Hindawi
Security and Communication Networks
Volume 2021, Article ID 5580939, 13 pages
https://doi.org/10.1155/2021/5580939

Research Article

Blockchain-Based Efficient Device Authentication Protocol for Medical Cyber-Physical Systems

Fulong Chen, Yuqing Tang, Xu Cheng, Dong Xie, Taochun Wang, and Chuanxin Zhao

Anhui Normal University, Wuhu, China

Correspondence should be addressed to Fulong Chen; long005@mail.ahnu.edu.cn

Received 28 February 2021; Revised 5 April 2021; Accepted 16 April 2021; Published 4 May 2021

Academic Editor: Ke Gu

Copyright © 2021 Fulong Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As the background of application in the field of smart health care, the flexible interaction between patients and medical system is provided by medical cyber-physical systems (MCPSs) to realize all-round three-dimensional medical service. According to the controllable and credible requirements of MCPS, it needs a secure and reliable device identity authentication mechanism to build the security barrier. Based on the blockchain technology, a lightweight authentication scheme is designed for sensor/execution devices, users, and gateway nodes in MCPS. The security analysis and experimental results show that the scheme can resist the existing attacks with better efficiency; thus, our proposed scheme can be efficiently applied to the medical field.

1. Introduction

We have witnessed the great development of the Internet, as well as the popularity of the Internet of Things (IoT) and IoT devices, including wireless sensors, smart phones, wearable devices, global positioning systems, and laser scanners. These devices are widely deployed around us to realize intelligent computing and services, such as logistics, retail, medical, intelligent city, and other application fields. However, the trusted authentication in IoTs has become a major issue that has to be considered in the rapid development of IoTs.

Closely related to IoTs, medical cyber-physical systems (MCPSs) [1] are a kind of unique cyber-physical systems (CPSs) in the field of modern medicine, which combines the system operations with independent equipment to provide patients with new monitoring functions, such as controlling the physiological closed loop and alarm process of drug infusion process. In the MCPS, there are many kinds of devices with different performance. With the development of blockchain technology, the blockchain-based authentication schemes can mitigate some attacks, which ensure the security of the system. How to ensure that the security authentication protocol can work efficiently and reliably when using the blockchain technology is the key problem to be solved. Hence, based on the blockchain technology, we propose a device authentication scheme to ensure secure access to medical data among sensor devices nodes, gateway nodes, and users in the medical cyber-physical system. Specifically, our contributions can be summarized as follows:

(1) We distinguish the identity of the device nodes in the information physical space and propose a device security authentication model based on blockchain for the medical cyber-physical system.

(2) We design a blockchain-based efficient device authentication protocol. Our scheme is suitable for device nodes with different computing, transmission, and storage capacities and uses blockchain technology to solve the trustworthiness problem of third-party service centers. Meanwhile, we use BAN

logic and formal proof to verify the feasibility of our scheme and the security of mutual authentication process and the session key.

2. Related Works

Based on the extensive application of radio frequency identification (RFID) in medical environment, He et al. [2] analyzed the security requirements of RFID authentication scheme and summarized the performance and security of RFID authentication scheme based on elliptic curve cryptography (ECC). They found that although most authentication schemes cannot meet all the security requirements and have satisfactory performance, some ECC-based authentication schemes are suitable for medical environment in terms of performance and security. Combined with cloud storage, cryptography, and other technologies, a large number of authentication schemes are also proposed. The wireless body area network (WBAN) plays an indispensable role in MCPS. It is a network composed of multiple wearable devices or embedded devices, using wireless technology for communication. Therefore, in WBAN environment, a security and reliable authentication scheme is essential. Xu et al. [3] proposed a safe lightweight authentication scheme for WBAN. With this scheme, forward secrecy can be guaranteed without asymmetric encryption, and the security of the scheme can be verified and analyzed by using ProVerif. Alhayajneh et al. [4] analyzed and evaluated the accuracy, cost, and feasibility of the most prominent biometric authentication technology and proposed to use a variety of biometric authentication schemes to ensure the confidentiality, integrity, and reliability of WBAN. Moosavi et al. [5] proposed an end-to-end security scheme for mobile medical IoTs. Their solutions include a secure and efficient end-user authentication and authorization architecture based on certificate DTLS handshake, end-to-end communication based on session recovery security, and strong mobility based on Internet intelligent gateway. Amin et al. [6] proposed a mutual authentication and key agreement protocol to protect the confidential information in the device in order to prevent unauthorized users from accessing the general device. Aiming at the challenges brought by the electronic health information management system using IoTs, including the communication security of wireless channel, the protocol between authentication key and entity, access control scheme, and other defects, Aghili et al. [7] proposed a new lightweight, secure, and efficient authentication protocol, which is also suitable for access control. Aiming at the problem of authentication in edge and IoT environments, Ma et al. [8] proposed a blockchain-based decentralized authentication modeling scheme. Their scheme is suitable for multiple types of authentication (such as password-based, certificate-based, biometric-based, and token-based authentication). The edge cloud system also has many devices with limited computing and storage capabilities. Thus, Zhang et al. [9] proposed a collaborative authentication scheme among users, edge cloud, and robots, which reduced the computational cost of identity verification and improved the verification efficiency. In order to provide more accurate and effective biometric identification, Zhang et al. [10] proposed a parallel ECG-based authentication called PEA for smart healthcare systems.

According to the survey of Altman Vilandrie and Company [11], due to the lack of security authentication and other security systems, the IoT system of small- and medium-sized enterprises is vulnerable to attacks, resulting in their annual income loss of up to 13%. Chandrasekhar et al. [12] reported that the protocol of Yeh's protocol has some shortcomings, including incomplete forward secrecy, nonmutual authentication, and key agreement between users and sensor nodes. Shi and Gong [13] proposed an ECC-based user authentication protocol for wireless sensor networks, which is more efficient in computing cost, communication cost and security. However, Choi et al. [14] found that the protocol of Shi is vulnerable to session key attack, stolen smart card attack, and sensor energy depletion attack. In addition, an attacker can easily obtain the user's identity because it is transmitted through a public channel without encryption. Therefore, Choi et al. improved the protocol by verifying the identification legitimacy of users so as to keep from sensor energy consumption attacks. Compared with the protocol of Shi, the protocol also makes use of ECC to calculate authentication messages without bringing more cost. Both [13, 14] transmit user identity and sensor identity in plaintext on the public channel, so that they cannot provide anonymity. Chen et al. [15] proposed transmission protection, storage protection, and access control of infrastructure framework in the context of privacy protection of community medical IoT but did not mention the device security authentication. Shu et al. [16] proposed the aggregate signature algorithm, but it lacks the application background. Xue et al. [17] proposed a wireless sensor network identity authentication and key protocol based on temporary credentials, which only uses hash and XOR calculation. It has relatively more security features and higher security level without generating more communication and computing costs, but the traditional third party is vulnerable to attack. In order to solve the problem that the restricted computing power and storage of the sensors are vulnerable to physical attacks, Liu et al. [18] proposed a lightweight three-factor and anonymous user authentication protocol. The solution uses hash algorithms, XOR operations, and PUF to achieve lightweight and physical security. The wireless sensor network is widely used in medical, military, industrial, security, and other fields. Recently, Kumar et al. [19] discussed a wireless sensor network authentication protocol for coal mine safety monitoring. In the IoT environment, trust has become ubiquitous. It is not enough to just authenticate individual users or devices. The reason is that the cointeraction and cooperation between users and devices are crucial in the IoT environment. In this case, information sharing, data fusion, and other elements, including the integration of people, devices, and environment, are great challenges.

Traditional device authentication methods usually perform authentication when users and devices are separated from each other. At the same time, attackers can eavesdrop on communications, forge authentication tokens [20], or

perform replay attacks to simulate actual users or devices. The existing authentication schemes rarely consider the space-time characteristics of IoT computing. In general, authentication usually performs settings at once, and once users or devices are authenticated, they can operate for a long time without any authentication. This kind of time-sensitive authentication still needs to be improved so as to realize sufficient long-term trust guarantee, which is continuous authentication. Once an attacker fortunately bypasses the authentication system, various destructive attacks can be carried out. Therefore, the system can only respond to the attack passively, and the security network of IoTs is threatened.

Recently, researchers have gradually applied blockchain to the medical field. The combination of MCPS and blockchain can allow us to promote the sharing of services and resources and simplify several time-consuming workflows in an automated manner during the encryption verification [21]. In cloud-assisted telecare medical information system (TMIS), cloud servers are vulnerable to attacks. To solve this problem, Son et al. [22] used blockchain technology to design a secure identity verification protocol. In addition, they used CP-ABE to achieve data access control. Although the blockchain-based authentication scheme can enhance the security of the system, it is necessary to consider the authentication credentials and the accounting method of the authentication process when we use the decentralized blockchain as a third party to achieve authentication. Especially, the existing blockchain consensus algorithms and authentication protocols no longer adapt to the wide range of devices with vastly different performance in MCPS.

3. MCPS and Its Security Model

In the part of related works, we analyze the existing security risks and threats of device authentication. Therefore, we need to further improve the device authentication scheme to ensure the safety and reliability.

3.1. Classification of Medical Devices. With the rapid and revolutionary development of medical information, the medical equipment is widely used. The medical devices are classified as follows.

The first kind is the diagnostic equipment. It includes physical diagnostic instruments (sphygmomanometers, thermometers, all kinds of physiological recorders, etc.), images (MRI, B ultrasound, CT scanning, etc.), analytical instruments, and electrophysiology (EEG, etc.). These devices are distributed in each diagnosis and treatment area of the hospital, and the devices connected to the network need strict identity authentication.

The second kind is the treatment equipment. It includes ward nursing equipment (sickbed, oxygen bottle, etc.), surgical equipment, radiotherapy equipment, and emergency equipment (ventilator, cardiac defibrillation pacemaker, etc.). This kind of devices needs to be authenticated to ensure the safe use.

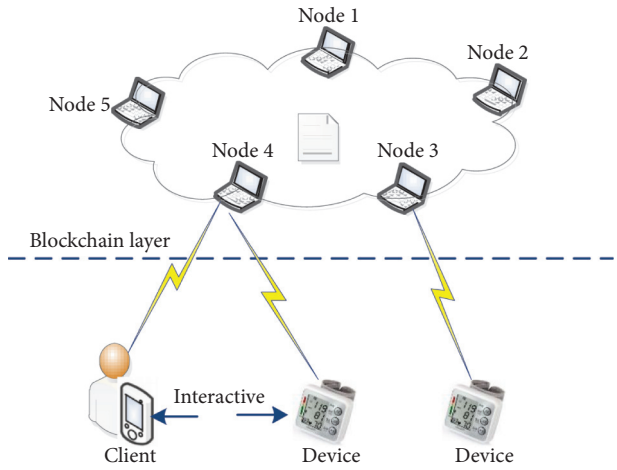

Figure 1: Model of device security authentication.

The third kind is the auxiliary equipment. It includes sterilization devices, refrigeration devices, and so on.

3.2. System Model. In order to study the problem of device security authentication in the MCPS, we first construct the system model of device security authentication based on the blockchain, as shown in Figure 1. The medical institutions are organized in a medical alliance chain to realize medical data sharing. The lower layer of the blockchain is composed of users and some medical equipment, which mainly completes data collection and other work; the blockchain layer is mainly used to realize the storage of medical data and the process of device security authentication.

As shown Figure 1, the device is mainly composed of sensor nodes. Sensor nodes can perceive various characteristics from different environments. In the MCPS, the collection process of medical data is mainly composed of medical professionals (doctors, patients, nurses, pathologists, etc.), sensors, and gateway nodes, as shown in Figure 2. The sensor nodes sense the patient's physical condition and then send the sign data in a certain electronic data format to the trusted gateway nodes of MCPS through the access point. As the core of the model in MCPS, the trusted gateway nodes execute the registration algorithm to provide the registration interface to all medical staffs. Medical staffs collect sensitive sign information of patients from the trusted gateway nodes, analyze them, and monitor patients' physical condition.

3.3. Architecture. MCPS increasingly relies on software to provide new functions, so that new medical software and devices can be more widely connected with the network to meet the needs of continuous monitoring of patients. The basic architecture of MCPS includes cyber space (including network space) and physical space (including user space), as shown in Figure 3. As the core of MCPS, cyber space includes the processing, storage, security access, and so on. Physical space is the physical basis of MCPS, including medical perception and control devices needed by users, such as electronic sphygmomanometer, heart rate, and pulse

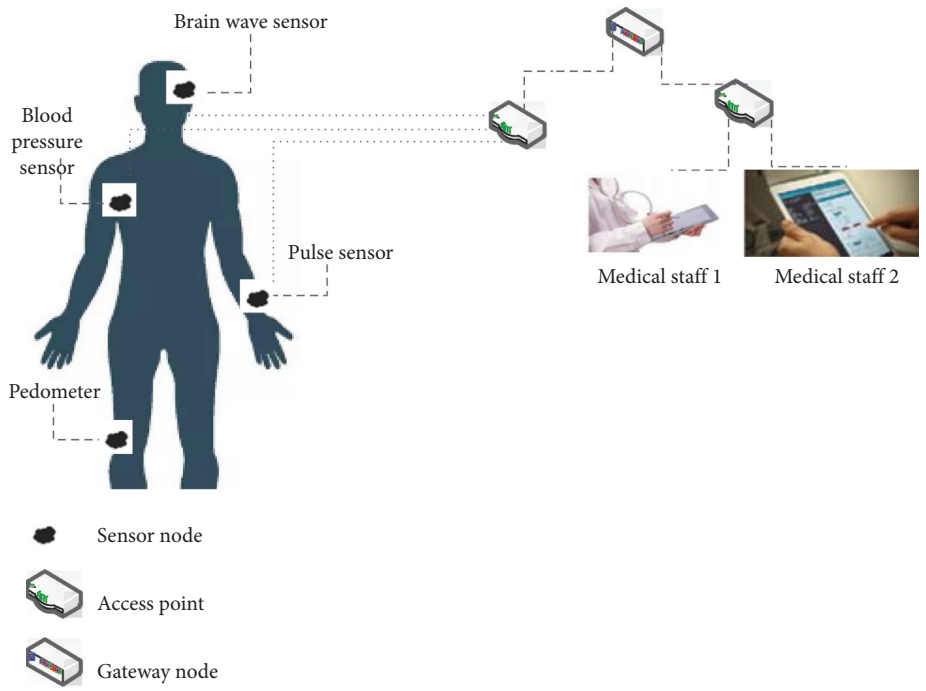

Figure 2: Collection process of medical data.

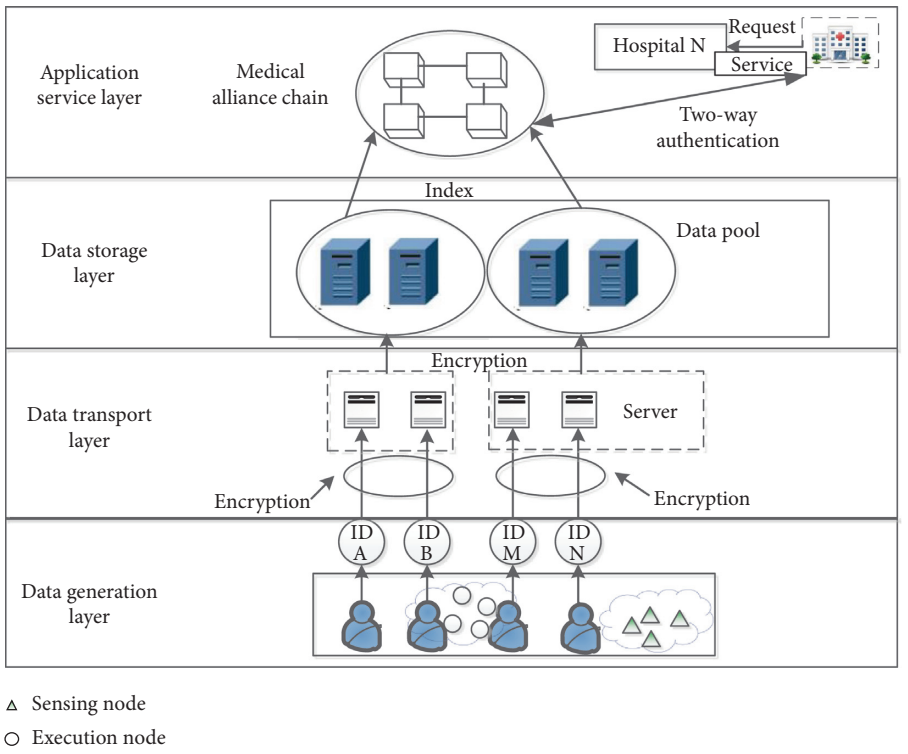

Figure 3: Blockchain-based architecture of MCPS.

collector, which are responsible for the collection and monitoring of user health information. MCPS is composed four layers such as data generation layer, data transport layer, data storage layer, and application service layer.

3.3.1. Data Generation Layer. At the bottom of MCPS architecture, it is mainly composed of a series of sensing nodes to collect the user's health information and transmit the collected data to the medical data storage space through the

tablet or other electronic devices. At the same time, after receiving the feedback information from the sensing nodes, the execution nodes complete the monitoring function of the user through the display or other alarms and execution devices and timely transmit the received information to the outside world, so as to realize the communication and feedback of information.

3.3.2. Data Transport Layer. It means that after the data collected by the data generation layer is encrypted or processed by other means, it is transmitted to the server by wired Ethernet or wireless transmission for storage. The service of the data transport layer is reflected through the running IPv4 or IPv6 protocol. Therefore, the level of data transport layer has a great relationship with the quality of network service, which requires higher network bandwidth, larger transmission range, faster transmission rate, stable transmission process performance, etc.

3.3.3. Data Storage Layer. The data storage object is the user's health information. The health information includes the user's medical records (sign data, outpatient medical records, hospitalization records, body temperature list, doctor's order list, laboratory test list, medical imaging examination data, special examination consent, operation consent, operation and anesthesia record list, pathological data, nursing records, and other medical records), etc. It uses blockchain and cloud storage technology to realize the secure storage and data sharing of medical records. The chain structure that stores the hash of medical data of each hospital, the digest, and the location index of medical data in cloud storage is called medical chain.

3.3.4. Application Service Layer. It focuses on application management and secure access to medical data. With the help of the platform technology of blockchain, we can provide data addition, deletion, insertion, decision-making, and diversified services. And the user can send the corresponding operation or control commands to the relevant execution nodes according to the access results to realize the feedback and exchange of information.

In the system model, we mainly combine the blockchain technology, build a system model of security authentication, and analyze the collection process of medical data under the blockchain. On the basis of this model, we need to consider how to ensure the security of the device node access. Therefore, we propose a secure data transmission protocol based on device authentication and key agreement. The proposed authentication protocol consists of six stages: system setup, user registration, user login, authentication, key change, and sensor node join. The symbols and descriptions used are shown in Table 1.

Table 1: Symbols and definitions.

Symbol	Description
BC	Blockchain center
SC	Smart card
U_i	User i (medical staff)
ID_i	ID of The user U_i
PW_i	Password of user U_i
GW_j	Gateway j
ID_g	Gateway node identifier
SN_k	The K^{th} sensor device node
$\mathrm{ID}_{\mathrm{sn}}$	Identifier of the sensor device node
S_{sn}	Shared key of sensor device and gateway node
SK_i	Session key
$\|$	Connection operation
$\oplus$	Exclusive or operation

4. Authentication Protocol

In this section, we propose a device security authentication scheme based on blockchain technology to ensure the security and reliability of sensor device nodes. The proposal in this section mainly includes the following parts.

4.1. Setup

(i) Step 1: the blockchain center BC selects S_{BC} as its private key and ID_g as the identifier of the gateway node and calculates

$$S_g = h\left(\mathrm{ID}_g \| S_{\mathrm{BC}}\right), \tag{1}$$

where S_g is selected as the private key of the gateway node.

(ii) Step 2: $\mathrm{ID}_{\mathrm{sn}}$ is the identifier of the sensor device node selected by the blockchain center BC, which calculates

$$S_{\mathrm{sn}} = h\left(\mathrm{ID}_{\mathrm{sn}} \| S_{\mathrm{BC}}\right). \tag{2}$$

It is the shared key between the gateway node and the sensor device node.

(iii) Step 3: $\{\mathrm{ID}_{\mathrm{sn}}, S_{\mathrm{sn}}\}$ is saved in SN_k by the blockchain center BC.

(iv) Step 4: the blockchain center BC saves $\{\mathrm{ID}_g, S_g, \mathrm{ID}_{\mathrm{sn}}, S_{\mathrm{sn}}\}$ and sends it to the gateway node GW_j in order to register SN_k with the gateway node.

4.2. User Registration. In order to access the medical data collected from sensor device nodes, each medical staff needs to register at the corresponding gateway. In the user registration stage, the medical staff sends the registration request to the gateway. After the preliminary verification, the gateway adds the user into its user list and sends one smart card storing user's identification information to the user. The

identification information may include some personalized parameters of the user, such as complex password in a certain length and identity credentials convenient for authentication in encrypted form. The steps of user registration are as follows:

(i) Step 1: the user selects a unique ID_i and PW_i, generates a random number r_1, and calculates

$$\mathrm{HPW}_i = h(r_1 \oplus \mathrm{PW}_i). \tag{3}$$

Then, the user sends $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$ to the gateway node GW_j.

(ii) Step 2: when the gateway node GW_j receives $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$, the gateway node GW_j generates another random number r_2 and calculates it at the timestamp T_1:

$$\begin{aligned} R_1 &= h(\mathrm{HPW}_i \| T_1), \\ R_2 &= h(\mathrm{HPW}_i \| \mathrm{ID}_g), \\ R_3 &= h(R_1 \| r_2 \| S_g) \oplus h(\mathrm{HPW}_i \| T_1). \end{aligned} \tag{4}$$

(iii) Step 3: the gateway node GW_j stores $\{r_2, T_1, \mathrm{ID}_g, h(\cdot), R_1, R_2, R_3\}$ in the smart card SC and then transmits it to the user U_i securely.

(iv) Step 4: when the user U_i receives $\{r_2, T_1, \mathrm{ID}_g, h(\cdot), R_1, R_2, R_3\}$, U_i calculates

$$\mathrm{HID} = h(\mathrm{PW}_i \| \mathrm{ID}_i) \oplus r_1). \tag{5}$$

And it writes it into the smart card.

4.3. User Login. In the login stage, the user U_i enters the identity identifier (identity credentials and password) in the device. The system first checks the correctness of the user input value and then sends the login message to the gateway. Once the authentication is successful, the user U_i can securely and legally access the remote computer data at any time according to the following steps:

(i) Step 1: the user U_i inserts the SC into the reader, then enters ID_i and PW_i.

(ii) Step 2: the user U_i selects a gateway node GID_j to obtain the data required by the user from the nearest sensor node.

(iii) Step 3: smart card calculates

$$\begin{aligned} r_1^* &= \mathrm{HID} \oplus h(\mathrm{PW}_i \| \mathrm{ID}_i), \\ \mathrm{HPW}_i^* &= h(r_1^* \oplus \mathrm{PW}_i), \\ R_2^* &= h(\mathrm{HPW}_i^* \| \mathrm{ID}_g). \end{aligned} \tag{6}$$

(iv) Step 4: the smart card checks whether R_2^* and R_2 are equal. If $R_2 = R_2^*$, the ID_i and PW_i of the user are verified; otherwise, the session is interrupted.

(v) Step 5: the smart card generates a random number r_3, and at T_2, it calculates

$$\begin{aligned} F_1 &= R_3 \oplus h(\mathrm{HPW}_i \| T_1), \\ F_2 &= h(T_2 \| r_3 \| F_1 \| \mathrm{ID}_g), \\ F_3 &= (r_3 \| T_2) \oplus F_1. \end{aligned} \tag{7}$$

(vi) Step 6: the smart card sends $\{\mathrm{ID}_{\mathrm{sn}}, F_2, F_3\}$ to the gateway node GW_j through the public channel.

4.4. Authentication. In the authentication stage, the gateway node first verifies the validity of the user's identity and then transmits the authentication message to the sensor device. After receiving the authentication message, the sensor device verifies the identification authenticity of the gateway node and then sends another message back to the gateway node so as to further prove its authenticity. After that, the gateway node sends a new message to the user node. In addition, the session key is calculated by each participant, including user nodes, gateway nodes, and sensor device nodes. In this stage, the following steps are performed to establish mutual authentication between the caregiver user node and the sensor device node.

(i) Step 1: when gateway node GW_j receives the login request $\{\mathrm{ID}_{\mathrm{sn}}, F_2, F_3\}$ at time T_3, GW_j calculates

$$\begin{aligned} F_1^* &= R_3 \oplus h(\mathrm{HPW}_i \| T_1) = h(R_1 \| r_2 \| S_g), \\ F_1^* \oplus F_3 &= (r_3^* \| T_2^*). \end{aligned} \tag{8}$$

(ii) Step 2: the gateway node GW_j checks whether $(T_3 - T_2)$ is less than ΔT, where ΔT is the maximum allowable transmission delay of the sender and receiver. If the condition is not met, terminate the session; otherwise, continue to the next step.

(iii) Step 3: the gateway node GW_j calculates

$$F_2^* = h(T_2^* \| r_3^* \| F_1^* \| \mathrm{ID}_g). \tag{9}$$

And it checks whether $F_2^* = F_2$. If met, the user U_i is authenticated; otherwise, the session is terminated.

(iv) Step 4: the gateway node GW_j generates a random number r_4 and calculates

$$\begin{aligned} R_4 &= h(\mathrm{ID}_{\mathrm{sn}} \| R_1 \| S_{\mathrm{sn}} \| r_4 \| T_3), \\ R_5 &= (r_3^* \| T_3 \| r_4) \oplus S_{\mathrm{sn}}, \\ R_6 &= R_1 \oplus h(\mathrm{ID}_{\mathrm{sn}} \| h(r_4) \| r_3^*). \end{aligned} \tag{10}$$

(v) Step 5: gateway node GW_j sends $\{\mathrm{ID}_{\mathrm{sn}}, R_4, R_5, R_6\}$ to sensor node SN_k.

(vi) Step 6: after the SN_k receives $\{\mathrm{ID}_{\mathrm{sn}}, R_4, R_5, R_6\}$, then at time T_4, it calculates

$$(r_3^{**} \| r_4^* \| T_3^*) = R_5 \oplus S_{\mathrm{sn}}. \tag{11}$$

(vii) Step 7: sensor device node SN_k checks whether $(T_4 - T_3)$ is less than ΔT. If the condition is not

met, terminate the session; otherwise, continue to the next step.

(viii) Step 8: sensor device node SN_k calculates

$$R_1^* = R_6 \oplus h\left(ID_{sn} \| h\left(r_4^*\right) \| r_3^{**}\right),$$
$$R_4^* = h\left(ID_{sn} \| R_1^* \| S_{sn} \| r_4^* \| T_3^*\right). \quad (12)$$

(ix) Step 9: the SN_k checks whether $R_4^* = R_4$. If met, it continues to the next step; otherwise, terminate the session.

(x) Step 10: the SN_k generates a random number r_5 and calculates

$$SK_i = h\left(R_1^* \| r_3^{**} \| r_4^* \| r_5\right),$$
$$B_1 = h\left(T_4 \| r_5 \| S_{sn} \| ID_{sn} \| T_3 \| SK_i\right), \quad (13)$$
$$B_2 = h\left(r_5 \| T_4\right) \oplus r_4^*.$$

(xi) Step 11: the SN_k sends $\{B_1, B_2\}$ to the gateway node GW_j.

(xii) Step 12: the GW_j receives the message $\{B_1, B_2\}$ at time T_5 and calculates

$$\left(r_5^* \| T_4^*\right) = B_2 \oplus r_4. \quad (14)$$

And it checks whether $(T_5 - T_4)$ is less than ΔT. If not met, the session is terminated; otherwise, continue to the next step.

(xiii) Step 13: the GW_j verifies whether $B_1^* = B_1$; if met, the SN_k is verified.

(xiv) Step 14: the GW_j continues to calculate

$$R_7 = h\left(SK_i \| R_1 \| r_4 \| T_5 \| R_4\right),$$
$$R_8 = \left(r_5^* \| r_4 \| T_5\right) \oplus r_3^*. \quad (15)$$

(xv) Step 15: the GW_j sends $\{R_4, R_7, R_8\}$ to the user U_i.

(xvi) Step 16: when the user receives $\{R_4, R_7, R_8\}$ at time T_6, the smart card calculates

$$\left(r_5^{**} \| r_4^* \| T_5^*\right) = R_8 \oplus r_3. \quad (16)$$

And it checks whether $(T_6 - T_5) \le \Delta T$; if not met, then terminate the session; otherwise, continue to the next step.

(xvii) Step 17: smart card calculates

$$R_7^* = h\left(SK_i \| R_1 \| r_4^* \| T_5^* \| R_4\right)$$
$$= h\left(SK_i \| h\left(HPW_i \| T_1\right) \| r_4^* \| T_5^* \| R_4\right). \quad (17)$$

If $R_7^* = R_7$, then both GW_j and SN_k authenticate with user U_i; otherwise, the session is terminated.

Among them, security authentication and key agreement phase is shown in Figure 4.

4.5. Password Change. This stage provides the user with the operation to change the password. An effective password change process can make the protocol friendly. In order to achieve this goal, the password change should not involve any other unnecessary participants, which can reduce communication costs and resist Denial of Service (DoS) attacks. Here are the steps to change the password:

(i) Step 1: the user U_i first inserts the SC into the reader device and then enters ID_i and PW_i.

(ii) Step 2: SC calculates

$$r_1^* = HID \oplus h\left(PW_i \| ID_i\right),$$
$$HPW_i^* = h\left(r_1^* \oplus PW_i\right),$$
$$R_2^* = h\left(HPW_i^* \| ID_g\right), \quad (18)$$
$$h\left(R_1 \| r_2 \| S_g\right) = R_3 \oplus \left(HPW_i \| T_1\right).$$

(iii) Step 3: SC compares R_2^* with R_2 already stored in *SC*. If $R_2^* = R_2$, the user identity and password are verified; otherwise, the session is terminated.

(iv) Step 4: U_i enters a new password PW_i^{new}.

(v) Step 5: SC calculates

$$HID^{new} = r_1^* \oplus h\left(PW_i^{new} \| ID_i\right),$$
$$HPW_i^{new} = h\left(r_1^* \oplus PW_i^{new}\right),$$
$$R_2^{new} = h\left(HPW_i^{new} \| ID_g\right), \quad (19)$$
$$R_3^{new} = h\left(R_1 \| r_2 \| S_g\right) \oplus h\left(PW_i^{new} \| T_1\right).$$

(vi) Step 6: the SC replaces R_2, R_3 and HID with the corresponding new values: R_2^{new}, R_3^{new}, and HID^{new}. Then, the password is changed successfully.

4.6. Sensor Node Join. When a new sensor device node needs to join the MCPS, the system will perform the following steps:

(i) Step 1: the blockchain center BC selects the new sensor node SN_k, uses ID_{sn} as its identifier, and calculates

$$S_{sn} = h\left(ID_{sn} \| S_{BC}\right). \quad (20)$$

And it stores $\{SN_k, S_{sn}\}$.

(ii) Step 2: BC sends $\{SN_k, S_{sn}\}$ to the gateway node.

(iii) Step 3: the gateway node stores this value and updates the information in the database.

5. Authentication Proof Based on Ban Logic

5.1. Definition of BAN. BAN (Burrows, Abadi, and Needham) logic is a popular identity authentication protocol analysis model. It helps to prove identity verification and key

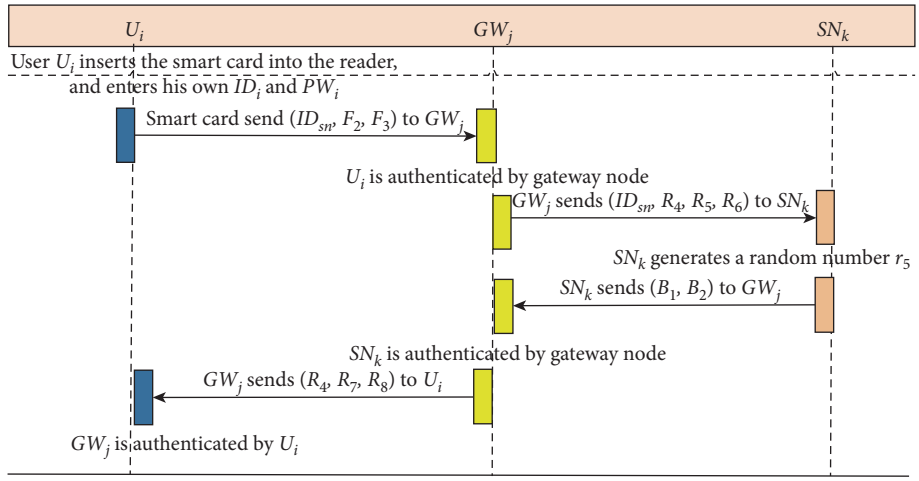

Figure 4: Security authentication and key agreement phase.

establishment, thereby proving the validity of the protocol [23, 24].

Now, we have defined some logical rules such as Message-Meaning rule (MM), Nonce-Verification rule (NV), Jurisdiction rule (J), Freshness-Conjuncatenation rule (FC), Session Key rule (SK), and Belief rule (B) used in the proof, and these rules are directly adopted from [25].

5.2. Formal Verification Process. All certification protocols need to achieve Goal 1, 2, . . ., 8. Here, the variables U_i, GW_j, and SN_k represent three subjects:

(i) Goal 1: $\mathrm{GW}_j| \equiv U_i \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$.

(ii) Goal 2: $\mathrm{GW}_j| \equiv U_i| \equiv U_i \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$.

(iii) Goal 3: $\mathrm{SN}_k| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{SN}_k$.

(iv) Goal 4: $\mathrm{SN}_k| \equiv \mathrm{GW}_j| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{SN}_k$.

(v) Goal 5: $\mathrm{GW}_j| \equiv \mathrm{SN}_k \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$.

(vi) Goal 6: $\mathrm{GW}_j| \equiv \mathrm{SN}_k| \equiv \mathrm{SN}_k \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$.

(vii) Goal 7: $U_i| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} U_i$.

(viii) Goal 8: $U_i| \equiv \mathrm{GW}_j| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} U_i$.

Make the following assumptions and analyze the initial state of the agreement:

(i) A_1: $U_i| \equiv \#(r_3, r_4, r_5)$.

(ii) A_2: $\mathrm{GW}_j| \equiv \#(r_3, r_4, r_5)$.

(iii) A_3: $\mathrm{SN}_k| \equiv \#(r_3, r_4, r_5)$.

(iv) A_4: $U_i| \equiv U_i \overset{F_1}{\leftrightarrow} \mathrm{GW}_j$.

(v) A_5: $\mathrm{GW}_j| \equiv \mathrm{GW}_j \overset{S_{sn}}{\leftrightarrow} \mathrm{GW}_j$.

(vi) A_6: $\mathrm{SN}_k| \equiv \mathrm{SN}_k \overset{S_{sn}}{\leftrightarrow} \mathrm{GW}_j$.

(vii) A_7: $\mathrm{GW}_j| \equiv \mathrm{GW}_j \overset{F_1}{\leftrightarrow} U_i$.

(viii) A_8: $\mathrm{GW}_j| \equiv U_i = > r_3$.

(ix) A_9: $\mathrm{SN}_k| \equiv \mathrm{GW}_j = > r_4$.

(x) A_{10}: $\mathrm{GW}_j| \equiv \mathrm{SN}_k = > r_5$.

(xi) A_{11}: $U_i| \equiv \mathrm{GW}_j = > r_4$.

Based on BAN logic rules and assumptions, we can analyze the ideal form of the protocol:

(i) Message 1: $U_i \longrightarrow \mathrm{GW}_j$: $\langle \mathrm{ID}_{\mathrm{sn}}, F_2, F_3 \rangle$

Using $P \triangleleft X$ rule:

R_1: $\mathrm{GW}_j \triangleleft \ll \mathrm{ID}_{\mathrm{sn}}, F_2$: $(T_2, r_3)_{F_1}, F_3$: $\langle r_3, T_2 \rangle_{F_1} \gg$

Using A_7, R_1 and MM rule:

R_2: $\mathrm{GW}_j| \equiv U_i| \sim (T_2, r_3, \mathrm{ID}_g)$

Using A_1, R_2 and FC rule:

R_3: $\mathrm{GW}_j| \equiv U_i| \equiv (T_2, r_3, \mathrm{ID}_g)$

Using A_8, R_3 and J rule, B rule, NV rule:

R_4: $\mathrm{GW}_j| \equiv r_3$

Using A_2, R_4 and SK rule:

R_5: $\mathrm{GW}_j| \equiv U_i \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$ (Goal 1).

Using A_2, R_5 and NV rule:

R_6: $\mathrm{GW}_j| \equiv U_i| \equiv U_i \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{GW}_j$ (Goal 2).

(ii) Message 2: $\mathrm{GW}_j \longrightarrow \mathrm{SN}_k$: $\langle \mathrm{ID}_{\mathrm{sn}}, R_4, R_5, R_6 \rangle$

Using $P \triangleleft X$ rule:

R_7: $\langle \langle \mathrm{ID}_{\mathrm{sn}}, R_4, R_5$: $\langle r_3, r_4, T_3 \rangle_{S_{sn}}, R_6 \rangle \rangle$:

Using A_6, R_7 and MM rule:

R_8: $\mathrm{SN}_k| \equiv \mathrm{GW}_j| \sim (r_3, r_4, T_3)$

Using A_2, R_8 and NV rule:

R_9: $\mathrm{SN}_k| \equiv \mathrm{GW}_j| \equiv (r_3, r_4, T_3)$

Using A_2, R_8 and J rule, FC rule:

R_{10}: $\mathrm{SN}_k| \equiv (r_3, r_4, T_3)$

Using R_{10} and B rule:

R_{11}: $\mathrm{SN}_k| \equiv r_4, \mathrm{SN}_k| \equiv r_3$

Using A_3, R_{11} and SK rule:

R_{12}: $\mathrm{SN}_k| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{SN}_k$ (Goal 3).

Using A_3, R_{12} and NV rule:

R_{13}: $\mathrm{SN}_k| \equiv \mathrm{GW}_j| \equiv \mathrm{GW}_j \overset{\mathrm{SK}_i}{\leftrightarrow} \mathrm{SN}_k$ (Goal 4).

(iii) Message 3: $\mathrm{SN}_k \longrightarrow \mathrm{GW}_j$: $\langle B_1, B_2 \rangle$

Using $P \triangleleft X$ rule:

R_{14}: $GW_j \triangleleft \langle \langle B_1 \colon (T_4, r_5, S_{sn}, ID_{sn}, T_3^*, SK_i)_{S_{sn}}, B_2 \rangle \rangle$
Using A_5, R_{14} and MM rule:
R_{15}: $GW_j| \equiv SN_k| \sim (T_4, r_5, SK_i)$
Using A_2, R_{15} and J rule, FC rule, NV rule:
R_{16}: $GW_j| \equiv SN_k| \equiv (T_4, r_5, SK_i)$
Using R_{16} and B rule:
R_{17}: $GW_j| \equiv r_5$
Using A_2, R_{17} and SK rule:
R_{18}: $GW_j| \equiv SN_k \overset{SK_i}{\leftrightarrow} GW_j$ (Goal 5).
Using A_2, R_{18} and NV rule:
R_{19}: $GW_j| \equiv SN_k| \equiv SN_k \overset{SK_i}{\leftrightarrow} GW_j$ (Goal 6).

(iv) Message 4:$GW_j \longrightarrow U_i$: $\langle R_4, R_7, R_8 \rangle$
Using $P \triangleleft X$ rule:
R_{20}: $U_i \triangleleft \langle \langle R_4, R_7, R_8 \colon \langle T_5, r_4, r_5 \rangle_{r_3} \rangle \rangle$
Using A_4, R_4, R_{20} and MM rule:
R_{21}: $U_i| \equiv GW_j| \sim (T_5, r_4, r_5)$
Using A_1, R_{21} and FC rule, NV rule:
R_{22}: $U_i| \equiv GW_j| \equiv (T_5, r_4, r_5)$
Using A_{11}, R_{22}, B rule and J rule:
R_{23}: $U_i| \equiv r_4$
Using A_1, R_{23} and SK rule:
R_{24}: $U_i| \equiv GW_j \overset{SK_i}{\leftrightarrow} U_i$ (Goal 7).
Using A_1, R_{24} and NV rule:
R_{25}: $U_i| \equiv GW_j| \equiv GW_j \overset{SK_i}{\leftrightarrow} U_i$ (Goal 8).

The above BAN logic discussion clearly proves the effectiveness and feasibility of the mutual authentication and session key protocol among user U_i, gateway node GW_j, and sensor device node SN_k.

6. Security Analysis and Discussion

6.1. Security Analysis. In this section, we mainly discuss the security issues to prove that our protocol is secure for all related security attacks.

6.1.1. Replay Attack. Assuming that the device authentication protocol maintains a global clock to synchronize timestamps against clock synchronization, we can verify whether it can effectively resist replay attacks and work smoothly or not. Affected by replay attack, the performance of the system will decline dramatically. Attackers usually capture the previously transmitted messages by the sender entity and resend them to the receiver entity to prove that the message was sent from the legitimate sender entity. Because the system timestamp is used in the protocol and the transmission delay time ΔT will be checked, the protocol always rejects the replay messages captured by the attacker due to the invalid transmission delay time. In the protocol, new random numbers are also used to identify duplicate messages. Therefore, the protocol proposed in this paper is resistant to replay attacks.

6.1.2. User Impersonation Attack. According to the attacker's ability, the attacker can eavesdrop all the transmitted messages through the public channel during the execution of the protocol. The attacker can modify the bugged message and retransmit it to the user in order to impersonate a valid user. The following will prove that the protocol in this paper provides strong security protection against user simulated attacks.

We suppose that the attacker eavesdrops on the message $\{ID_{sn}, F_2, F_3\}$ and tries to generate another valid message, which will be authenticated by the gateway. In order to generate a forged message, the attacker must calculate the following valid parameters:

$$\begin{aligned} F_2 &= h\left(T_2 \| r_3 \| F_1 \| ID_g\right), \\ F_3 &= \left(r_3 \| T_2\right) \oplus F_1. \end{aligned} \tag{21}$$

However, the attacker could not calculate the effective $F_1 = R_3 \oplus h(HPW_i \| T_1)$, where $HPW_i = h(r_1 \oplus PW_i)$ as PW_i and r_1 are unknown to the attacker. In addition, it is not feasible to simulate and guess all unknown constraints in polynomial time. As a result, attackers cannot generate or guess other valid messages in polynomial time.

6.1.3. Offline User Identity and Password Guessing Attacks. Assuming that most users use simple ID_i and PW_i for identity recognition, it is easy to guess ID_i and PW_i in polynomial time. However, during the execution of the protocol in this paper, the user's ID_i and PW_i are protected by an irreversible one-way hash function. Therefore, the attacker cannot extract user information $\{ID_i, PW_i\}$. An attacker may try to extract multiple parameters such as $R_2, R_3, F_2, F_3, R_4, R_5, B_1$, and B_2 from the offline state of the user and then guess and verify user's ID_i and PW_i. All these parameters are known to the attacker as follows.

The attacker finds the constraint parameters F_2 and F_3 of the smart card. The constraint parameters F_2 and F_3 of the smart card are defined as

$$\begin{aligned} F_2 &= h\left(T_2 \| r_3 \| F_1 \| ID_g\right), \\ F_3 &= \left(r_3 \| T_2\right) \oplus F_1, \end{aligned} \tag{22}$$

where $HPW_i^* = h(r_1^* \oplus PW_i)$.

From these relationships, it can be clearly seen that PW_i is protected by an irreversible one-way function, and an attacker cannot extract ID_i, PW_i, r_1^*, and S_g. If an attacker tries to guess the constraint parameters, he must guess all unknown values to verify whether the guessed value is not feasible in polynomial time. If the identity, password, and random number are all N characters and the key of the gateway S_g is M characters, then the probability of guessing the parameters at the same time is about $(1/2^{12N+M})$[26].

6.1.4. Sensor Device Node Simulated Attack. According to our assumption, an attacker can intercept messages during the execution of the protocol $\{B_1 B_2\}$. After intercepting this message, the attacker attempts to generate another valid message that will be verified by the gateway node GW_j,

where $B_1 = h(T_4 \| r_5 \| S_{sn} \| ID_{sn} \| T_3 \| SK_i)$, $B_2 = h(r_5 \| T_4) \oplus r_4^*$. However, an attacker cannot calculate effective intercepted messages without knowing the valid SK_i and r_5, and these messages are protected by the one-way hash function. Therefore, the attacker cannot generate valid other messages. Therefore, our protocol can resist simulated attacks on sensor nodes.

6.1.5. Gateway Node Simulation Attack. In the proposed protocol, the gateway node sends $\{ID_{sn}, R_4, R_5, R_6\}$ and $\{R_4, R_7, R_8\}$ to the sensor and the user. Using these messages, both the sensor node and the user can verify the legitimacy of the gateway node. It is now assumed that an attacker can intercept these two messages.

(i) Case 1: if the attacker intercepts the message between GW_j and SN_k, namely, $\{ID_{sn}, R_4, R_5, R_6\}$, through the public channel, where $R_4 = h(ID_{sn} \| R_1 \| S_{sn} \| r_4 \| T_3)$, $R_5 = (r_3^* \| T_3 \| r_4) \oplus S_{sn}$, and $R_6 = R_1 \oplus h(ID_{sn} \| h(r4) \| r_3^*)$, the attacker attempts to generate another message and send it to the sensor node to simulate as a legitimate gateway. However, the calculation of R_4, R_5, and R_6, respectively, depends on the random number r_4. It should be noted that due to the irreversible properties of the one-way hash function, an attacker cannot extract this value. Since S_{sn} is a shared key parameter between the gateway node and the sensor device node, an attacker cannot guess it in polynomial time.

(ii) Case 2: if the attacker intercepts the message between GW_j and U_i through the public channel, that is, $\{R_4, R_7, R_8\}$, where $R_7 = h(SK_i \| R_1 \| r_4 \| T_5 \| R_4)$ and $R_8 = (r_5^* \| r_4 \| T_5 \|) \oplus r_3^*$, then the attacker tries to generate another message and transmit it to the user U_i to impersonate legal gateway. However, the calculation of R_7 and R_8 depends on R_1 and r_4. Also, it should be noted that the attacker cannot extract the values generated due to the irreversibility of the one-way hash function, and these values cannot be guessed in polynomial time. In addition, the user terminated the connection due to an invalid message. Therefore, if an attacker initiates a gateway simulation attack, it may be captured.

6.1.6. Long-Term Key Security. The authentication protocol uses several keys, such as S_{BC} (private key of BC), S_g (the private key of gateway node), and S_{sn} (the shared key between gateway node and sensor device node). It is worth noting that in the setup stage, $S_g = h(ID_g \| S_{BC})$ and $S_{sn} = h(ID_{sn} \| S_{BC})$. Because the keys are protected by a one-way hash function, attackers cannot retrieve them. Similarly, the key of the gateway node S_g cannot be retrieved. Therefore, in the protocol of this chapter, all keys are highly protected.

6.1.7. Mutual Authentication. In this protocol, all entities will authenticate each other to verify the validity of their identities before the actual information sharing or retrieval occurs. During the implementation of the protocol, the gateway node first authenticates the user's identity according to the received login message $\{ID_{sn}, F_2, F_3\}$, and then the sensor node uses the message $\{ID_{sn}, R_4, R_5, R_6\}$ received from the gateway device node to verify the identity of the gateway node. Similarly, the gateway uses the message $\{B_1, B_2\}$ to authenticate the sensor node, and the user uses the message $\{R_4, R_7, R_8\}$ to authenticate the gateway node. As a result, all participants involved use their own messages to authenticate with each other.

6.1.8. Perfect Forward Confidentiality. This protocol provides perfect forward secrecy, which means that even if one of the long-term keys is disclosed, the session key will not be disclosed. For example, we suppose that the long-term key of the gateway node is disclosed to the attacker in some way. The attacker then attempts to calculate the session key used in the protocol. Even if the secret key is known, the attacker cannot calculate the random number used in the protocol and will not know the shared secret key between the gateway node and the sensor device node. Because the session key depends on a random number, the attacker cannot calculate it. If we assume that the session key used in the protocol has been destroyed by the attacker, the attacker will try to calculate the previous session key. The attacker was unable to calculate the previous session key because he could not extract any confidential information from the compromised session key $SK_i = h(R_1^* \| r_3^{**} \| r_4^* \| r_5)$. Therefore, our protocol has perfect forward confidentiality.

6.1.9. Effective Authentication. In order to prolong the service life of sensor devices, we hope to reduce the computation cost of sensor and the number of bits it must transmit. In this paper, we also prove that the computation cost of authentication messages of sensor nodes is very low as shown in Table 2. The bits of transmitted message are also less as shown in Table 3. In addition, the sensor node first checks the legitimacy of the user and gateway node by comparing R_4^* with the received R_4 and then performs further calculation and communication processes, which prevent the attacker from repeatedly sending false messages to harm the sensor device node. If the sensor device node participates in the calculation and communication messages as the response of the false message, it will cause unnecessary battery consumption of the sensor device node. Therefore, the protocol provides effective authentication.

6.1.10. Valid Key Changes. When a user suspects that his password has been leaked, the registered user will change their password. Therefore, the protocol proposed in this paper needs the password change function. Registered users can change their passwords in the agreement. Users do not need any support from the gateway node or the registry during the password change process, which reduces the load on the channel and also can resist the DoS attack. In addition, in order to reduce the computation cost, the system

Table 2: Computation cost.

	Shi [13]	Choi [14]	Xue [17]	Kumar [19]	Our protocol
U_i	7 H + 3 ECC	12 H + 3 ECC	10 H	8 H	8 H
GW_i	5 H + 1 ECC	5 H + 1 ECC	14 H	9 H	7 H
SN_k	4 H + 2 ECC	7 H + 2 ECC	6 H	5 H	6 H
Total	16 H + 6 ECC	24 H + 6 ECC	30 H	22 H	21 H
Execution time	0.386 s	0.390 s	0.015 s	0.011 s	0.0105 s

Table 3: Communication cost.

	Shi [13]	Choi [14]	Xue [17]	Kumar [19]	Our protocol
Total communication cost (bits)	2656	3040	2144	1792	1664
Communication cost of sensor devices (bits)	2656	3040	1440	800	832
Sensor device cost (%)	100	100	67.16	44.64	50

Table 4: Comparison of security requirements.

	Shi [13]	Choi [14]	Xue [17]	Kumar [19]	Our protocol
User anonymity	×	×	×	√	√
Resist smart card theft attack	×	×	×	√	√
Resist session key attack	×	√	√	√	√
Resist sensor energy consumption	×	√	√	×	√
Resist internal attacks	√	√	×	√	√
Resist offline password guessing	√	√	×	√	√
Resist replay attacks	√	√	√	√	√
Resistance to man in the middle attacks	√	√	√	√	√
Resist user counterfeiting attack	√	√	√	√	√
Mutual authentication	√	√	√	√	√
Key agreement between user and sensor	√	√	√	√	√

will verify the correctness of the personal information such as the identity and password before calculating the new value with the new password. Therefore, the password change stage is effective and practical.

6.2. Performance Evaluation

6.2.1. Comparison of Security Performance. We compare the security performance of the proposed scheme with the protocols Shi [13], Choi [14], Xue [17], and Kumar [19]. In Table 4, it can be seen that the protocols of Shi [13] are vulnerable to several attacks, such as smart card theft and session key attack. In addition, the protocol of Shi is easy to expose the anonymity of users. From this table, it is clear that our proposed protocol provides strong security protection against related attacks, including user anonymity, password guessing attack, user sensor simulation attack, internal attack, smart card theft attack, and session key disclosure attack. Our improved protocol can provide more adequate security protection, because it can meet all the security requirements. Our protocol is the only one that can resist all known attacks and provide all required security functions.

6.2.2. Comparison of Computation Cost. In Table 2, H, S, and ECC represent the execution time of hash function, symmetric encryption/decryption, and ECC dot product, respectively. The computation amount of user registration is one-time. Therefore, we do not pay attention to this time. Due to the resource constrained nature of gateway nodes and sensor nodes, we find that Shi et al. [13] used elliptic curve points to calculate authentication messages, and our protocol mainly uses encryption one-way hash function h, XOR"$\oplus$", and connection"$\|$" operations to provide security identity authentication. Because the cost of exclusive or and concatenation is negligible, we only consider the cost of the hash function. In addition, the computational complexity of Li [27] can be roughly expressed as $(\mathrm{ECC} > S > h)$. As described in Li [27], we assume that one-way hash function (H), symmetric key encryption/decryption algorithm, and ECC of scalar point of elliptic curve need 0.0005, 0.0087, and 0.063075 seconds respectively. From Table 2, we find that the computing cost of our protocol is $(8H + 7H + 6H) = 21 \times 0.0005 = 0.0105$ s, while the computing cost of sensor device node is $6H = 6 \times 0.0005 = 0.003$ s. That is, in our protocol, the computing cost of sensor node is 28% of the total computing cost. Table 2 shows that the computation cost of our protocol is lower than the protocols Shi [13], Choi [14], Xue [17], and Kumar [19]. Therefore, our protocol is suitable for the security authentication of sensor nodes in the medical cyber-physical systems, which can save resources and increase service life.

6.2.3. Comparison of Communication Cost. As shown in Table 3, we compare the communication overhead in this paper with the methods discussed in Shi [13], Choi [14], Xue [17], and Kumar [19]. Communication overhead is the total

number of bits required for transmission during the login and authentication stages. Now, we assume that the participants' identities, random numbers, and timestamps are 32 bits, the results of AES are 512 bits, the ECC points are 320 bits, and the message digests of SHA1 are 160 bits. It can be seen from the results that the total communication cost of our scheme is the lowest, and the cost of sensor devices is low, which can keep the sensor devices active for a long time.

7. Conclusions and Future Works

In this paper, a security authentication model of medical cyber-physical systems based on blockchain is proposed, and the process of data collection and transmission is described in detail. Then, we propose an authentication scheme of sensor devices. The process includes system initialization, user registration, user login, security authentication and key negotiation, password change, and adding sensor nodes. Finally, we analyze the availability and security of the proposed scheme.

Compared with the traditional device identity authentication scheme, this scheme has the following advantages: first, taking the blockchain node as the authentication third party can solve the untrustworthy problem of the third party and also can resist the attacker's attack on the third party's data center to prevent data leakage. Second, the authentication scheme can be adapted to device nodes with different computing, transmission, and storage capacities. At the same time, it can also save the energy consumption of device nodes and increase the service life. Third, the device nodes can be added dynamically. Because the transaction speed of alliance chain is fast, each node has its own private key, the transaction cost is not high, and it cannot be tampered with. However, due to the multiple data types and high complexity of data transactions in the device nodes of the medical cyber-physical systems, and with the needs of the use process, the device nodes need to be added to collect new data. The medical institutions can be connected with the alliance chain, which can provide an innovative way for the medical cyber-physical systems architecture and make the system efficient, safe, and traceable.

Although our scheme has made some progress in the research of device identity authentication, there are still some shortcomings of our work. The following problems need further research:

(1) A new security authentication protocol for sensor devices in the medical cyber-physical systems is proposed in this paper, which is used to authenticate legitimate users and sensor devices. The protocol realizes the security requirements of authentication process at a lower cost and saves the cost of devices life. Mutual authentication and key establishment can also be completed. In the future, we hope that the scheme of device security authentication can be extended to other application fields to complete the device security authentication with the blockchain technology.

(2) The security authentication scheme proposed in this paper is based on the blockchain technology. However, we only analyze the security and effectiveness of the scheme in theory and realizes the simple construction of medical alliance chain. In further, we can use the Hyperledger Fabric to complete more rigorous experimental simulation [28]. The open platform of Hyperledger Fabric, which is open-source and free of charge, provides a modular and scalable architecture and can be used in various industries from banking and health care to supply chain.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the colleagues and students in Anhui Provincial Key Laboratory of Network and Information Security. The authors thank the National Natural Science Foundation of China under grant no. 61972438 and Key Research and Development Projects in Anhui Province under grant no. 202004a05020002 for supporting this research.

References

[1] F. Junior, D. Schneider, and R. Adler, "Dynamic risk management for cooperative autonomous medical cyber-physical systems"" in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, pp. 216–231, Turku, Finland, September 2019.

[2] D. He and S. Zeadally, "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72–83, Feb. 2015.

[3] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[4] A. Alhayajneh, A. Baccarini, G. Weiss et al., "Biometric authentication and verification for medical cyber physical systems," *Electronics*, vol. 7, no. 12, 436 pages, 2018.

[5] S. R. Moosavi, T. N. Gia, E. Nigussie et al., "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2016.

[6] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 1, pp. 53–61, 2017.

[7] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: lightweight three-factor Authentication, access control and ownership transfer scheme for E-health systems in IoT," *Future Generation Computer Systems*, vol. 96, pp. 410–424, 2019.

[8] Z. Ma, J. Meng, J. Wang et al., "Blockchain-based decentralized authentication modeling scheme in edge and IoT

environment"" *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116–2123, 2021.

[9] Y. Zhang, Y. Qian, D. Wu, M. S. Hossain, A. Ghoneim, and M. Chen, "Emotion-aware multimedia systems security," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 617–624, 2019.

[10] Y. Zhang, R. Gravina, H. Lu, M. Villari, and G. Fortino, "PEA: parallel electrocardiogram-based authentication for smart healthcare systems," *Journal of Network and Computer Applications*, vol. 117, pp. 10–16, 2018.

[11] S. H. Islam and G. P. Biswas, "Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys," *Wireless Personal Communications*, vol. 82, no. 4, pp. 2727–2750, 2015.

[12] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health information exchange," *Computers & Security*, vol. 67, pp. 73–88, 2017.

[13] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography"" *International Journal of Distributed Sensor Networks*, Article ID 730831, 2013.

[14] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.

[15] F. Chen, Y. Luo, J. Zhang et al., "An infrastructure framework for privacy protection of community medical internet of things," *World Wide Web*, vol. 21, no. 1, pp. 33–57, 2018.

[16] H. Shu, P. Qi, Y. Huang et al., "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems"" *Sensors*, vol. 20, no. 5, 1521 pages, 2020.

[17] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[18] Z. Liu, C. Guo, and B. Wang, "A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT," *IEEE Access*, vol. 8, pp. 195914–195928, 2020.

[19] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 2, pp. 641–660, 2019.

[20] R. Amin and G. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS"" *Journal of Medical Systems*, vol. 39, no. 3, 33 pages, 2015.

[21] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[22] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, pp. 192177–192191, 2020.

[23] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[24] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks*, vol. 104, pp. 137–154, 2016.

[25] P. Kumar and H. Lee, "Cryptanalysis on two user authentication protocols using smart card or wireless sensor networks," in *Proceedings of the IEEE Wireless Advanced (WIAd)*, pp. 241–245, London, UK, 2011.

[26] B. Vaidya, D. Makrakis, and H. Mouftah, "Two-factor mutual authentication with key agreement in wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 2, pp. 171–183, 2016.

[27] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Computer Communications*, vol. 35, no. 2, pp. 188–195, 2012.

[28] X. Cheng, F. Chen, D. Xie et al., "Design of a secure medical data sharing scheme based on blockchain"" *Journal of Medical System*, vol. 44, no. 2, 52 pages, 2020.