XAI Driven Intelligent IoMT Secure Data Management Framework

Wei Liu, *Member, IEEE*, Feng Zhao, *Member, IEEE*, Lewis Nkenyereye, Shalli Rani, *Senior Member, IEEE*, Keqin Li, *Fellow, IEEE*, and Jianhui Lv, *Member, IEEE*

***Abstract*—The Internet of Medical Things (IoMT) has transformed traditional healthcare systems by enabling real-time monitoring, remote diagnostics, and data-driven treatment. However, security and privacy remain significant concerns for IoMT adoption due to the sensitive nature of medical data. Therefore, we propose an integrated framework leveraging blockchain and explainable artificial intelligence (XAI) to enable secure, intelligent, and transparent management of IoMT data. First, the traceability and tamper-proof of blockchain are used to realize the secure transaction of IoMT data, transforming the secure transaction of IoMT data into a two-stage Stackelberg game. The dual-chain architecture is used to ensure the security and privacy protection of the transaction. The main-chain manages regular IoMT data transactions, while the side-chain deals with data trading activities aimed at resale. Simultaneously, the perceptual hash technology is used to realize data rights confirmation, which maximally protects the rights and interests of each participant in the transaction. Subsequently, medical time-series data is modeled using bidirectional simple recurrent units to detect anomalies and cyberthreats accurately while overcoming vanishing gradients. Lastly, an adversarial sample generation method based on local interpretable model-agnostic explanations is provided to evaluate, secure, and improve the anomaly detection model, as well as to make it more explainable and resilient to possible adversarial attacks. Simulation results are provided to illustrate the high performance of the integrated secure data management framework leveraging blockchain and XAI, compared with the benchmarks.**

***Index Terms*—Explainable artificial intelligence, Internet of Medical Things (IoMT), secure data management, blockchain, bidirectional simple recurrent unit, local interpretable model-agnostic explanations.**

I. Introduction

IN THE age of digital transformation, the healthcare sector has not remained untouched by the sweeping wave of technological advancements. The emergence of the Internet of Medical Things (IoMT) is a testament to the profound changes that have been ushered into healthcare [1], [2], [3]. IoMT, a confluence of medical devices and applications that connect to healthcare IT systems through online networks, has redefined the contours of patient care and medical data management. IoMT has bridged the gap between traditional healthcare practices and the demands of a rapidly evolving digital world by facilitating real-time monitoring, enabling remote diagnostics, and promoting data-driven treatment [4]. However, as with any technological evolution, the IoMT brings challenges that must be addressed to harness its full potential. At the forefront of these challenges is the issue of security and privacy. Medical data, inherently sensitive and personal, demands the highest levels of protection [5], [6].

The integration of blockchain with the IoMT is emerging as a beacon of hope in the face of mounting challenges [7], [8], [9], [10]. This fusion promises to address the vulnerabilities and inefficiencies inherent in traditional data management systems, particularly in the medical domain. Blockchain, at its core, is a decentralized ledger system. Unlike centralized databases vulnerable to single points of failure, blockchain operates on a network of nodes [11], [12], [13]. Each node has a copy of the entire blockchain, ensuring that even if one or more nodes are compromised, the entire system's integrity remains intact. This decentralized nature of blockchain offers robustness and resilience that traditional systems cannot match. The IoMT encompasses many devices, from wearable health monitors to smart inhalers. These devices continuously generate sensitive data, ranging from a patient's heart rate to medication intake [14].

The adoption of blockchain alone cannot ensure its integrity and confidentiality. We can further optimize the security protocols by conceptualizing these transactions as a two-stage Stackelberg game. In game theory, the Stackelberg game is a model of strategic interaction where one player, the leader, moves first, and the other, the follower, moves after observing the leader's action [15]. Translating this to the realm of IoMT and blockchain, the leader could be the primary data transmitter (like

Received 10 March 2024; revised 6 April 2024; accepted 16 April 2024. Date of publication 3 June 2024; date of current version 4 February 2026. This work was supported in part by the Guiding Science and Technology Plan Project of Jinzhou Science and Technology Bureau in 2023 under Grant JZ2023B005. *(Corresponding author: Feng Zhao.)*

Wei Liu and Feng Zhao are with the Department of Emergency Medicine, Shengjing Hospital of China Medical University, Shenyang 110004, China (e-mail: lw2487551906@163.com; zhaojz120@163.com).

Lewis Nkenyereye is with the Department of Computer and Information Security, Sejong University, Seoul 3000, South Korea (e-mail: nkenyele@sejong.ac.kr).

Shalli Rani is with the Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab 140401, India (e-mail: shalli.rani@chitkara.edu.in).

Keqin Li is with the Department of Computer Science, State University of New York, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

Jianhui Lv is with the Department of Network, Peng Cheng Laboratory, Shenzhen 518057, China (e-mail: lvjh@pcl.ac.cn).

Digital Object Identifier 10.1109/JBHI.2024.3408215

an IoMT device), and the followers could be secondary entities like data receivers or validators. By structuring interactions in this manner, one can ensure that the primary data transactions are always a step ahead, further bolstering security. Perceptual hashing creates a unique digital fingerprint for data, allowing for easy identification and verification [16], [17], [18]. By using this technology in conjunction with blockchain, it becomes straightforward to confirm the rights and interests of every participant in an IoMT data transaction.

However, security is but one facet of the challenge. The vast amounts of data IoMT devices generate necessitate intelligent systems that can process, analyze, and make sense of this data. This is where the role of explainable artificial intelligence (XAI) becomes paramount. XAI, as the name suggests, is not just about creating intelligent systems but also about making these systems transparent and understandable [19]. In the context of IoMT, this means developing models that can accurately detect anomalies and cyberthreats and explain their decision-making processes in a comprehensible manner to humans. Using bidirectional simple recurrent units (Bi-SRU) for modeling medical time-series data addresses the challenge of accurate anomaly detection [20]. Bi-SRU performs exceptionally well in anomaly detection within IoMT-generated medical time-series data, especially compared to standard recurrent neural network (RNN) or long short-term memory (LSTM) networks. Its bidirectional architecture captures temporal dependencies more effectively and is designed to mitigate the vanishing gradient problem, thus enhancing performance. Traditional models often grapple with the issue of vanishing gradients, which can impede their performance. This limitation can be effectively overcome by leveraging Bi-SRU, paving the way for more accurate and efficient anomaly detection.

Nevertheless, the quest for a robust and secure IoMT data management system continues. The ever-evolving landscape of cyber threats demands that these models not only detect anomalies but also remain resilient in the face of adversarial attacks. The necessitates the development of methods that can assess, improve, and secure the anomaly detection model. This is achieved by using an adversarial sample generation method based on local interpretable model-agnostic explanations (LIME) [21]. By enhancing the explainability of the model and ensuring its robustness, this method ensures that the IoMT data management system remains transparent and secure.

To address the incongruity between reducing dimensions and preserving features in imbalanced industrial Big Data, the authors introduced a novel learning model called variational long short-term memory (VLSTM) for intelligent anomaly detection, which relies on reconstructed feature representations [22]. In [23], the authors introduced the weighted isolation forest and siamese gated recurrent unit (WIF-SGRU) algorithm to detect anomalies in scenarios with limited sample data. In [24], the authors presented an improved autoencoder for unsupervised anomaly detection (IAEAD). In [25], the authors proposed a data anomaly detection method named BS-iForest (box plot-sampled iForest) for wireless sensor networks based on a variant of isolation forest. In [26], the authors proposed a novel end-to-end model that integrates the one-class support vector machine (SVM) into a convolutional neural network (CNN), named the deep one-class (DOC) model. In [27], the authors introduced and put into operation the SAnDet (software-defined networking anomaly detector) framework, a system for detecting anomalies based on intrusion, tailored to leverage the functionalities provided by software-defined networking architecture, serving as a controller application. In [28], the authors put forward a proficient method for anomaly detection known as AnoGLA, which considered the intricate communication patterns among network structure and node attributes.

In conclusion, integrating blockchain and XAI offers a holistic solution to the challenges posed by the IoMT. The proposed framework differs by incorporating a two-stage Stackelberg game into the blockchain model for IoMT data transactions, a novel approach. Additionally, integrating perceptual hash technology for data rights confirmation is a unique feature that maximizes participant protection. The framework is designed to fortify data management within the IoMT ecosystem by harnessing the inherent security features of blockchain technology. By integrating these features, we aim to provide a robust solution for securely managing sensitive medical data transactions. To further bolster the analytical capabilities of the framework, we employ Bi-SRU, which is adept at processing and analyzing time-series medical data, providing enhanced anomaly detection while circumventing the limitations posed by vanishing gradients that often afflict traditional recurrent neural networks. Additionally, we refine the framework's security posture and interpretability by integrating an adversarial sample generation method that LIME informs. Accordingly, the contributions of this work are summarized as follows.

1) This study introduces an integrated framework that combines the strengths of blockchain and XAI to manage IoMT data securely and intelligently, addressing the pressing security and privacy concerns in the IoMT landscape.
2) This study leverages blockchain's traceability and tamper-proof characteristics to ensure the secure transaction of IoMT data. By transforming these transactions into a two-stage Stackelberg game, we offer a novel approach to data security.
3) To address the challenges of anomaly and cyberthreat detection in medical time-series data, this study models the data using Bi-SRU, which enhances detection accuracy and overcomes the common problem of vanishing gradients that many traditional models face.
4) This study proposes a method based on LIME for adversarial sample generation. This method serves multiple purposes: it assesses, improves, and secures the anomaly detection model. By enhancing the model's explainability, it ensures that the system remains transparent. Additionally, it fortifies the model against potential adversarial attacks, ensuring robustness.

The rest of the paper is organized as follows. Section II studies the blockchain-based IoMT data security transaction scheme. Section III presents an IoMT secure data management

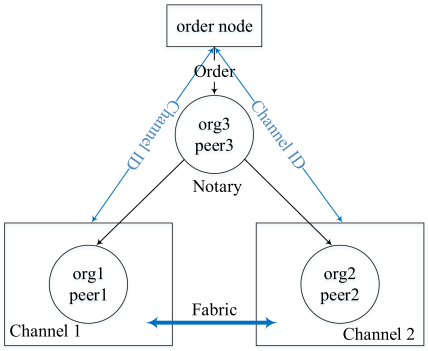


Fig. 1. Dual-chain architecture diagram of IoMT data security transaction scheme.

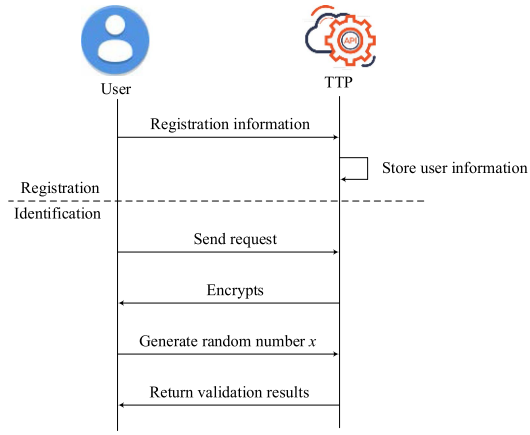


Fig. 2. Registration process.

framework based on Bi-SRU and XAI. The experimental study is conducted in Section IV. Section V provides our concluding remarks along with the directions for future research.

II. Blockchain-Based IoMT Data Security Transaction Scheme

There are three types of entities in the proposed IoMT data security transaction scheme: IoMT devices, users, and IoMT data brokers. The scheme uses a dual-chain architecture for IoMT data transactions, and the main-chain supports ordinary IoMT data transaction behaviors, that is, data transactions between IoMT devices and users. Dual-chain architecture offers several advantages over traditional single-chain approaches regarding performance, scalability, and security. By separating the main chain and side chain transactions, the dual-chain design enables efficient handling of different types of transactions, reducing latency and improving throughput. The isolation of the chains also enhances security by minimizing the impact of potential attacks and providing enhanced privacy features. However, the dual-chain architecture may introduce additional complexity and coordination overhead compared to single-chain approaches.

The profit game is mainly calculated and traced by the transaction records on the main-chain. On the sidechain, resale price agreement, profit distribution, and other data trading behaviors with resale as the goal are completed between IoMT devices and IoMT data brokers. This design choice is instrumental in addressing the unique demands of IoMT ecosystems, where rapid processing of large data volumes must not compromise the stringent security requirements associated with patient data. The dual-chain approach enhances the scalability and flexibility of data management in IoMT and ensures greater resilience against unauthorized alterations, thereby fortifying the trust in digital healthcare infrastructures. The overall architecture of the scheme is shown in Fig. 1. The Fabric cross-channel way is used to realize the dual-chain architecture. The notary node is used to carry out cross-chain calls of smart contracts (chain codes) between channels. The peer node is consistent with the single-chain execution and can perform basic operations on smart contracts. Under the dual-chain architecture, notary nodes can query and trace the ledgers of different channels.

A. Registration of Transaction Participants

Anyone who can participate in current public blockchain transactions gets verified without authentication, there are no restrictions on participation, transparency is high, and since many users have transaction records, integrity is guaranteed. However, anonymous users have malicious behavior, usually in fake transactions, which increases the waiting time for legitimate transaction verification, as the blockchain verifies all transactions, eventually overloading the system network. In the proposed scheme, users must complete authentication to prevent fake transactions, and any individual who wants to act as IoMT data brokers or make transactions in the system must go through the corresponding authentication process. The authentication process is carried out off-chain, and the whole process is divided into two steps: user registration and verification. TTP stands for trusted third party, as shown in Fig. 2.

The user registration process is divided into two steps, which are the generation of user identity parameters and the saving of identity information.

Step 1: The user generates public parameters GenInfo $\rightarrow$ $(\mathrm{PK_U}, \mathrm{SK_U}, \mathrm{ID}, \mathrm{pwd})$, which are the user's public key, private key, identity ID, and password to enter the system.

Step 2: The user sends the registration information to TTP using TTP's public key.

$$enc\left(\left(ID, H\left(pwd||H\left(ID\right)\right), PK_U\right), PK_{TTP}\right). \quad (1)$$

where $H(\mathrm{pwd}||H(\mathrm{ID}))$ represents the hash of identity ID and password, which is used for verification in subsequent steps. After receiving the user information, the TTP decrypts it with the private key $\mathrm{SK_{TTP}}$ and stores it in the server for storage.

B. Profit Game

First, the profit distribution game process of loMT devices and IoMT data brokers in the transaction is described in stages. The

maximum profit calculation of IoMT devices and the maximum profit constraints are shown in (2).

$$\begin{aligned}
&\max_{r,y} P(r,y) = \sum_{i\in I}\sum_{j\in J}\sum_{k\in K}(1-r_{ik})p_k y_{ijk} \\
&\quad + \sum_{j\in J}\sum_{k\in K}(p_k - c_{0jk})y_{0jk} \\
&\text{s.t.} \sum_{i\in I} y_{ijk} + y_{0jk} = \delta_{jk}, (\forall j \in J, \forall k \in K) \\
&y_{ijk} \in \{0,1\}, (\forall i \in I, \forall j \in J, \forall k \in K) \\
&r_{ik} \in [0,1], (\forall i \in I, \forall k \in K). \qquad (2)
\end{aligned}$$

where $P(r, y)$ represents the profit of IoMT devices, I, J, and K represents the node set and dataset, $1 - r_{ik}$ represents the revenue share of IoMT devices after each round of reselling data, and p_k represents the price of selling a certain data. y_{ijk} is quantitative, and a value of 1 means that node i sends data k to node j.

This scheme allows IoMT data buyers to become IoMT data brokers, but the buyers need to reach distribution price and profit distribution with IoMT devices on the sidechain. After that, the designated user can participate in the sales behavior through the main-side chain contract anchor. The game process of calculating the maximum profit of IoMT data brokers is shown in (3).

$$\begin{aligned}
&\max_{r,y} R(r,x,y) = \sum_{j\in J}(r_{ik}p_k - c_{ijk})y_{ijk} - x_{ik}p_k \\
&\quad - l_{ik}\ln\frac{1}{1+o_k - x_{ik}o_k} \\
&\text{s.t. } x_{ik}\delta_{jk} \geqslant y_{ijk}, (\forall i \in I, \forall j \in J, \forall k \in K) \\
&x_{ik} \in \{0,1\}, (\forall i \in I, \forall k \in K). \qquad (3)
\end{aligned}$$

where $R(r, x, y)$ represents the profit maximization game process of IoMT data brokers, r_{ik} represents the profit share of reselling data after the buyer becomes IoMT data brokers, $(r_{ik}p_k - c_{ijk})y_{ijk}$ represents the final profit obtained by IoMT data brokers, $x_{ik}p_k$ represents IoMT data brokers have paid for IoMT data k and downloaded and stored it to their nodes, and $l_{ik}\ln\frac{1}{1+o_k-x_{ik}o_k}$ represents the cost of storing IoMT data k is related to the size of IoMT data k and the measurement weight l_{ik} of cost.

C. Transaction Authority Control

The buyer needs to provide a zero-knowledge proof to the trusted node, and the trusted node calls the smart contract to return the encrypted hash value and the corresponding IoMT devices or IoMT data brokers' public key to the buyer [29]. The zero-knowledge proof steps are as follows.

Step 1: Setup$(\alpha, \beta, \gamma, \delta, x \leftarrow Z_p^*)$. The parameters σ and τ are generated by selecting random numbers in the integer field Z_p^*.

$$\sigma = ([\sigma_1]_1, [\sigma_2]_2). \qquad (4)$$

$$\sigma_1 = \left(\alpha, \beta, \delta, \{x^i\}_{i=0}^{n-1}, \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0}^{n-2}\right). \qquad (5)$$

$$\sigma_2 = \left(\beta, \gamma, \delta, \{x^i\}_{i=0}^{n-1}\right). \qquad (6)$$

$$\tau = (\alpha, \beta, \gamma, \delta, x). \qquad (7)$$

Step 2: Prove$(\pi \leftarrow \prod\sigma)$. Select two random numbers r and s and compute $\pi = \prod\sigma = ([A]_1, [C]_1, [B]_2)$.

$$A = \alpha + \sum_{i=0}^{m}\alpha_i u_i(x) + r\delta. \qquad (8)$$

$$B = \beta + \sum_{i=0}^{m}\alpha_i v_i(x) + s\delta. \qquad (9)$$

$$\begin{aligned}
C = &\frac{\sum_{i=l+1}^{m}\alpha_i(\beta u_i(x) + \alpha_i v_i(x) + w_i(x)) + h(x)t(x)}{\delta} \\
&+ As + rB - rs\delta. \qquad (10)
\end{aligned}$$

Step 3: Verify$(0/1 \leftarrow \varphi)$. Verify whether the equality is equal through (16) to determine whether the verification is passed, $0/1$ represents the flag of whether the verification is passed or not. If the verification is passed, the trusted node needs to send the cryptographic hash value and the corresponding Rivest–Shamir–Adleman public key. If the verification fails, it will return the verification failure result.

$$\begin{aligned}
[A]_1 \cdot [B]_2 = &[\alpha]_1 \cdot [\beta]_2 \\
&+ \sum_{i=0}^{l}\alpha_i\left[\frac{\beta u_i(x) + \alpha_i v_i(x) + w_i(x)}{\gamma}\right]_1 \\
&[\gamma]_2 + [C]_1 \cdot [\delta]_2. \qquad (11)
\end{aligned}$$

D. Transaction Authorization Verification

Resale rights are confirmed and verified in this scheme through main-side chain coordination. IoMT devices submit the perceptual hashing value of IoMT data on the side-chain (using pHash perceptual hashing algorithm), and use discrete cosine transform to reduce the frequency of multimedia data. The pHash applies a discrete cosine transform to the multimedia data to reduce the frequency and generate a compact hash value. This hash value is then stored on the blockchain, allowing for efficient comparison and verification of data rights. The smart contract compares the similarity of hash values to confirm data ownership and permissions.

In the transaction authority control and verification process, smart contracts play a crucial role. The main functionalities of the smart contracts include storing and verifying the cryptographic hash values of IoMT data, managing access control policies, and executing the verification logic. When a data transaction is initiated, the smart contract retrieves the corresponding hash value from the blockchain and compares it with the provided hash value. It then checks the access control policies to ensure the requesting party has the necessary permissions. If the verification is successful, the smart contract authorizes the transaction and updates the blockchain state accordingly. Specific

events or transactions trigger the execution of smart contracts and are automatically enforced by the consensus mechanism of the blockchain network.

E. Stackelberg Gaming Profit Distribution

This subsection will use Stackelberg game theory to break down the profit distribution process. Stackelberg game belongs to the master-slave game model in this paper. Followers are IoMT data brokers who want to resell IoMT data, and the leader is IoMT devices. The game's strategy is that IoMT devices allow IoMT data brokers to resell the IoMT data in the division r, and that IoMT data brokers store and sell IoMT data x and y. The calculation of the maximum values of $P(r, y)$ and $R(r, x, y)$ determines the maximum payout of a player in a finite order Stackelberg game.

The two-stage Stackelberg game is particularly suited for scenarios where one party's decisions influence the subsequent choices of others. In the context of IoMT, data transmitters, as leaders, first establish security protocols, anticipating potential actions from receivers. As followers, the receivers respond to these protocols, aiming to maximize their utility, which could include data integrity, access speed, and confidentiality. The Stackelberg model facilitates the identification of equilibrium strategies that ensure optimal security measures are in place, allowing for predicting outcomes from these interactions and enabling the system to adapt proactively to various strategic moves by either party. The two-stage Stackelberg game Nash equilibrium is calculated as follows.

$$P\left(r^*, y^*\right) \geq P\left(r, y^*\right), \forall r. \tag{12}$$

$$R\left(x^*, y^*, r^*\right) \geq R\left(x, y, r^*\right), \forall x, y. \tag{13}$$

where x^*, y^*, and r^* are the optimal values of x, y, and r, indicating that the Nash equilibrium can be reached fastest under these values.

To analyze the Nash equilibrium of the two-stage Stackelberg game, we need to analyze stage 2 first: the maximum return $\max R(r, x, y)$ of IoMT data brokers according to (3). For the objective function, the key variable that determines the profit of IoMT data brokers is x_{ik}, which turns the originally quantitative x_{ik} into a discrete variable within [0, 1]. Since the change of x_{ik} will increase monotonically with the quantification of y_{ijk}, the constraint function (4) will become

$$x_{ik}\, \delta_{jk} = y_{ijk}\ , \forall i \in I, \forall j \in J, \forall k \in K. \tag{14}$$

Substitute (15) into (3), and find the first derivative to calculate the maximum value,

$$\frac{\partial R\left(x, y\right)}{\partial x_{ik}} = \sum_j r_{ik} p_k \delta_{jk}\ - \sum_j c_{ijk}\delta_{jk} - p_k - \frac{o_k l_{ik}}{1 + o_k - x_{ik} o_k}. \tag{15}$$

Since (15) is a concave function, let $\frac{\partial R(x,y)}{\partial x_{ik}} = 0$, x_{ik} can be converted into a discrete variable in [0, 1], and we have

$$x_{ik}^* = -\frac{l_{ik}}{r_{ik} p_k \sum_j \delta_{jk} - \sum_j c_{ijk}\delta_{jk} - p_k} + 1 + \frac{1}{o_k}. \tag{16}$$

To ensure that x_{ik}^* is a discrete variable in [0, 1], the following constraints need to be added.

$$r_{ik} p_k \sum_j \delta_{jk} - \sum_j c_{ijk}\delta_{jk} - p_k \leq o_k l_{ik}. \tag{17}$$

$$\left(r_{ik} p_k \sum_j \delta_{jk} - \sum_j c_{ijk}\delta_{jk} - p_k\right)(o_k + 1) \geq o_k l_{ik}. \tag{18}$$

Equation (17) ensures that $x_{ik} \leq 1$, and (18) ensures that $x_{ik} \geq 0$. After the above steps, x_{ik} is quantitatively transformed from 0, 1 to a discrete variable within [0, 1].

III. Bi-SRU and XAI –Based IoMT Secure Data Management Framework

This section uses anomaly detection using Bi-SRU and XAI to address different aspects of data security and transparency in IoMT transactions.

A. Anomaly Detection Using Bi-SRU

Anomaly detection is a technique used to identify unusual patterns or deviations from the norm in data. In IoMT data security, this could be used to detect abnormal behavior or data patterns that might indicate a security breach or unauthorized access. Bi-SRU effectively captures dependencies in sequential data, which could help analyze IoMT data streams. Anomaly detection using Bi-SRU can be a part of the IoMT data security scheme. It can help identify unusual patterns in IoMT data transactions, potentially signaling security breaches or unauthorized access, which aligns with the scheme's goal of ensuring data integrity and security. Bi-SRU employs bidirectional processing, allowing the model to capture dependencies in both forward and backward directions. Additionally, Bi-SRU utilizes a reset gate mechanism with skip connections, alleviating the vanishing gradient problem by providing direct access to earlier hidden states. This enables the model to effectively maintain information flow and learn from long-range dependencies.

IoMT applications play a pivotal role in modern healthcare by continuously generating vast amounts of data, particularly multivariate time series data. This data type captures various measurements recorded over time, such as heart rate, blood pressure, temperature, and more. The complexity of IoMT data is heightened by intricate seasonal patterns operating at multiple scales, making it a unique and challenging dataset to work with. The architecture is shown in Fig. 3.

The forward and backward SRU capture dependencies in both directions. Consider a sample sequence:

The forward pass is as follows.

$$\vec{h}_1 = f\left(T_1, BP_1, HR_1\right)\ \vec{h}_2 = f\left(T_2, BP_2, HR_2, \vec{h}_1\right)\ \vec{h}_3 = f\left(T_3, BP_3, HR_3, \vec{h}_2\right). \tag{19}$$

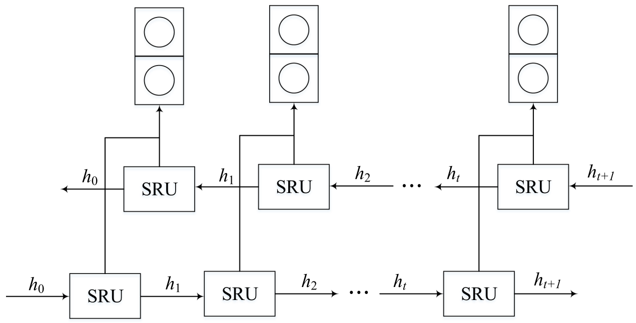


Fig. 3. Bi-SRU architecture.

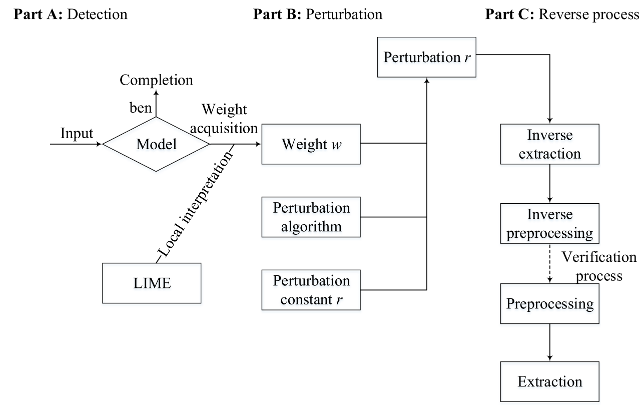


Fig. 4. LIME-based adversarial sample generation.

where $\vec{h}_t$ is the forward encoding at timestep t, T_t is the temperature at timestep t, BP_t is the blood pressure at timestep t, and HR_t is the heart rate at timestep t.

And the backward pass is as follows.

$$\overleftarrow{h}_3 = f\left(T_3, BP_3, HR_3\right)\ \overleftarrow{h}_2 = f\left(T_2, BP_2, HR_2, \overleftarrow{h}_3\right)\ \overleftarrow{h}_1 = f\left(T_1, BP_1, HR_1, \overleftarrow{h}_2\right). \tag{20}$$

where $\overleftarrow{h}_t$ is the backward encoding at timestep t.

The final encoding at each step contains both contextual information.

$$h_1 = \left[\vec{h}_1; \overleftarrow{h}_1\right]\quad h_2 = \left[\vec{h}_2; \overleftarrow{h}_2\right]\quad h_3 = \left[\vec{h}_3; \overleftarrow{h}_3\right]. \tag{21}$$

where h_t is the final concatenated encoding at timestep t.

This allows capturing long-range dependencies in complex IoMT data.

A single SRU contains a memory cell c_t and forget gate f_t:

$$\tilde{x}_t = Wx_g x_t + b_g\ f_t = \sigma\left(W_{fg} x_t + b_f\right)\ c_t = f_t \odot c_{t-1} + (1 - f_t) \odot x_t\ y_t = g\left(c_t\right). \tag{22}$$

where x_t is the input, W, b are learned weights and biases, σ is the sigmoid activation, g is the output activation, and $\odot$ denotes element-wise multiplication.

A reset gate r_t with skip connections tackles vanishing gradients:

$$r_t = \sigma\left(W_{rg} x_t + b_r\right)\ y_t = r_t \odot g\left(c_t\right) + (1 - r_t) \odot x_t. \tag{23}$$

The model is trained on normal IoMT data. At test time, anomaly scores are calculated using reconstruction error between the Bi-SRU embeddings and original input.

The error distribution can be modeled as a Gaussian:

$$p\ (x) = \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{(x-\mu)^2}{2\sigma^2}}. \tag{24}$$

The error value x is converted into an anomaly score $s \in [0, 1]$ using the Gaussian CDF:

$$s = 1 - \Phi\left(\frac{x - \mu}{\sigma}\right). \tag{25}$$

By leveraging Bi-SRU and modeling the reconstruction error as a Gaussian distribution, the model can effectively detect anomalies in complex IoMT time series data.

B. XAI for Trust and Transparency

XAI within the IoMT data security scheme can enhance trust and transparency. Users and stakeholders can better understand how and why certain decisions are made, such as data access approvals or transaction verifications. The LIME method generates local explanations for the anomaly detection model's predictions by perturbing input features and observing the impact on the model's output. We can identify the most influential features by analyzing these explanations and understanding the model's decision-making process. Furthermore, by generating adversarial samples that can fool the model, we can assess its robustness and iteratively improve its resilience to potential adversarial attacks.

The generation process of adversarial samples mainly contains four parts: detection (part A), perturbation (part B), reverse process (part C), and verification (bottom dashed line), as shown in Fig. 4.

Therefore, the problem solved by the adversarial example generation method can be described as follows.

$$\begin{cases} f\ (\boldsymbol{x}) = \text{mal} \\ f\ (\boldsymbol{x} + \boldsymbol{r}) = \text{ben} \end{cases}. \tag{26}$$

$$g\ (\boldsymbol{x}) = g\left(\boldsymbol{x} + \boldsymbol{r}\right). \tag{27}$$

where mal (malicious) is the malicious code classification label, ben (benign) is the benign code classification label, $\boldsymbol{x}$ is the input of the target classifier f, indicating the features extracted from the malicious code, $\boldsymbol{r}$ is the perturbation of $\boldsymbol{x}$ (perturbation), function g is the main program function for obtaining samples, $g(\boldsymbol{x})$ is the original main program function of $\boldsymbol{x}$, and $g(\boldsymbol{x} + \boldsymbol{r})$ is the modified main program function.

The perturbation constant $\boldsymbol{R}$ is used to describe the cost and ability boundary of the attacker in a specific attack scenario, that is, the adversarial capability - the ability of the attacker to modify the sample within a limited cost and keep the main program properties of the original sample. The following is the

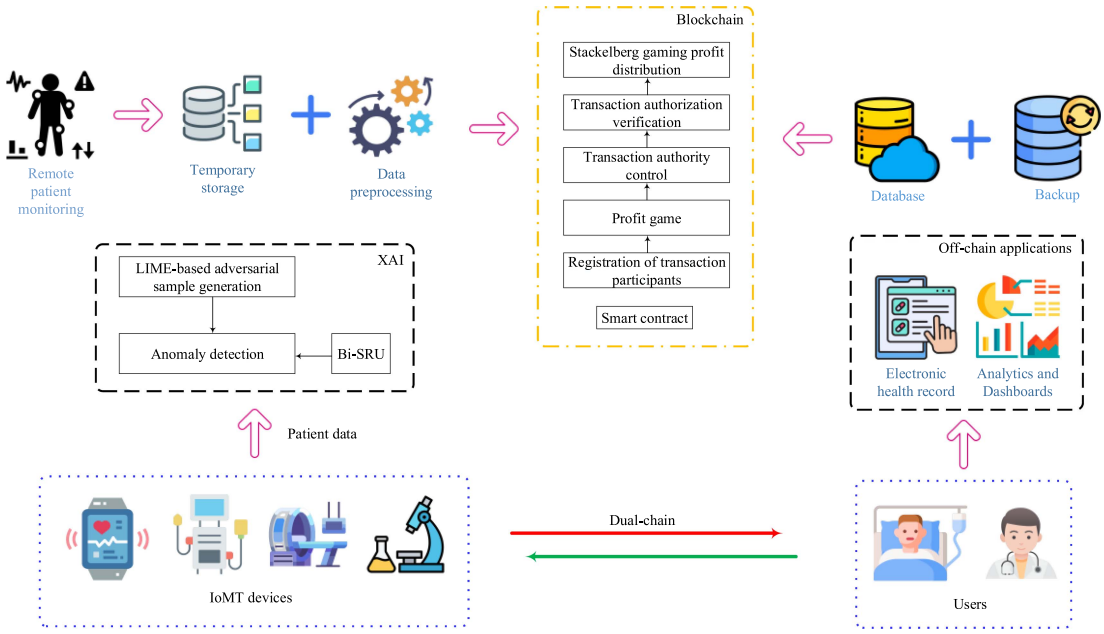


Fig. 5 Overall architecture of the blockchain-XAI framework for IoMT data management.

general form of $\boldsymbol{R}$.

$$\boldsymbol{R} = \{(d_i, s_{i1}, s_{i2})\, s_{i1} \leq s_{i2}, d_i \in [0,1]\}_{i=1}^{k} . \tag{28}$$

where k is a positive integer and d_i, s_{i1}, and s_{i2} are real numbers. $\boldsymbol{R}$ is a $k \times 3$ vector containing k perturbation rules. ith denotes the ith perturbation rule, and usually, one or two perturbation rules are used to describe one kind of feature, corresponding to addition and deletion rules.

The LIME-based adversarial sample generation method involves perturbing the input features of normal samples to create adversarial examples that can fool the anomaly detection model. The perturbations are guided by the local explanations provided by LIME, which highlight the features that have the most significant impact on the model's predictions. By iteratively modifying these influential features, we generate adversarial samples close to the model's decision boundary. These samples are then used to evaluate the model's robustness by testing its ability to classify them as normal or anomalous correctly. The insights gained from this evaluation are used to fine-tune the model's parameters, update the feature representation, or incorporate additional regularization techniques to improve its resilience against adversarial attacks.

In the LIME method, a simple model g is chosen to simulate the target classifier, and in this case a linear model is used as an example, so that $g(\boldsymbol{x})$ can be expressed as follows.

$$\boldsymbol{R} = \{(d_i, s_{i1}, s_{i2})\, s_{i1} \leq s_{i2}, d_i \in [0,1]\}_{i=1}^{k} . \tag{29}$$

where $\boldsymbol{\omega} = \{\boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \boldsymbol{\omega}_3, \cdots, \boldsymbol{\omega}_m\}$ is a parameter of g.

In the context of IoMT anomaly detection, the explanations generated by the LIME-based method can be presented as user-friendly to healthcare professionals and patients. For instance, when an anomaly is detected in a patient's vital signs data, the system can provide an explanation highlighting the specific features that contributed to the anomaly, such as an unusual heart rate pattern or a sudden drop in oxygen saturation levels. This explanation can help healthcare professionals understand the underlying reasons for the anomaly and take appropriate actions. Similarly, when the system recommends a particular treatment plan, it can explain the key factors considered, such as the patient's medical history, current symptoms, and predicted outcomes. This transparency allows healthcare professionals to assess the reliability and validity of the recommendation, fostering trust in the system.

Fig. 5 depicts the overall architecture of the blockchain-XAI framework for IoMT data management. Users, including patients, healthcare providers, and insurers, can access data or analytic outputs governed by smart contracts. Perceptual hashes verify the integrity and authenticity of data flowing across this pipeline.

IV. Experiments

A. Blockchain-Based IoMT Scheme

The blockchain-based IoMT data security transaction scheme proposed in this paper uses simulation experiments to test relevant performance. The simulation configuration is i7-11370H 3.30GHz CPU, 32 GB memory, and Raspberry Pi 4B ARM development board. The scheme is divided into three aspects: smart contract performance testing, zero-knowledge proof efficiency test, and gaming profit distribution change test.

1) Smart Contract Performance: RNN model temporal sequences but suffer from long-term dependency problems.

We test the running time and throughput of smart contracts used in the blockchain-based IoMT data security transaction scheme: the advantages of a dual-chain architecture compared to a single chain; generated and verified zero-knowledge proofs

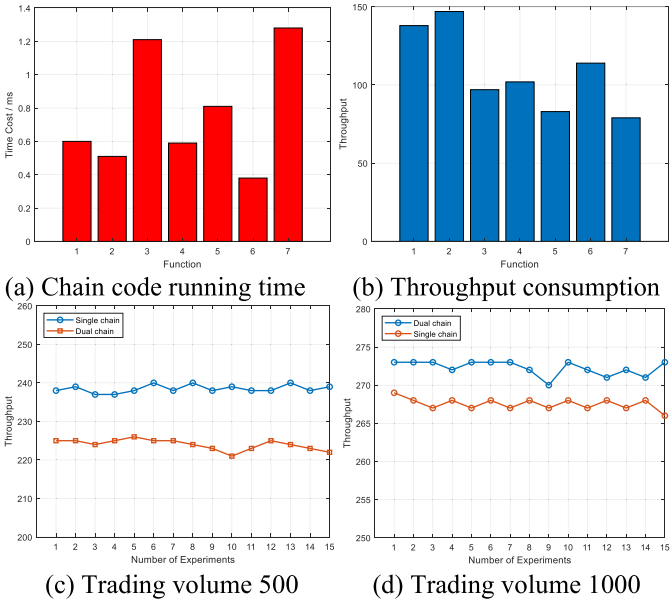


Fig. 6. Running time of chain code, throughput test and throughput test results under dual chain and single chain.

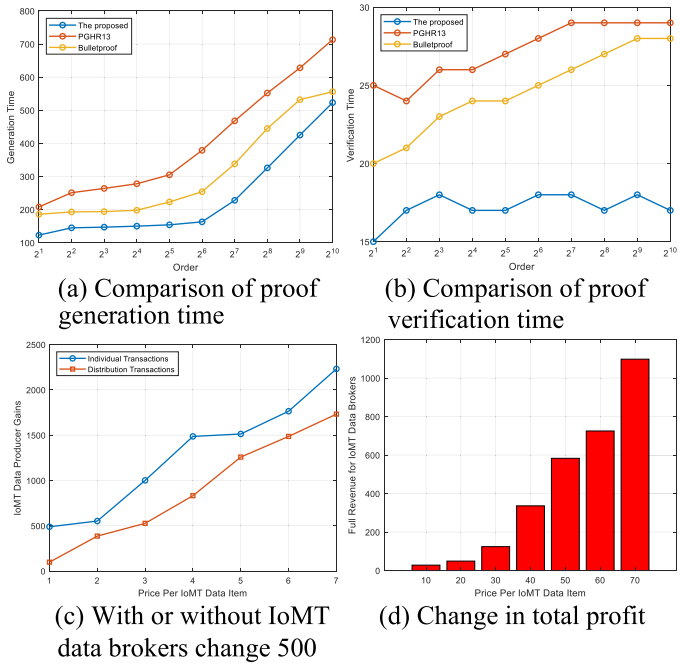


Fig. 7. Zero-knowledge proof efficiency comparison and distribution trading advantage.

under different numbers of leaf nodes; finally, the profits of IoMT devices and IoMT data brokers are tested when using a two-stage Stackelberg game. The IoMT data transaction process is simulated using the Caltech-256 dataset [30].

Figs 6(a) and (b) show the running time of smart contracts and throughput test results. Seven main functions are tested: IoMT device registration, buyer registration, IoMT data search, price agreement, perception hash detection, main-chain IoMT data transaction, and node zero-knowledge proof verification. Figs 6(c) and (d) show the comparison results of throughput in double-chain and single-chain architecture in blockchain-based IoMT data security transaction schemes under three nodes, which is a comparison of throughput in query. Through experiments, it can be seen that Fig. 6(c) corresponds to 500 trading volumes, and Fig. 6(d) corresponds to 2000 trading volumes. In the case of larger trading volumes, throughput has a significant improvement, and double-chain query has obvious advantages compared with a single chain.

2) Zero-Knowledge Proof Efficiency: Compared with the mainstream zero-knowledge proof frameworks PGHR13 and Bulletproof, the blockchain-based IoMT data security transaction scheme simplifies sending the commitment value. The efficiency of the generation time and verification time of the zero-knowledge proof in the blockchain-based IoMT data security transaction scheme is tested when the value is the same. The results are shown in Figs 7(a) and (b). Experiments have proven that the blockchain-based IoMT data security transaction scheme significantly improves generation and verification time compared with existing schemes.

3) Gaming Profit Distribution Changes: Fig. 7(c) and (d) show the profit income of the participants when the price of IoMT data items increases and the revenue profit share remains constant. Fig. 7(c) shows the profit situation after IoMT devices sell data alone. After joining IoMT data brokers, the profit of IoMT devices significantly improved. Fig. 7(d) shows the change in the total profit of IoMT data brokers when the price of IoMT data increases and the r_{ik} is constant. With the increasing price of IoMT data items, the profit of IoMT data brokers also shows a linear increase.

B. IoMT Secure Data Management Framework

1) Bi-SRU Anomaly Detector: The experiments are performed on the UNSW-NB15 and ToN_IoT datasets containing modern IoMT attack data [31]. A total of nine different attack types are included, which are password attacks, ransomware, scanning, backdoor, denial of service (DoS), distributed DoS (DDoS), man in the middle (MITM), code injection, and cross-site scripting (XSS).

Additionally, normal background traffic without any attacks is also included. The diverse attack types allow a thorough evaluation of anomaly detection performance.

Raspberry Pis, Arduinos, sensors, medical devices, etc., generate 24GB of labeled network traffic over 16 days. Unlike outdated synthetic datasets, this testbed effectively represents a natural healthcare IoMT deployment. Each network flow is treated as one timestep with 43 features, including protocol, packet size, flags, source IP, destination IP, etc. The hyperparameters are tuned using random search optimization. The model is trained for 100 epochs with early stopping based on the validation loss. The experiments are performed with an Intel Core i7-11370H 3.30GHz CPU, 32GB RAM, and NVIDIA RTX A2000 GPU.

TABLE I
COMPARISON OF ANOMALY DETECTION PERFORMANCE

Model	Accuracy	Precision	Recall	F1-Score
VLSTM	96.42%	94.23%	93.41%	93.82%
WIF-SGRU	97.84%	96.15%	95.53%	95.84%
IAEAD	96.82%	94.67%	93.92%	94.29%
BS-iForest	94.73%	92.87%	89.78%	91.29%
DOC	91.45%	89.06%	86.53%	87.77%
SAnDet	88.23%	89.18%	82.57%	86.91%
AnoGLA	96.48%	94.83%	93.40%	94.11%
Bi-SRU	99.72%	98.45%	97.96%	98.20%

The proposed Bi-SRU anomaly detector is compared against state-of-the-art recurrent neural networks and classical detection algorithms: VLSTM [22], WIF-SGRU [23], IAEAD [24], BS-iForest [25], DOC [26], SAnDet [27], AnoGLA [28].

The anomaly detection performance of the proposed Bi-SRU model is compared to state-of-the-art benchmarks. The average results over ten runs on the ToN_IoT dataset are presented in Table I.

The Bi-SRU model achieves a considerably higher accuracy of 99.72% compared to VLSTM (96.42%) and WIF-SGRU (97.84%). The precision, recall, and F1-score are also substantially improved. This empirically demonstrates the superiority of modeling IoMT time series data using Bi-SRU compared to standard recurrent networks. Among classical techniques, the IAEAD achieves the highest accuracy of 96.82%. However, the proposed Bi-SRU model outperforms it substantially by nearly 3%, demonstrating the effectiveness of Bi-SRU for intrusion detection in IoMT networks. The precision, recall, and F1-score metrics are also markedly higher.

Then, the detection accuracy on each of the nine IoMT attack types between Bi-SRU and benchmarks is shown in Table II.

The high accuracy of the Bi-SRU model in detecting various IoMT attack types, as demonstrated in Table II, positively impacts the XAI-driven intelligent IoMT secure data management framework. The exceptional performance of the Bi-SRU model in detecting a wide range of IoMT attack types ensures comprehensive security for healthcare systems, significantly enhancing the ability to identify potential threats, including common attack vectors like password breaches, ransomware, scanning, and more. The Bi-SRU model's high accuracy means it can detect IoMT attacks early, which is crucial for mitigating potential damage and reducing the impact of cyberattacks on medical data and patient safety. With its superior performance, the Bi-SRU model is less likely to generate false alarms, which can disrupt healthcare operations and lead to unnecessary interventions, more efficient use of resources, and a reduction in false positives.

2) LIME-based Adversarial Sample Generation: Attack experiments and comparison experiments are carried out separately to verify the effectiveness of the LIME-based adversarial sample generation (LASG) method proposed in this paper. The attack experiment is used to test the attack effect of the proposed method on the target classifier. Comparison experiments are used to compare with similar methods to strengthen the theory's validity.

This paper collects two disjoint sets of Win32 PE files, and for each PE file, the ASM file generated by the disassembly of its IDA pro is used to represent the PE file. The benign samples are derived from applications from over 50 vendors installed in the system image. The malicious samples contain ASM files corresponding to 10868 Win32 PE malware programs from nine malicious code families, including Ramnit and Lollipop.

Since the attacker hopes that the identified initially malicious samples will be marked as benign after being changed into adversarial samples, the difference between the true positive rate TPR before and after the attack is the proportion of effective adversarial samples. For intuitive consideration, the ratio of the difference between the TPR before and after the attack and the TPR before the attack is called the attack success rate and is denoted as ASR, then

$$\mathrm{ASR} = 1 - \frac{\mathrm{TPR}_{\mathrm{after}}}{\mathrm{TPR}_{\mathrm{before}}}. \tag{30}$$

To thoroughly test the effect of the method, the target classifiers can be divided into 18 according to the used algorithms or feature differences, as shown in Table III, including LASG, BS-iForest, DOC, multilayer perceptron (MLP) [32] algorithms, and the features include API, opc-2gram, opc-3gram.

The alg set represents the algorithm, and the fea set represents the feature, the cartesian product of the alg and fea sets. There are 12 ordered pairs of combinations (#1 to #12 in Table III), and a number represents a combination. For example, #1 represents (API, IAEAD), a classifier trained using API features and the IAEAD algorithm. Considering that the MLP-based model may have significant property differences according to the number of hidden layers, two additional groups of classifiers with different numbers of layers are set for #10 to #12 classifiers, so there are 18 target classifiers.

In the attack experiment, 60% of the malicious sample data set is used to train the target classifier. The LASG method generates adversarial samples of the above 180 attack samples to attack each target classifier. The disturbance constant is used to control the disturbance size, and the disturbance size-TPR diagram and disturbance size-ASR diagram were plotted to obtain the attack effect under different disturbance intensities. To further enhance the persuasion, this paper designs a comparative experiment: MalGAN and ZOO, two advanced black box adversarial sample generation methods, generate adversarial samples of attack samples, attack #1, #4, #7, #10, #13, #16 classifiers, record the changes before and after TPR attack, and perform comparative analysis with LASG method.

Fig. 8 shows the change graphs of TPR and ASR generated by attacking each target classifier by generating adversarial samples based on different perturbation dimensions (pd). Looking at the TPR graph, it can be found that the TPR of 18 classifiers drops to the level close to 0; that is, in the case of high perturbation cost, the proposed method successfully attacks almost 100% of any malicious code classifier.

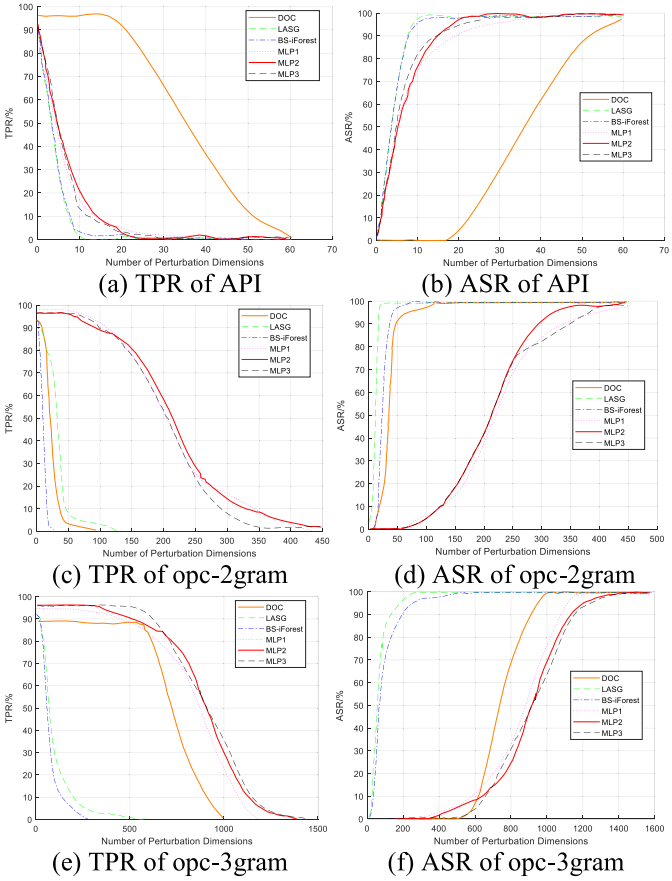
In the comparison experiment, MalGAN and ZOO generate adversarial samples of attack samples and attack #1, #4, #7, #10, #13, and #16 classifiers. Each classifier has different properties and different parameters. We choose the parameters that make

TABLE II
COMPARISON OF DETECTION ACCURACY

Attack Type	VLSTM	WIF-SGRU	IAEAD	BS-iForest	DOC	SAnDet	AnoGLA	Bi-SRU
Password	97.21%	98.12%	98.67%	93.81%	89.73%	87.03%	95.83%	99.51%
Ransomware	94.38%	96.23%	97.46%	91.27%	87.36%	84.28%	95.28%	98.62%
Scanning	96.51%	98.73%	98.91%	92.63%	88.92%	85.49%	95.37%	99.18%
Backdoor	97.82%	98.63%	99.11%	94.17%	90.26%	88.02%	97.54%	99.73%
DoS	98.17%	98.91%	99.46%	95.63%	91.84%	90.38%	96.63%	99.82%
DDoS	97.38%	98.37%	98.81%	93.17%	90.45%	86.74%	95.82%	99.46%
MITM	95.91%	97.82%	98.36%	92.45%	88.27%	84.59%	95.37%	98.94%
Code Injection	96.73%	98.17%	98.91%	93.81%	89.45%	86.78%	96.74%	99.67%
XSS	94.92%	96.45%	97.63%	91.37%	86.91%	83.74%	94.65%	98.78%

TABLE III
CLASSIFIER SETTING

Algorithms	opc-2gram	opc-3gram	API
LASG	#2	#3	#1
BS-iForest	#5	#6	#4
DOC	#8	#9	#7
MLP1	#11	#12	#10
MLP2	#14	#15	#13
MLP3	#17	#18	#16



(a) TPR of API (b) ASR of API
(c) TPR of opc-2gram (d) ASR of opc-2gram
(e) TPR of opc-3gram (f) ASR of opc-3gram

Fig. 8. Zero-knowledge proof efficiency comparison and distribution trading advantage.

TABLE IV
API FEATURE CLASSIFIER AND TPR COMPARISON

Adversarial sample generation methods	TPR / %					
	#1-LASG	#4-BS-iForest	#7-DOC	#10-MLP1	#13-MLP2	#16-MLP3
Without attack	89.6	98.8	95.4	92.3	95.6	95.1
ZOO	57.8	91.2	61.7	69.5	72.8	70.5
MalGAN	0	1.78	0.6	0	0	0
LASG	0	0	1.7	0	1.2	0

the adversarial samples more effective. After many experiments, the summary combined with the LASG method is shown in Table IV.

It can be seen from Table IV that both MalGAN and the proposed LASG method have good effects, and the attack effects are similar (TPR is reduced to a lower level, and the reduction is similar). ZOO does not perform well in the experiments, with TPR above 50% after the attack. MalGAN reduces TPR to 0 for classifiers #1, #10, #13, #16, and 1.67% and 0.56% for classifiers #4 and #7. The proposed LASG method reduces the TPR of #1, #4, #10, and #16 classifiers to 0. However, the TPR of #7 and #13 classifiers dropped to 1.67% and 1.1%, respectively.

The API feature in the experiment is One-Hot, and the corresponding value should be 0 or 1. However, ZOO may have -3, -1, and 2 values in the feature, and only through screening can we obtain the required adversarial samples, which will further reduce the effective adversarial samples. MalGAN is suitable for One-Hot type features and mainly contrasts the perturbative dimension of its generated pairs of anti-samples. Table V shows the average perturbation dimension pd of MalGAN and the proposed LASG method when they achieve good attack effects on each classifier. Among them, in the case of similar attack effects, the proposed LASG method has a smaller average disturbance dimension than the sample generated by MalGAN. This may be because the proposed LASG method has the design of the disturbance size of the needle.

TABLE V
MEAN PERTURBATION DIMENSION OF ADVERSARIAL SAMPLES

Adversarial sample generation methods	pd / number					
	#1	#4	#7	#10	#13	#16
MalGAN	26.5	24.6	99.8	23.6	34.1	28.4
The proposed	9.67	11.7	43.2	15.5	13.4	13.9

TABLE VI
TRAINING TIME COMPARISON (IN SECONDS)

Dataset Size	Bi-SRU	VLSTM	WIF-SGRU	IAEAD
10,000	85.2	92.4	88.7	95.3
50,000	402.7	438.1	419.5	451.2
100,000	792.5	861.8	825.4	887.9
500,000	3,885.6	4,225.3	4,048.1	4,357.2

Detecting and addressing these biases is crucial in healthcare to ensure fairness and avoid discrimination. In the medical field, explaining why an AI system flags a particular data point as anomalous is vital.

The proposed blockchain and XAI-driven framework holds significant potential for transforming healthcare data management and improving patient care. By integrating the framework with electronic health record systems, healthcare providers can ensure the security, integrity, and privacy of sensitive patient data while enabling seamless and authorized access across different healthcare entities. The framework can also be deployed in remote patient monitoring scenarios, allowing for secure and real-time transmission of vital signs and health data from IoMT devices to healthcare professionals, enabling timely interventions, personalized treatment plans, and improved patient outcomes. Furthermore, the framework facilitates secure data sharing among healthcare providers, fostering collaboration and knowledge exchange while maintaining patient confidentiality. Integrating XAI techniques enhances the interpretability and trustworthiness of AI-driven decision support systems, empowering healthcare professionals to make informed decisions. Overall, the proposed framework has the potential to revolutionize healthcare delivery, enable early disease detection, and promote personalized medicine while ensuring data privacy and security.

Subsequently, we conducted experiments on varying-sized datasets to evaluate the computational efficiency and scalability of the Bi-SRU anomaly detector. We compared the training and inference times with the baseline methods. Table VI presents the training times (in seconds) for different dataset sizes.

The Bi-SRU model demonstrates faster training times than the baseline methods across all dataset sizes. As the dataset size increases, the training time grows linearly, indicating good scalability. Table VII shows the inference times (in milliseconds) for different dataset sizes.

TABLE VII
INFERENCE TIME COMPARISON (IN MILLISECONDS)

Dataset Size	Bi-SRU	VLSTM	WIF-SGRU	IAEAD
10,000	12.5	14.2	13.6	15.1
50,000	58.7	66.9	64.2	69.3
100,000	115.3	131.5	126.1	136.2
500,000	565.8	644.2	618.4	667.5

TABLE VIII
SPEEDUP ON DISTRIBUTED COMPUTING ENVIRONMENT

Number of Nodes	Training Time (s)	Inference Time (ms)	Speedup Ratio
1	3,885.6	565.8	1.00
2	1,978.4	288.2	1.96
4	1,012.7	147.5	3.84
8	519.3	75.6	7.48

To further assess the scalability of the Bi-SRU model, we evaluated its performance in a distributed computing environment using Apache Spark. Table VIII presents the speedup achieved by the Bi-SRU model when trained on multiple nodes.

The proposed model exhibits faster training and inference times than the baseline methods, making it suitable for real-time IoMT anomaly detection tasks. The linear growth of training and inference times concerning the dataset size indicates good scalability. Furthermore, the Bi-SRU model's ability to achieve significant speedup in a distributed computing environment highlights its potential for large-scale IoMT deployments.

V. CONCLUSION

The proposed integrated framework, which combined blockchain technology and XAI, addressed the critical challenges surrounding the security, transparency, and intelligent management of medical data in the IoMT. It enhanced the secure transaction of IoMT data while protecting privacy and individual rights, utilizing a dual-chain architecture and perceptual hash technology. Bi-SRU was used for anomaly detection within medical time-series data, while a LIME-based adversarial sample generation method enhanced the explainability and robustness of the anomaly detection model. Simulation results demonstrated the superior performance of the proposed framework compared to benchmark solutions.

However, the proposed framework has limitations, such as the computational overhead associated with blockchain consensus mechanisms and AI model training. The consensus process can be resource-intensive, potentially impacting the system's scalability. Training complex AI models for anomaly detection and explainability also requires significant computational resources and time. These limitations can hinder the framework's deployment in resource-constrained environments and real-time applications. Addressing these challenges requires further research into lightweight consensus algorithms, model compression techniques, and efficient training strategies. Another challenge is the scalability and performance of the framework in handling large volumes of IoMT data in real-time. As the number of connected

devices and the volume of generated data continue to grow, the framework needs to process and analyze the data efficiently to support timely decision-making and interventions, which may require optimizations in terms of data processing, storage, and transmission protocols.

REFERENCES

[1] C. X. Huang, J. Wang, S. H. Wang, and Y. D. Zhang, "Internet of medical things: A systematic review," *Neurocomputing*, vol. 557, Nov. 2023, Art. no. 126719.

[2] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 53–71, Jan. 2020.

[3] M. Masud et al., "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 2021.

[4] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of medical things security assessment framework," *IEEE Internet Things J.*, vol. 8, Dec. 2019, Art. no. 100123.

[5] Q. G. Zhang, B. Z. Lian, P. Cao, Y. Sang, W. L. Huang, and L. Y. Qi, "Multi-source medical data integration and mining for healthcare services," *IEEE Access*, vol. 8, pp. 156010–165017, 2020.

[6] F. Khan, B. V. V. S. Prasad, S. A. Syed, I. Ashraf, and L. K. Ramasamy, "An efficient, ensemble-based classification framework for Big medical data," *Big Data*, vol. 10, no. 2, pp. 151–160, Apr. 2022.

[7] R. A. Alsemmeari, M. Y. Dahab, A. A. Alsulami, B. Alturki, and S. Algarni, "Resilient security framework using TNN and blockchain for IoMT," *Electronics*, vol. 12, no. 10, May 2023, Art. no. 2252.

[8] N. Shahdadpuri, S. Krishna, S. Reddy, C. Ganesh, K. Agarwal, and S. Bhattacharya, "Cloud-based fault prediction using IoT in office automation for improvisation of health of employees," in *Proc. 3rd Int. Conf. Adv. Comput. Innov. Technol. Eng.*, 2023, pp. 1240–1244.

[9] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7655, Aug. 2021.

[10] Z. T. Lian, Q. K. Zeng, W. Z. Wang, T. R. Gadekallu, and C. H. Su, "Blockchain-based two-stage federated learning with non-IID Data in IoMT system," *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 4, pp. 1701–1710, Aug. 2023.

[11] T. M. Choi and T. Siqin, "Blockchain in logistics and production from blockchain 1.0 to blockchain 5.0: An intra-inter-organizational framework," *Transp. Res. Part E: Logistics Transp. Rev.*, vol. 160, Apr. 2022, Art. no. 102653.

[12] Y. Gao, H. L. Lin, Y. J. Chen, and Y. L. Liu, "Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15785–15795, Nov. 2021.

[13] A. Lakhan et al., "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 664–672, Feb. 2023.

[14] T. Y. Zhu, L. Kuang, J. Daniels, P. Herrero, K. Z. Li, and P. Georgiou, "IoMT-enabled real-time blood glucose prediction with deep learning and edge computing," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 3706–3719, Mar. 2023.

[15] V. B. Lopez, E. D. Vecchia, A. Jean-Marie, and F. Ordonez, "Stationary strong stackelberg equilibrium in discounted stochastic games," *IEEE Trans. Autom. Control*, vol. 68, no. 9, pp. 5271–5286, Sep. 2023.

[16] S. Aggarwal et al., "An artificial intelligence-based stacked ensemble approach for prediction of protein subcellular localization in confocal microscopy images," *Sustainability*, vol. 15, no. 2, Jan. 2023, Art. no. 1695.

[17] X. F. Wang, Q. Zhang, C. T. Jiang, and J. R. Xue, "Perceptual hash-based coarse-to-fine grained image tampering forensics method," *J. Vis. Commun. Image Representation*, vol. 78, Jul. 2021, Art. no. 103124.

[18] X. F. Wang, X. R. Zhou, Q. Zhang, B. C. Xu, and J. R. Xue, "Image alignment based perceptual image hash for content authentication," *Signal Process.: Image Commun.*, vol. 80, Feb. 2020, Art. no. 115642.

[19] W. Saeed and C. Omlin, "Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities," *Knowl. Based Syst.*, vol. 263, Mar. 2023, Art. no. 110273.

[20] J. Ling, Z. S. Zhu, Y. Luo, and H. Wang, "An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit," *Comput. Elect. Eng.*, vol. 91, May 2021, Art. no. 107049.

[21] M. R. Zafar and N. Khan, "Deterministic local interpretable model-agnostic explanations for stable explainability," *Mach. Learn. Knowl. Extraction*, vol. 3, no. 3, pp. 525–541, Jun. 2021.

[22] X. K. Zhou, Y. Y. Hu, W. Liang, J. H. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Trans. Ind. Inform.*, vol. 17, no. 5, pp. 3469–3477, May 2021.

[23] J. F. Wang, Y. Jia, D. B. Wang, W. J. Xiao, and Z. F. Wang, "Weighted IForest and siamese GRU on small sample anomaly detection in healthcare," *Comput. Methods Programs Biomed.*, vol. 218, May 2022, Art. no. 106706.

[24] Z. Cheng, S. W. Wang, P. Zhang, S. Q. Wang, X. W. Liu, and E. Zhu, "Improved autoencoder for unsupervised anomaly detection," *Int. J. Intell. Syst.*, vol. 36, no. 12, pp. 7103–7125, Dec. 2021.

[25] J. X. Chen, Z. L. Zhang, R. X. Qian, J. F. Yuan, and Y. J. Ren, "An anomaly detection method for wireless sensor networks based on the improved isolation forest," *Appl. Sci.*, vol. 13, no. 2, Jan. 2023, Art. no. 702.

[26] J. Y. Sun, J. Shao, and C. K. He, "Abnormal event detection for video surveillance using deep one-class learning," *Multimedia Tools Appl.*, vol. 78, no. 3, pp. 3633–3647, Feb. 2019.

[27] S. Zavrak and M. Iskefiyeli, "Flow-based intrusion detection on software-defined networks: A multivariate time series anomaly detection approach," *Neural Comput. Appl.*, vol. 35, no. 16, pp. 12175–12193, Jun. 2023.

[28] Q. F. Ding and J. G. Li, "AnoGLA: An efficient scheme to improve network anomaly detection," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103149.

[29] P. W. Chi, Y. H. Lu, and A. Guan, "A privacy-preserving zero-knowledge proof for blockchain," *IEEE Access*, vol. 11, pp. 85108–85117, 2023.

[30] S. H. S. Basha, S. K. Vinakota, V. Pulabaigari, S. Mukherjee, and S. R. Dubey, "Autotune: Automatically tuning convolutional neural networks for improved transfer learning," *Neural Netw.*, vol. 133, pp. 112–122, Jan. 2021.

[31] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.

[32] J. P. A. Maranhao, J. P. C. L. d. Costa, E. P. de Freitas, E. Javidi, and R. T. de Sousa, "Noise-robust multilayer perceptron architecture for distributed denial of service attack detection," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 402–406, Feb. 2021.