Research on Identity Authentication and Privacy Protection Mechanisms for IoMT

Chenchen Wang

***Abstract*—With the rapid advancement of Medical Internet of Things (IoMT) technology, the interconnectivity of medical devices and data sharing have greatly enhanced smart healthcare. However, these developments also introduce critical security challenges, including data privacy breaches, inefficient identity authentication, and coarse-grained access control. To address the privacy preservation and secure authentication requirements for multi-stakeholder collaboration in medical ecosystems, this paper proposes a secure IoMT architecture that integrates multi-layered privacy protection mechanisms with lightweight authentication. The architecture aims to enable trusted data sharing, fine-grained access control, and efficient identity verification. This study focuses on two key contributions:(1) Lightweight Batch Verification Algorithm Using Schnorr Digital Signatures: A bidirectional identity authentication mechanism between sensor nodes and mobile terminals is developed. This mechanism ensures data integrity while substantially reducing computational overhead. (2) Local Differential Privacy Protection for Medical Data Sharing: To mitigate privacy leakage risks during data sharing, a privacy-preserving framework is designed. By strategically injecting calibrated noise into medical datasets, individual privacy is preserved without compromising data utility. This approach balances personalized privacy requirements with analytical validity, effectively preventing inference-based privacy attacks.**

***Index Terms*—Medical Internet of Things; Identity authentication; Local differential privacy protection; Schnorr digital signature; Batch verification**

I. Introduction

With the continuous development of technology and the improvement of living standards, people are paying more and more attention to their personal physical health. However, existing medical services and resources cannot meet people's existing healthcare needs. In recent years, with the rapid development of the Internet of Things and intelligent medical information technology, the medical Internet of Things has become an important means of achieving medical information sharing and collaborative work. Medical Internet of Things (IoT) is an extension of IoT technology in the medical field. Its purpose is to connect various sensors, medical devices, intelligent terminals, and information systems together through IoT sensing and communication technology, in order to achieve the collection, transmission, real-time monitoring, remote management, and intelligent analysis of medical data, and to meet the network of people to things and things to things communication for hospital operation and medical services. The medical Internet of Things can enable the interconnection and interoperability of medical production factors such as medical equipment, intelligent terminals, and medical facilities, realizing the "perception of all things, interconnection of all things, and intelligence of all things" in medical business, completely eliminating "information silos" and "data fragmentation", and greatly improving medical efficiency.

However, the issue of privacy leakage has become increasingly prominent. In order to improve the privacy and practicality of the medical Internet of Things, many scholars have focused on researching identity authentication and privacy protection methods. This paper aims to study the identity authentication and privacy protection mechanisms for the medical Internet of Things, in order to solve the security and privacy protection problems currently existing in intelligent healthcare, and to meet the security and privacy protection needs of the medical Internet of Things.

Through this study, we hope to provide an effective solution to improve the security and privacy protection of the medical Internet of Things, promote the secure sharing and collaborative work of medical information. We believe that by adopting advanced identity authentication and privacy protection mechanisms, the medical Internet of Things will be able to improve the efficiency and quality of medical work while protecting patient privacy.

Manuscript received May 10, 2025

Chenchen Wang, School of Computer Science and Technology, TianGong University, TianJin, China

II. Releated Work

A. Identity Authentication

The identity authentication scheme in the medical Internet of Things is mainly about improving and developing key algorithms and optimizing the cost of identity authentication. With the continuous development of the Internet of Things and medical technology, there have been many discoveries about identity authentication protocols in the medical Internet of Things.

In 2020, Mwittende and Ali et al.[1] proposed a bilinear based certificateless authentication scheme. However, for sensors, this solution will increase computing power and storage space, which will impose a huge burden on sensors with limited resources. Therefore, Zhang, He, and others[2] proposed an identity based encryption signature obfuscation method that utilizes mobile device resources to sign and encrypt data collected by sensors, reducing the burden on sensors. Xu et al.[3] and Thumbur et al.[4] also proposed a lightweight identity authentication scheme, respectively. In order to securely and efficiently transmit data between sensor nodes and intelligent terminals, it is not only necessary to achieve fast identity authentication, but also to establish session keys to encrypt data transmission[5]. At the same time, in order to accelerate communication, session keys

need to be established. However, one-on-one authentication methods can limit identity authentication efficiency[6][7]. Shen and Chang et al.[8] proposed a lightweight identity authentication scheme based on sensor and smart terminal identity authentication and session key sharing. Although the authentication efficiency is improved, it is susceptible to impersonation attacks. Xu and Chen et al.[9] proposed a lightweight scheme for anonymous authentication, taking into account the data privacy issues present in the medical Internet of Things.

B. Privacy Protection

The privacy protection in the medical Internet of Things mainly focuses on preventing the leakage of private data while ensuring the statistical characteristics of data. Privacy Preserving Data Publishing (PPDP) technology[10]-[12] is a centralized privacy protection based on a fully trusted third-party platform. The current PPDP technology mainly includes data encryption[13][14], data anonymity[15]-[17] and data perturbation[18]-[21].

PPDP technology based on data encryption uses encryption methods, such as homomorphic encryption[22][23], to hide information and protect privacy. Although this method has high data security and accuracy, and it is also very difficult for attackers to crack ciphertext, the computational cost is high and it is often used in distributed environments. In the big data environment, data not only needs to realize its usefulness, but also needs to ensure that the privacy of the participants and data providers is not leaked. Therefore, traditional encryption and decryption methods are completely insufficient.

Based on anonymous PPDP technology , in order to ensure data privacy is not leaked, in addition to removing some attributes of the data, some attributes should also be retained. This technology aims to weaken the correlation between sensitive attributes and individuals by performing generalization and suppression operations on data, in order to reduce the risk of privacy data leakage and ensure the authenticity and practicality of the data.

The perturbation based PPDP technique distorts the original data by adding noise or false data, as well as numerical exchange. Therefore, attackers cannot infer the correct original data based on the distorted data. However, this technology can cause significant information loss for a single data point, and its application scope is limited.

Collecting privacy protection data refers to participants being able to perform privacy protection locally, and then aggregate and analyze it on smart terminals. Unlike PPDP technology, which relies on fully trusted third-party platforms, this technology moves privacy protection to the local end without relying on third-party trusted platforms, reducing the risk of privacy leakage.

Differential privacy[22] is a widely recognized and robust privacy protection model, which is based on data distortion and achieves privacy protection by adding noise to the data. It is not related to the background knowledge possessed by the attacker, and even if the attacker possesses all data except for a certain participant data, it is still impossible for them to

obtain the privacy information of the participant. Therefore, differential privacy has received much attention since its proposal in 2006. However, differential privacy is also assumed to have a fully trusted third party during data processing, that is, centralized differential privacy[22][23]. In fact, there is no fully trusted third party, so some researchers have proposed a Local Differential Privacy (LDP) data collection framework[24]-[29], which not only has the characteristics of centralized differential privacy technology to quantify privacy attacks, but also refines the protection of personal sensitive information, and protects data privacy locally, alleviating the risk of third-party privacy litigation.

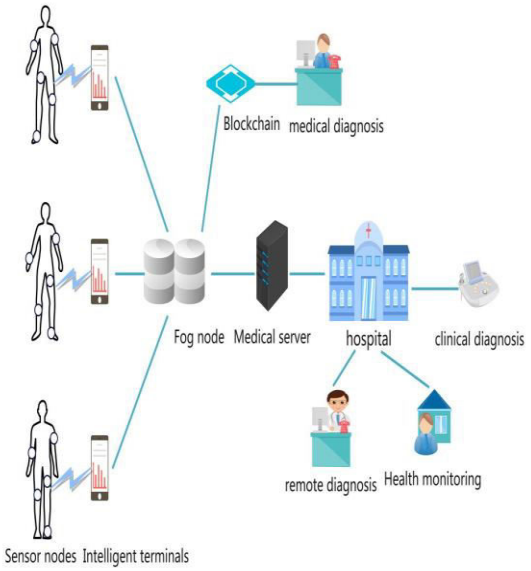
There are currently three types of perturbation mechanisms for localized differential privacy, namely random response[30], information distortion[31], and information compression[32]. Among them, random response technology is the mainstream disturbance technology, and the degree of disturbance can be directly quantified, with excellent performance. Random Response Technology (RTT) was proposed in the 1960s to collect statistical characteristics of sensitive data, add random noise to sensitive data, and hide individual information. At present, researchers have considered the personalized privacy needs of participants and applied the same perturbation treatment to individuals with the same needs.

III. Experimental Methods

In medical Internet of Things (IoMT) scenarios, secure transmission of sensor data, patient privacy protection, and fine-grained data sharing face multiple challenges. Firstly, traditional identity authentication methods struggle to balance lightweight operations with high security in resource-constrained environments between sensors and patient terminals. Particularly in batch verification scenarios, excessive computational overhead and communication costs may lead to efficiency bottlenecks and security vulnerabilities, failing to ensure data integrity and source reliability. To address these challenges, this paper proposes a lightweight batch verification scheme based on Schnorr digital signatures for IoMT data security transmission and privacy protection. A bidirectional identity authentication mechanism between sensor nodes and mobile terminals is developed, which guarantees data integrity while significantly reducing computational resource consumption. Additionally, to overcome the limitations of traditional Randomized Response (RR) mechanisms—including homogeneous privacy protection levels and insufficient differentiated protection for sensitive data—we innovatively propose a multi-dimensional sensitivity-adaptive Randomized Response perturbation mechanism.

A. System Model

The system model of the Medical Internet of Things proposed in this article is shown in Figure 1. The system model mainly includes six types of objects: sensor nodes, intelligent terminals, fog nodes, blockchain, medical servers, and medical staff.



Figue1 The Architecture Diagram of IoMT

1) Sensor nodes

Sensor nodes are responsible for collecting various medical data on or around patients, such as physiological parameters, motion data, etc.

2) Intelligent terminal

Intelligent terminals, as personal devices for patients or healthcare workers, receive sensor data and can perform local processing, display, and user interaction. For example, patients can monitor their own health status through smart terminals, while medical staff can use smart terminals to view patient data or perform remote monitoring.

3) Fog node

The fog node is located at the edge of the network and is responsible for receiving and processing data from sensor nodes. Fog nodes can provide real-time data processing, storage, and computing capabilities, reducing data transmission latency.

4) Blockchain

Blockchain will store abnormal data processed by fog nodes, and other medical staff can access the blockchain to query and verify the recorded abnormal data, achieving real-time monitoring and collaborative processing of patients.

5) Medical servers

Medical servers are located on higher-level networks or clouds, responsible for summarizing and storing large amounts of medical data, supporting medical information management systems, data analysis, and decision-making.

6) Medical staff

Medical staff can access data from medical servers through intelligent terminals or other devices, enabling remote monitoring, diagnosis, and treatment.

B. Achieving Goals

This article mainly studies the identity authentication technology and privacy protection of the medical Internet of Things. The specific research work is as follows:

1) Identity authentication is a major service of the medical Internet of Things, which enables intelligent terminals (i.e. access points) to verify the legitimacy of sensor nodes participating in communication. Only messages sent by authorized nodes can be detected and collected. However, traditional TCP/IP network authentication schemes have high computational and communication costs, and due to limitations in computing power, energy, and memory, these schemes are not suitable for the medical Internet of Things. Therefore, it is necessary to design a lightweight identity authentication between sensor nodes and intelligent terminals, which not only ensures security but also emphasizes efficiency and adaptability, achieves resource management and control, and protects the privacy of nodes.

2) Personal data contains a large amount of sensitive information, such as personal identity, health status, and financial information. If this information is leaked, it will cause very serious consequences to oneself. Therefore, data privacy protection should be adopted to strengthen the protection intensity and prevent data leakage.

C. Schnorr Batch-Verified Lightweight Identity Authentication

With the exponential growth of the scale of Internet of Things (IoT) devices, traditional identity authentication schemes face severe challenges in scenarios with limited resources. On the one hand, the computational overhead of signature verification for each item is difficult to meet the real-time requirements of low-power devices. On the other hand, when a large number of devices access concurrently, the centralized authentication architecture is prone to communication congestion and single-point failure risks. Especially in high-security scenarios such as the Internet of Medical Things (IoMT), it is necessary to ensure strong privacy protection capabilities for identity authentication while also taking into account the lightweight deployment requirements of device terminals. Aiming at the above problems, this section proposes a lightweight identity authentication protocol based on batch verification of Schnorr digital signatures (SBV-LIA) to reduce resource consumption, lower costs, conduct rapid verification, enhance security, and provide an efficient and secure lightweight authentication method for IoMT devices. Its workflow is shown in Figure 2.

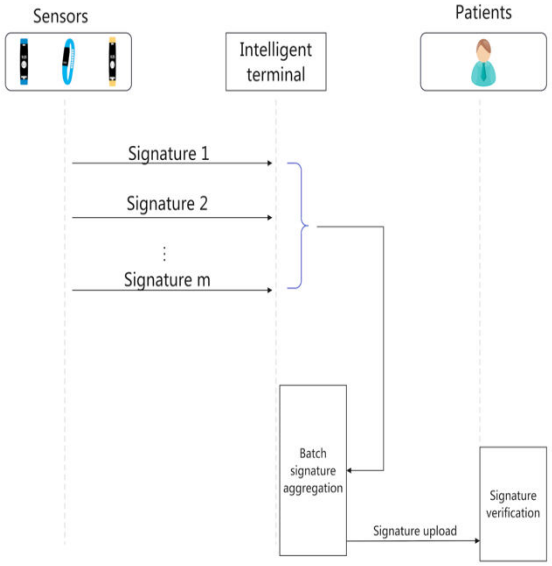


Figure2 Flow chart of SBV-LIA

1) Scheme Description

The process of identity authentication based on Schnorr between the sensor and the patient mainly consists of three parts, namely key generation, signature generation, and signature verification. The specific signature scheme is as follows:

a) Key Generation

i. Firstly, select large prime numbers p and q, where q is a prime factor of $p-1$, and $p \geq 2^{512}$, $q \geq 2^{160}$.

ii. Select a generator g of Z_p, and g satisfies: $g^q = 1 \ mod \ p$ where $q \neq 1$. H is a one-way hash function.

iii. Randomly select $u_i (1 < u_i < q)$. Calculate: $y_i = g^{u_i} \ mod \ p$. Then u_i serves as the private key of one sensor, and y_i serves as the public key of this sensor.

b) Signature Generation

i. The sensor randomly selects an integer k_i $(1 < k_i < q)$. Calculate $r_i = g^{k_i} mod \ p$.

ii. Calculate the formula: $h_i = H(r_i, M_i)$. where M_i is the signed message of this sensor.

iii. Calculate the formula: $s_i = k_i - u_i h_i \ mod \ q$. Take (h_i, s_i) as the signature of the sensor for the data M_i.

c) Signatue Verification

After the patient successively receives multiple signed messages M_i and signatures (h_i, s_i) from the sensor, the patient will verify the correctness of the signatures in batches. The specific steps are as follows:

i. Firstly, calculate: $r_i' = g^{s_i} y_i^{h_i} \ mod \ p$.

ii. Secondly, calculate: $h_i' = H(r_i', M_i)$.

iii. Calculate the collected batch signatures: $\sum_{i=1}^{n} s_i = \sum_{i=1}^{n} k_i - u_i h_i$.

iv. The patient checks: $\sum_{i=1}^{n} h' = \sum_{i=1}^{n} h$ whether it holds? If it holds, then (h_i, s_i) is a legal signature of M_i, and the patient will receive the data transmitted by the sensor; if it does not hold, the signature is invalid, and the patient will not receive the data transmitted by the sensor.

2) Analysis of the Correctness and Security of the Schnorr Signature Scheme

a) The correctness proof of the above signature is as follows:

$$\prod_{i=1}^{n} r'_i = g^{\sum_{i=1}^{n} s_i} y_i^{\sum_{i=1}^{n} h_i}$$

$$= \prod_{i=1}^{n} y_i^{h_i} \ g^{\sum_{i=1}^{n} s_i}$$

$$= \prod_{i=1}^{n} g^{u_i h_i} \ g^{\sum_{i=1}^{n} k_i - u_i h_i}$$

$$= g^{\sum_{i=1}^{n} u_i h_i} \ g^{\sum_{i=1}^{n} k_i - u_i h_i}$$

$$= g^{\sum_{i=1}^{n} k_i} = \prod_{i=1}^{n} r_i$$

From $\prod_{i=1}^{n} r'_i = \prod_{i=1}^{n} r_i$, we can get $H(r'_i, M_i) = H(r_i, M_i)$. That is $h'_i = h_i$. It can be seen that the signature (h_i, s_i) is valid.

b) Security Analysis

Strong Randomness: The random numbers used in Schnorr signatures are crucial. The signer, that is, the sensor, needs to select a random number and associate it with the discrete logarithm. If the generation of the random number is not random enough, it may lead to the leakage of the private key. And the strong randomness of random number generation is a major feature of Schnorr signatures.

Selective Message Attack: In a selective message attack, the attacker will try to forge signatures to fit specific messages. Protocols based on Schnorr signatures can usually resist selective message attacks because the signature verification process is carried out for the entire message space, not just for a single message.

Existential Forgery Attack: An existential forgery attack means that the attacker can generate a new signature that is valid under the signature algorithm without accessing the information of the legitimate signature. Protocols based on Schnorr signatures have strong resistance to existential forgery attacks because the security of Schnorr signatures is based on the discrete logarithm problem, and the attacker cannot find an equivalent signature of the legitimate signature within a reasonable time.

D. Research on the Data Privacy Protection Mechanism Based on Local Differential Privacy Protection

In the research on identity authentication and privacy protection for the Internet of Medical Things, this chapter focuses on the issue of balancing privacy protection and data availability. Aiming at the defects of the traditional Randomized Response (RR) mechanism, such as the simplification of privacy protection levels and the insufficient differential protection of sensitive data, this chapter innovatively proposes a multi-dimensional sensitivity adaptive randomized response perturbation mechanism.

1) Local Differential Privacy Data Collection Mechanism Based on Randomized Response

This section focuses on the exploration of personalized privacy security for multi-dimensional discrete symmetric privacy sources within the RR model. The relevant theories presented here are equally applicable to the RR model of binary discrete sources.

The localized data collection framework based on Randomized Response consists of two key components: client-side data perturbation and aggregated statistical analysis. The specific workflow is as follows:

Client-Side Data Perturbation: For an m discrete finite privacy source Y with a predefined prior distribution $P_Y = [P_1, P_2, \ldots, P_m]$, a sample set $Y = \{Y_1, Y_2, \ldots, Y_n\}$ from N participants is independently and identically distributed. Assume each participant (or sensor) holds one privacy-sensitive value. The sample Y_N undergoes randomized processing to generate perturbed data, which is then transmitted to data collectors such as smart terminals. Every privacy sample is perturbed via this randomized response mechanism.

Aggregated Statistical Analysis: Data collectors (e.g., smart terminals) aggregate the perturbed data $Y = \{Y_1, Y_2, \ldots, Y_n\}$ from N participants (sensor nodes) and perform statistical analysis to infer the distribution of the privacy source. The goal of collecting privacy-protected data in this section is to determine the prior distribution of the privacy source.

In this chapter, we adopt the Gradient Randomized Response (GRR) technique, which inherently falls within the framework of traditional Randomized Response (RR) models.

This model can be structured as a transmission process of a multi-dimensional discrete channel. The specific details of the model are as follows:

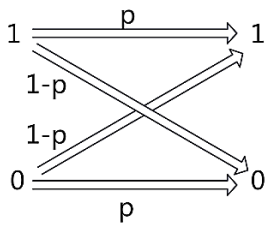


Figure2 Binary Symmetric Channel Modeling of the Randomized Response Process

Set the privacy source $Y = \{Y_1, Y_2, \ldots, Y_n\}$ (where $|Y| = m \geq 2$). After being perturbed by the privacy protection mechanism based on randomized response, the output is $H = \{H_1, H_2, \ldots, H_n\}$. Since this privacy protection mechanism can be represented as the conditional probability $P_{H\backslash Y}(H = h\backslash Y = y) = P_{H\backslash Y}(h\backslash y)$ of mapping $Y = y$ to $H = h$. If the multi-dimensional discrete channel is symmetric, then $Dom(Y) = Dom(H)$. This chapter mainly focuses on the symmetric privacy channel. Therefore, for the convenience of processing and analysis, when $i = j$, $Y_i = H_i (i, j \in \{1, 2, \ldots, m\})$.

By default, privacy information is of great significance to the localized privacy protection data collection mechanism of the CRR model, and the degree of privacy protection should not vary due to differences in sensitive values, that is, the privacy protection requirements for different sensitive values are the same. Assume that P_{CRR} is the privacy protection mechanism of the CRR model, which can be represented by an $m \times m$ row-stochastic matrix, and its expression form is:

$$P_{CRR}(h_j|y_i) = \begin{cases} P, & j = i \\ \dfrac{1-P}{m-1}, & j \neq i \end{cases}$$

That is, regardless of the sensitive values, the same privacy protection measures are implemented: the m-CRR model maintains the original value with a constant probability P and randomly outputs one of the remaining m-1 sensitive values with a probability of $(1-P)/(m-1)$. Additionally, P_{CRR} is an $m \times m$ symmetric matrix and has full rank, meaning it is an invertible matrix.

As indicated by the relevant formulas, the CRR model provides uniform privacy protection for all sensitive values, which raises an issue: some less sensitive values are overprotected, while highly sensitive values receive insufficient protection. In real-world scenarios, the sensitivity of different values varies significantly, and the required protection intensity should correspondingly differ, as privacy attackers may gain different benefits and cause varying impacts from different sensitive values. In view of this, this paper meticulously designs a personalized randomized response mechanism based on the CRR model. This mechanism aims to achieve personalized privacy-protected data collection, thereby enhancing participants' willingness to contribute data and alleviating their concerns about privacy issues.

2) Research on the Local Differential Privacy Mechanism of Personalized Randomized Response Based on the Weight of Sensitive Values

After adopting the Local Differential Privacy (LDP) data collection mechanism based on Randomized Response, the privacy protection capability of medical data during the transmission process has been significantly enhanced. However, traditional methods apply a uniform privacy protection intensity to all sensitive values, that is, they assign the same noise perturbation parameter to attribute values of different sensitivity levels (such as patients' ages, diagnostic results, gene sequences, etc.). This "one-size-fits-all" strategy not only leads to a waste of resources (for example, excessive noise addition to low-sensitivity attributes), but also may reduce the actual privacy protection effect of highly sensitive data. To address this issue, this subsection proposes a personalized randomized response mechanism based on the weight of sensitive values (Weighted Randomized Response, WRR), which achieves differential privacy protection by dynamically assigning weights to sensitive values.

The dataset used in this section focuses on a single dimension. This dataset contains a sensitive attribute X, and this attribute has m sensitive values, that is $X = \{x_1, x_2, \ldots, x_m\}$. In the CRR mechanism, for each sensitive value $x_i \in X$, the original value is maintained with the same probability P. Due to the consistent perturbation parameter, the degree of privacy protection is also the same.

However, in the PRR mechanism, we set the perturbation parameter according to the weight of the sensitive value to achieve personalized privacy protection. Let the probability that the sensitive value x_i is maintained in the PRR mechanism be (w_i), and it needs to satisfy the following conditions: (1) Non-negativity: For each sensitive value $x_i \in X, P(w_i) \in (0, 1]$. (2) Monotonicity: For any two sensitive values $x_i, x_j \in X$, if the sensitive value weight $w_i \geq w_j$, then the corresponding perturbation probability $(w_i) \geq P(w_j)$. This indicates that the subjective sensitivity of the sensitive value increases with the increase of the sensitive value weight, and its demand for privacy protection also increases accordingly.

The PRR model incorporates the key element of the weight of sensitive values to meet personalized privacy requirements. Its privacy protection mechanism P_{PRR} is expressed as:

$$P_{PRR}(h_j|y_i) = \begin{cases} P(w_i) & j = i \\ \dfrac{1-P(w_i)}{m-1} & j \neq i \end{cases}$$

In the m-PRR model, for the sensitive value $x_i \in X$, it responds with the probability of $P(w_i)$ and outputs the original value, and with the probability of $(1 - P(w_i))/(m-1)$, it responds and outputs one of the other m-1 sensitive values. The modeling of its m-ary symmetric channel is shown in the following figure 4:

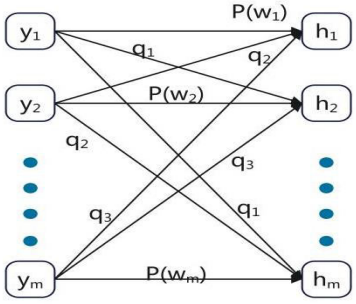


Figure 4 Modeling of m-ary Symmetric Channel for

Personalized Randomized Response Mechanism

As shown in the figure, the PRR model achieves the goal of personalized privacy protection. It applies low-intensity privacy protection to sensitive values with lower sensitivity and high-intensity privacy protection to sensitive values with higher sensitivity.

This chapter constructs a personalized privacy protection mechanism based on randomized response. This mechanism not only gives individuals control over their own private data but also, according to the strength of privacy needs, implements perturbation processing of corresponding intensities, effectively alleviating individuals' privacy concerns. In addition, when specific privacy leakage conditions are met, the data collection party can analyze and process the data, and then obtain relevant results.

IV. Experimental Results

A. Schnorr Batch-Verified Lightweight Identity Authentication

The batch identity authentication scheme based on Schnorr digital signature (SBV-LIA), significantly improves the identity authentication efficiency between sensor nodes and patient terminals in the Internet of Things medical scenarios by introducing the batch signature verification mechanism and the parallel processing architecture. It also saves resources and reduces consumption.

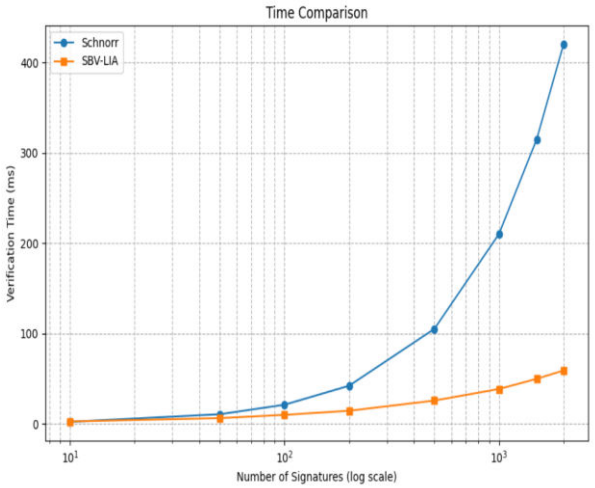


Figure 5 Comparison Graph of Number of Signatures vs. Verification Time

From Figure 5, we can see that when the number of signatures is 10, 20, 50, 100, 200, 500, 1000, 1500, and 2000, the verification time of our proposed SBV-LIA scheme is significantly lower than that of single-signature verification. Moreover, as the number of signatures increases, the time-saving advantage of our scheme becomes more pronounced. For example, when the number of signatures is 2000, the verification time of the SBV-LIA scheme is less than one seventh of the single-signature verification time. Additionally, as the number of signatures rises, the performance improvement ratio of SBV-LIA becomes increasingly large, reaching up to 86% when the number of signatures is 2000. Figure 3-3 clearly demonstrates the significant advantages of our proposed SBV-LIA scheme in large-scale scenarios, making it suitable for high-concurrency medical IoT systems or blockchain networks and notably enhancing computational efficiency.

B. Research on the Data Privacy Protection Mechanism Based on Local Differential Privacy Protection

1) Security Analysis

The privacy level of local differential privacy (LDP) can be explored from the following aspects:

Decentralization: Since LDP does not require a central server to store raw data, all privacy protection operations are completed on the user side. This avoids the risk of all data leakage caused by attacks or compromises on the central server.

Noise Addition: By adding random noise (such as Laplace noise or Gaussian noise) on the user side, attackers are prevented from inferring individual sensitive information by observing the output results.

Post-Processing Invariance: The output of LDP still satisfies differential privacy guarantees for any subsequent post-processing operations (such as aggregation or analysis), ensuring that privacy protection is maintained throughout the entire data processing flow.

2) Experimental Analysis

The following shows the relationship between ε and attack success rate obtained by varying ε.

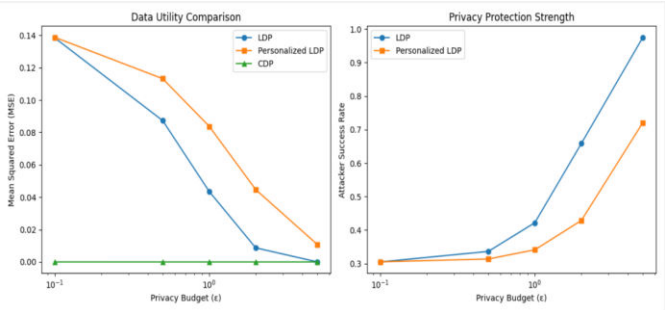


Figure 6 ε versus Attack Success Rate

From the comparative experimental graph in Figure 6, it can be seen that CDP (Centralized Differential Privacy) provides better data utility when ε is small but relies on a trusted third party; LDP (Local Differential Privacy) does not require a trusted party but incurs greater utility loss; personalized LDP offers a compromise between flexibility and security.

V. Conclusions

The rapid development of the Internet of Medical Things (IoMT) has brought revolutionary changes to the healthcare field. Through device interconnection and data sharing, it has significantly improved diagnosis and treatment efficiency as well as service quality, enabling patients to enjoy technological benefits such as remote monitoring and personalized diagnosis and treatment. However, the high sensitivity of medical data (e.g., disease diagnosis records, genetic information, medication history, etc.) makes it a primary target for hacker attacks. Statistics show that in 2023, the average single loss caused by global medical data breaches reached $10.8 million, far exceeding other industries. Data breaches not only threaten patient privacy but also risk damaging the reputation of medical institutions, leading to legal disputes, and causing social trust crises.

Therefore, how to achieve efficient operation and cross-institutional collaboration of IoMT systems while ensuring data security and privacy compliance has become a core issue urgently needing resolution in both academia and industry.

Aiming at the problem of effectively protecting user identity and data privacy security in IoMT, and combining the actual needs of medical scenarios, this paper constructs a privacy protection and security authentication system covering the entire process of "data collection-transmission-storage-sharing." It also proposes identity authentication and data privacy protection schemes for this application scenario:

1) For the resource-constrained characteristics of edge terminals such as wearable devices and implantable sensors, as well as the integrity and security of sensor data, a lightweight identity authentication method based on Schnorr digital signature batch verification is proposed. This method accelerates identity verification between sensors and patients, saving resources and reducing consumption.

2) To address the privacy leakage risks in medical data sharing, a data privacy protection mechanism based on local differential privacy protection is designed. By adding noise, it fulfills personalized privacy protection requirements.

This paper proposes storage and access schemes for user data to solve the problems of identity authentication and privacy protection in IoMT, significantly improving the utilization of medical resources.

ACKNOWLEDGMENT

The paper is not supported by any project.

REFERENCES

[1] G. Mwitende, I. Ali, N. Eltayieb, et al. Certificateless Authenticated Key Agreement for Blockchain-Based WBAN. Telecommunication Systems, 2020, 74(3): 347-365.W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] Y. Zhang, D. He, Y. Li, et al. Efficient Obfuscation for Encrypted Identity-Based Signatures inWireless Body Area Networks. IEEE Systems Journal, 2020, (99): 1-9.

[3] Z. Xu, C. Xu, W. Liang, et al. A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things[J]. IEEE Access, 2019, 7:53922-53931.

[4] G. Thumbur, G. S. Rao, P. V. Reddy, et al. Efficient Pairing-Free Certificateless Signature Scheme for Secure Communication in Resource-Constrained Devices[J]. IEEE Communications Letters, 2020, 24(8): 1641-1645. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[5] D. Yuan, X. Peng, T. Liu, et al. A novel approach to authenticated group key transfer protocol based on AG codes[J]. High Technology Letters, 2019, 25(2): 129-136.

[6] H. Tan, I. Chung. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor[J]. IEEE Access, 2019, 7: 151459-151474.

[7] B. Huang, G. Liu, M. Xu. Security Authentication Protocol for Nodes in Wireless Sensor Networks Based on Clusters[J]. Computer Engineering, 2016, 42(7): 117-122.

[8] J. Shen, S. Chang, J. Shen, et al. A lightweight multi-layer authentication protocol for wireless body area networks[J]. Future Generation Computer Systems, 2018, 78(3): 956-963.

[9] Z. Xu, C. Xu, H. Chen, et al. A lightweight anonymous mutual authentication and key agreement scheme for WBAN[J]. Concurrency and Computation: Practice and Experience, 2019, 31(14): e5295.

[10] Liu J, Zhang Z, Sun R , et al. An efficient certificateless remote anonymous authentication scheme for wireless body area networks. 2012:3404-3408.

[11] He D, Chen C, Chan S, et al. Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks. IEEE J Biomed Health Inform, 2013, 17(3):664-674.

[12] Ali A, Khan F A. Key Agreement Schemes in Wireless Body Area Networks: Taxonomy and State-of-the-Art. Journal of Medical Systems, 2015, 39(10):115.

[13] He D, Zeadally S. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine, 2015, 53(1):71-77.

[14] Jiang Q, Ma J, Wei F, et al. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. Journal of Network and Computer Applications, 2016, 76(dec.):37-48.

[15] Yu,Ge,Yuesheng,et al.TinyZKP: A Lightweight Authentication Scheme Based on Zero-Knowledge Proof for Wireless Body Area Networks.Wireless Personal Communications An Internaional Journal, 2014.

[16] Chen B C, Kifer D, LeFevre K. Privacy-preserving data publishing. Foundations and Trends in Databases,2009,2(1):1-167

[17] Jayapradha J, Prakash M. An efficient privacy-preserving data publishing in health care records with multiple sensitive attributes//2021 6th International Conference on Inventive Computation Technologies (ICICT). IEEE, 2021: 623-629.

[18] Song J, Zhong Q, Wang W, et al. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sensors Journal, 2020, 21(16): 17430-17438.

[19] Khalimov G, Kotukh Y, Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field//2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, 2021: 1-7.

[20] Vaidya J, Clifton C. Privacy preserving naive bayes classifier for vertically partitioned data//Proceedings of the 4th Siam International Conference on Data Mining. Florida,USA, 2004: 22-24.

[21] Wang Y, Tian J, Yang C, et al. Research on anonymous protection technology for big data publishing//2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS). IEEE, 2016: 438-441.

[22] Goswami P, Madan S. Privacy preserving data publishing and data anonymization approaches: A review//2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, 2017: 139-142.

[23] Gao Y, Luo T, Li J, et al. Research on k anonymity algorithm based on association analysis of data utility//2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, 2017: 426-432.

[24] Jiang H, Pei J, Yu D, et al. Applications of differential privacy in social network analysis: A survey. IEEE Transactions on Knowledge and Data Engineering, 2021, 35(1): 108-127.

[25] Xiao X, Tao Y, Chen M. Optimal random perturbation at multiple privacy levels. Proceedings of the VLDB Endowment, 2009, 2(1): 814-825.

[26] Du M, Wang K, Xia Z and Zhang Y. Differential privacy preserving of training model in wireless big data with edge computing. IEEE Transactions on Big Data,2020, 6(2):283-295.

[27] Gadepally K C and Mangalampalli S.Effects of noise on machine learning algorithms using local differential privacy techniques. //Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) . Toronto,ON,Canada:IEEE,2021:1-7.

[28] Li S, Zhao S, Min G, Qi L, Liu G. Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things. IEEE Internet of Things Journal. 2021 Mar 24;9(16):14542-50.

[29] Su Y, Yang B, Yang C, Tian L. FPGA-based hardware accelerator for leveled ring-LWE fully homomorphic encryption. IEEE Access,2020,8:168008-25.

[30] Warner, Stanley L. "Randomized response: A survey technique for eliminating evasive answer bias." Journal of the American Statistical Association 60.309 (1965): 63-69.

[31] Sarwate, A D, Sankar L. A rate-disortion perspective on local differential privacy.//Proceedings of the 2014 52nd Annual Allerton Conference on Communication, Control, and Computing.Monticello,IL,USA: IEEE,2015:903-908.

[32] Xiong S, Sarwate A D, Mandayam N B. Randomized requantization with local differential privacy. //Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) .Shanghai,China:IEEE,2016:2189-2193.