqasah, and S. Algarni, "Enhancing heart disease classification with m2masc and cnn-bilstm integration for improved accuracy," *Scientific Reports*, vol. 14, no. 1, p. 24221, 2024.
[59] M. Alkhammash, "A metaheuristic approach to detecting and mitigating ddos attacks in blockchain-integrated deep learning models for iot applications," *IEEE Access*, 2024.
[60] A. K. Ranjan and P. Kumar, "Ensuring the privacy and security of iot-medical data: A hybrid deep learning-based encryption and blockchain-enabled transmission," *Multimedia Tools and Applications*, vol. 83, no. 33, pp. 79 067–79 092, 2024.
[61] H. Assiri, "Piranha foraging optimization algorithm with deep learning enabled fault detection in blockchain-assisted sustainable iot environment," *Sustainability*, vol. 17, no. 4, p. 1362, 2025.
[62] A. Goel and S. Neduncheliyan, "Security enhancement of decentralized healthcare system by transformer blockchain mechanism," *Engineering and Applied Science Research*, vol. 51, no. 6, pp. 772–783, 2024.