A Secure Framework for Data Sharing in Private Blockchain-Based WBANs

LIJUN XIAO¹,², DEZHI HAN², (Member, IEEE), XIANGWEI MENG³, WEI LIAO⁴, AND KUAN-CHING LI⁵, (Senior Member, IEEE)

¹Big Data Development and Research Center, Guangzhou College of Technology and Business, Guangzhou 511442, China
²School of Information Engineering, Shanghai Maritime University, Shanghai 411201, China
³School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 425100, China
⁴College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
⁵Department of Computer Science and Information Engineering, Providence University, Taichung 43301, Taiwan

Corresponding author: Kuan-Ching Li (kuancli@pu.edu.tw)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672338 and Grant 61873160, and in part by the Scientific Research Project of the Guangzhou College of Technology and Business under Grant KA202031.

ABSTRACT With the development of sensor devices, wireless sensor networks have been widely used, and Wireless Body Area Networks (WBANs) are relatively common application scenarios in wireless sensor networks. The wearable device is used to collect physiological data of the human body, and the server device is adopted to store physiological data of the human body. The openness of the network environment and network devices’ dynamic nature make WBANs vulnerable to security threats from attackers. The centralized two-hop architecture contains only one hub node, and the data stored in the hub node may be tampered with by attackers. Once attackers occupy the node, the entire network will be paralyzed. To tackle such an issue, it is proposed in this article a model in WBANs architecture based on Blockchain technology, where the authentication protocol and blind signature protocol between nodes are designed in the new WBANs model, making the Blockchain data transmission system in a wireless network environment secure and reliable. Experimental results show that the proposed method is promising and shows higher levels of safety and stability than other methods.

INDEX TERMS WBANs, private blockchain, dynamic, authentication, blind signature.

I. INTRODUCTION

With the development of the mobile Internet, several sensor nodes and server nodes can be connected to form a wireless sensor network. Sensor nodes are responsible for perceiving the environment and collecting data and transmitting the collected data to the server node, whereas the server node is responsible for processing and storing the data sent by the sensor node [1]–[3]. Wireless body area network (WBAN) is a small sensor network composed of sensor nodes worn on the patient’s body for collecting physiological data of the human body. The sensor node will send the collected physiological data to the server node [4], [5]. For such, medical staff can remotely monitor the vital signs of the disabled at home, the elderly, patients recovering from post-surgery, or people with high morbidity to achieve the assessment of the patient’s physical condition. Besides, WBANs can also be used to monitor athletes’ bodies. The coaching staff monitors the changes in athletes’ physiological data during physical training in real-time, prompting athletes to control training intensity [6], [7].

The data is collected, processed, and transmitted by intelligent terminals in a mobile medical environment. After that, it is linked to the user’s physiological characteristics, environmental location, and other private information. The security and privacy protection of these data are bottlenecks for the large-scale promotion of modern medical services. The resource-constrained wearable devices and PDA cannot meet the computationally expensive operations, nor can they provide sufficient local storage space for medical systems.

With the rapid development of various network security technologies, personal medical and copyright data will face the risk of being accessed intentionally or unintentionally by unauthorized personnel [8]. For example, the information system of Anthem (the second-largest medical insurance company in the United States) was hacked in 2015,
WBANs should consider its lightweight characteristics [12].

The stability of the server node and the security of the data stored in the database is the latter. DoS attacks can cause server nodes to fail and cause the entire system to crash. That is, WBANs from different regions face the dilemma of the lack of collaboration in data sharing [13], as also existing WBANs frameworks cannot solve these problems. Therefore, designing a reasonable and adequate WBANs architecture model is a pre-requisite for ensuring network stability, with the application of Blockchain technology to build a cloud server layer of WBANs that can effectively resist DoS attacks [14]. Besides, each server node in WBANs has its jurisdiction. As human body motion sensor nodes establish communication with server nodes in different regions, the network’s dynamic nature is another major feature of WBANs.

As the leading technology to realize mobile medicine, compared with wireless sensor networks, WBANs have the following characteristics: (1) Network dynamics, WBANs sensor nodes can be placed in the body or human body, and the addition and deletion of nodes cannot affect the normal operation of other parts. The network topology changes with human activity patterns, (2) WBANs have strict requirements on the power consumption of nodes. Especially the sensor devices implanted in the body cannot be replaced arbitrarily, they should not generate more energy consumption and maintaining longer running time, and (3) WBANs transmit and process medical data and environmental location data related to the human body, which involves user privacy and requires exceptionally high security.

A. RELATED WORK
Reasonable and adequate WBANs architecture model is an essential pre-requisite for ensuring network security and stability. In 2012, IEEE released the Wireless Body Area Network (WBAN) standardization protocol: IEEE 802.15.6 [15]. In 2018, Li et al. proposed a three-tier mobile medical system and designed a new anonymous mutual authentication scheme [16] as the first layer network composed of sensor nodes and supernodes is used to collect patients’ physiological data, the controller nodes of the second layer network are responsible for the communication between the internal and external nodes of the BAN, and the third layer network is used to store the patient’s physiological data.

The network model using Blockchain technology has a better ability to prevent data from being tampered, so thus, researchers have widely used in many fields based on the characteristics of Blockchain in recent years. In order to solve the challenge where attackers can easily leak patient data stored on cloud servers, a data-sharing framework based on Blockchain is proposed [17]. By using only authenticated users to access the Blockchain, the scheme has robust scalability in the structure of the block, so the reliability of the system is improved. Furthermore, the system’s transaction data volume in the unit time period was tested. Zang et al. proposed a Blockchain-based secure and privacy-preserving PHI sharing (BSPP) scheme for improving the diagnosis of
II. BACKGROUND

WBANs play an essential role in the field of medical monitoring. Doctors can monitor the physiological data of patients wearing sensor nodes in real-time. The sensor node will send the data to the hub node after detecting the abnormal physiological data of the patient, and the hub node will store the data for the user to use. The traditional WBANs network model is a two-hop centralized architecture, as depicted in Figure 2. There are three types of nodes in the network: sensor node, supernode, and hub node. Among them, the sensor node and supernode belong to the first layer network, also called Intra-BAN. The sensor node is used to collect physiological data of patients. A few parameters are stored in its memory for mutual authentication and key agreement with the hub node.

In order to ensure the long-term operation of the device, the sensor node can only use XOR operation and a one-way hash function that consumes less energy. Generally speaking, a sensor node with a communication radius of 2m cannot send data directly to the hub node [22]. Therefore, the sensor node needs a mobile device that is not limited by resources and is used to receive, store, and manage the data collected by the sensor node. In the centralized double-hop network model, a single server device is prone to a single point of failure when it encounters an attack, which is not conducive to the system’s stable operation. Therefore, the network model is suitable for small WBANs.

Blockchain belongs to a distributed database system. Many nodes in the network together maintain a linked list of connected blocks, and systems use cryptography to add new blocks and maintain the security of the Blockchain [23]. An attacker modifying the data of a particular block on the Blockchain will cause the hash value of the block to change, which in turn causes the block to fail to connect to the next block. Therefore, a distributed database built using Blockchain technology has a better ability to prevent data from being tampered with. All nodes in the system use a unified smart contract to maintain the Blockchain’s security and generate new blocks.

The consensus mechanism is an algorithm for adding new blocks to nodes in the Blockchain system. In the public Blockchain, the mainstream consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) [24]. Each node of the PoW consensus mechanism obtains the right to generate heart blocks through computing power competition. In order to reduce the consumption of resources by the PoW consensus mechanism, the researchers proposed a PoS consensus mechanism. The PoS consensus mechanism does not use the computing power of nodes as the only standard for competing to generate new block rights. The number and duration of nodes holding coins are used as equity. The system will give different nodes the difficulty of generating new blocks according to the value of the node’s equity. Therefore, the node with the higher value of equity has a better chance of generating new blocks. DPoS is further optimized based on PoS, changing the competition of all nodes in the system to the competition of some nodes. Only the nodes on the campaign have the power to generate

FIGURE 2. A network model for centralized two-hop WBANs.
new blocks. Each node on the campaign cyclically generates new blocks. DPoS is weak in decentralization, but it can effectively reduce the resources consumed by generating new blocks. PoS and DPoS have many similarities with PoS in the way of adding new blocks.

### III. BLOCKCHAIN-BASED WBANs

The use of Blockchain technology to build a double-hop distributed architecture of WBANs is shown, as depicted in Figure 3. The architecture is composed of three layers: perception layer, cloud server layer, and Beyond-WBANs. The perception layer, composed of a sensor node and supernode, is responsible for collecting physiological data of the patient’s body and sending the physiological data to the cloud server layer. The sensor node worn by the patient’s body is limited by energy consumption and cannot directly send data to the hub node in the cloud server layer, and thus, the supernode with strong communication capability needs to forward the data collected by the sensor node. The supernode belongs to the relay node does not store and calculate the forwarded data, can communicate with the local hub node as well as communicate with hub nodes in other regions to achieve cross-region access of sensor nodes and supernode.

Many hub nodes utilize Blockchain technology to build cloud server layers of WBANs. Each hub node has its jurisdiction to manage all sensor nodes and supernodes in the area. Hub node has reliable computing power, communication capacity, and storage capacity, and can effectively achieve mutual authentication and key negotiation with the sensor node. After the hub node receives the data from the sensor node, it will be stored in the database in the form of a private Blockchain. The data is divided into node registration data and patient physiological data. Node registration data is used for mutual authentication and key agreement between the hub node and the sensor node, where users can access patient physiological data that include doctors, nurses, and patients. They can access the patient’s physiological data by accessing any hub node.

The security analysis of the scheme proposed is based on the threat model, and the characteristics of the attacker are as follows. 1) The system administrator has the highest privilege of the system, which can be trusted entirely and can not be impersonated by the attacker. 2) In the phase of authentication and key agreement, The attacker can modify, intercept, and replay the data transmitted in the public channel. 3) The attacker can access the database of the hub node and obtain the data recorded on the Blockchain. 4) In the phase of network node consensus, the data transmitted between hub nodes cannot be intercepted by attackers, because in the Byzantine hypothesis, if the data transmitted between entities is intercepted, then the Byzantine hypothesis has no solution.

### A. AUTHENTICATION AND KEY AGREEMENT

The notations used to describe the sensor node key agreement are given in Table 1. The data sent by the sensor node to the hub node through a supernode is in the public channel, so the authentication and key agreement between nodes are needed before the session is established. The lightweight authentication protocol in WBANs usually uses XOR operation and one-way hash function. The protocol is divided into three phases: The initialization phase, registration phase, and authentication phase [25]. The system administrator gives each hub node the same master key \( k_{HN} \) in the initialization phase for the authentication of the hub node and sensor node during the registration phase.

![Figure 3. The architecture of Blockchain-based WBANs.](image-url)
First, the system administrator gives the supernode unique identity \( id_{SN} \) and stores it in its memory. After that, the sensor node generates registration data, which contains the unique and secret identity \( id_{SN} \) and the parameter \( \alpha \) used for authentication, and it is stored in the memory of the sensor node. The system administrator uses the sensor node’s key \( k_N \) to encrypt the supernode’s identity identifier \( id_{SN} \) and the sensor node’s registration data \( (id_N, \alpha) \) to retrieve the cipher-text \( E_{k_N}(id_{SN}, id_N, \alpha) \). The Hub node packs the ciphertext \( E_{k_N}(id_{SN}, id_N, \alpha) \) of all registered data in the area per unit time into a data package and stores it in the form of a Blockchain in the database of the hub node, which process is summarized in “Algorithm 1”.

In the authentication phase, the sensor node performs mutual authentication and key agreement with the hub node through the supernode. The sensor node generates the time stamp \( t_N \) and the authentication parameter \( H_1 \), and sends the data tuple \( (H_1, t_N) \) to the supernode. After receiving the data tuple \( (H_1, t_N) \), the supernode adds its identity \( id_{SN} \) to the data tuple, and sends the tuple \( (id_{SN}, H_1, t_N) \) to the hub node. After the hub node receives the data, it generates authentication parameters \( H_1^* \). Checks \( H_1^* = H_1 \), if they are not equal, the authentication fails. If they are equal, the authentication is successful. The Hub node generates a timestamp \( t_{HN} \), authentication parameter \( H_2 \), and session key \( k_S \). Store the session key \( k_S \) in memory for encrypted transmission of data. The Hub node sends data tuple \( (id_{SN}, H_2, t_{HN}) \) to the supernode. Supernode forwards the data tuple \( (H_2, t_{HN}) \) to the sensor node. After receiving the data, the Sensor node generates the identity authentication parameter \( H_2^* \). Checks \( H_2^* = H_2 \), if they are not equal, the authentication fails, and the session key \( k_S \) is generated and stored in memory with the process summarized in “Algorithm 2”, if otherwise.

**Algorithm 2 Authentication Phase**

**Input:** \( N \) authentication and key agreement request, \( HN \) in the WBANs

**Output:** Reach the session key between \( N \) and \( HN \)

1. for each \( n \in N \) do
2. \( t_N \leftarrow \) generate timestamp;
3. \( H_1 \leftarrow \) generate authentication parameter;
4. \( N \rightarrow SN, \) send data \( (id_N, H_1, t_N) \);
5. end for
6. for each \( n \in SN \) do
7. \( N \rightarrow SN, \) receive data \( (id_N, H_1, t_N) \);
8. \( SN \rightarrow HN, \) send data \( (id_{SN}, id_N, H_1, t_N) \);
9. end for
10. for each \( n \in HN \) do
11. \( N \rightarrow SN, \) receive data \( (id_{SN}, id_N, H_1, t_N) \);
12. \( H_1^* \leftarrow \) generate authentication parameter;
13. If \( (H_1^* \neq H_1) \) then
14. check fails;
15. else
16. \( t_{HN} \leftarrow \) generate timestamp;
17. \( H_2 \leftarrow \) generate SN authentication parameter;
18. \( k_S \leftarrow \) generate session key;
19. store \( k_S \) in \( HN \)’s memory;
20. \( HN \rightarrow SN, \) send data \( (id_{SN}, H_2, t_{HN}) \);
21. end if
22. end for
23. for each \( n \in SN \) do
24. \( HN \rightarrow SN, \) receive data \( (id_{SN}, H_2, t_{HN}) \);
25. \( SN \rightarrow N, \) send data \( (H_2, t_{HN}) \);
26. end for
27. for each \( n \in N \) do
28. \( SN \rightarrow N, \) receive data \( (H_2, t_{HN}) \);
29. \( H_2^* \leftarrow \) generate authentication parameter;
30. If \( (H_2^* \neq H_2) \) then
31. check fails;
32. else
33. \( k_S \leftarrow \) generate session key;
34. store \( k_S \) in \( N \)’s memory;
35. end if
36. end for

**B. BLOCKCHAIN FOR STORING REGISTRATION DATA AND PHYSIOLOGICAL DATA**

The public Blockchain is suitable for the network environment with high openness. The network nodes involved in maintenance include both honest and malicious nodes. The honest node will generate new blocks according to the smart contract’s provisions, though the malicious node will try to forge the data recorded in the new block. To encourage nodes in the network to generate new blocks, the public Blockchain needs to design a reasonable reward mechanism to lure more nodes to participate in it.

The WBANs network model designed in this proposed work saves sensor nodes registration data and patient physiological data in the form of a private blockchain. The advantages of using private Blockchain are to facilitate the management of network nodes. The hub nodes at the cloud server layer can effectively complete the maintenance of the Blockchain and the generation of new blocks. The participation of more external nodes has no more practical significance for maintaining the Blockchain’s security in WBANs. Therefore, all hub nodes in the cloud server layer establish two sets of private blockchains. The first set of private Blockchain records the registration data of the sensor node. The second set of private Blockchain records the patient’s physiological data. Each set of private Blockchain consists of two private Blockchains, as shown in Figure 4.

One private Blockchain is a data private Blockchain, and the other private Blockchain is authentication private Blockchain. The data private Blockchain is used to record the data to be recorded by the group’s private Blockchain. The authentication private Blockchain is used to verify whether the data recorded by the data private Blockchain is complete. The structure of each private Blockchain is the same, consisting of a block header and block body. The block header contains the hash value of the previous block to generate a fast timestamp in this area. The hash value of the previous block...
is used to connect the current block to ensure that the attacker does not easily tamper the Blockchain. The timestamp is used to record the time when the current block is generated. The data to be recorded in a unit time in the block recording system. The maintenance of the private Blockchain and the generation of new blocks are all the hub node’s responsibility, so no reward mechanism is used. The consensus mechanism in this article does not use the PoW or PoS consensus mechanism commonly used in public Blockchain. A simple, safe, and active private consensus mechanism is adopted.

The private consensus mechanism is designed for the characteristics of the authentication of private Blockchain and the data private Blockchain. The private consensus mechanism only needs relatively low calculation overhead and communication overhead to have network nodes reaching a consensus on the same transaction. The network node is acted by the hub node of the cloud server layer, and the system administrator grants its authority.

The private consensus mechanism does not obtain the right to generate blocks by competing with network nodes’ computing power, so thus, each hub node can produce new blocks, acting as a network node that maintains the Blockchain’s security and stability.

1) PRIVATE BLOCKCHAIN FOR RECORDING REGISTRATION DATA
A set of private Blockchains storing registration data consists of two private Blockchains. The one private Blockchain is the data private Blockchain, and the other private Blockchain is the authentication private Blockchain. The entire private Blockchain is used to record the registration data of the nodes.

To facilitate the management of the private Blockchain, each block records a set of registration data of the same personal wearable device. That is, registration data of a supernode and the m sensor nodes it manages. When the server node performs authentication and key agreement with the sensor node, it only needs to access one block to obtain the authentication data. There are multiple sets of supernodes and sensor nodes registering in the same time period, so thus, multiple blocks are generated. Blocks generated in unit time are joined into block groups using a one-way hash function. There is only one block group per unit time. The hash function value of a block group is the data that the authentication private Blockchain needs to record.

Authentication private Blockchain is used to verify consistency when each node generates a new block and to verify that the data recorded by the entire private Blockchain is complete. The data structure of the entire private Blockchain and the certified private Blockchain is the same, consisting of a block header and block body. The block header contains the block ID, the block’s size, the hash value of the previous block, and the time stamp that generated the block. Block bodies are used to record the data. Suppose there are n hub nodes in the network, and the computing power, storage capacity, and communication capacity of each hub node are the same. First of all, all hub nodes generate a new block at a unified time, and the block body of the new block records the registration data of a supernode and the sensor nodes it manages in a unit time. Next, the hub node uses a one-way hash function to get the hash function value for the new block. Due to each hub node’s computing power the same, it can generate the same new block and new block hash value at the same time. The private consensus mechanism does not require the hub node to calculate a random number when generating a new block. Therefore, the hub node generates a new block very quickly.

Again, the one-way hash function is used to connect the new blocks generated per unit time into the block group. The hub node calculates the hash function value of the block group and generates a new block of the authentication private Blockchain for recording the hash function value of the block group. Finally, each hub node packages the generated block group of the data private Blockchain and the block of the authentication private Blockchain into data packets, which are sent to other hub nodes in the network. Other hub nodes will receive n−1 data packets. The hub node compares the block of the authentication private Blockchain generated by itself with the blocks of the received authentication private Blockchain. If the block generated by the hub node is the same as the block received by more than 2/3, the block group of the data private Blockchain generated by the hub node is added to the data private Blockchain, and the block of the authentication private Blockchain is added to the authentication private Blockchain. If they are different, the verification process fails, and the hub node needs to regenerate a new block and send the data packet to other hub nodes in the network again. This process completes the addition of data to the data private Blockchain and the authentication private Blockchain.

The private consensus mechanism follows the principle of majority node effectiveness. New block generated by most nodes and private Blockchains stored by most nodes are legal. The sensor node’s key encrypts the registration data stored on the data private Blockchain. Even if the attacker steals the data private Blockchain, the plain text cannot be obtained. The block structure that stores the registration data of the sensor node and supernode in the data private Blockchain is depicted in Figure 5.
2) PRIVATE BLOCKCHAIN FOR RECORDING PHYSIOLOGICAL DATA
To save the cost of local server management and data storage, the medical system stores the patient’s physiological data on a third-party server. Though, such a structure is also prone to single points of failure so that users cannot access the data. To this end, this article stores the user’s data in the hub node’s database in a private Blockchain. Even if a single hub node fails, users can access other hub node databases across regions. The structure and consensus mechanism of a set of private Blockchains that record patient physiological data are the same as the set of private Blockchains that record registration data, with the process summarized in “Algorithm 3”. The hub node receives patient physiological data collected by the sensor node and uses proxy re-encryption technology to convert the ciphertext to a cipher that users can decrypt. After that, the private consensus mechanism is used to add the ciphertext to the data private Blockchain. Users can obtain the patient’s physiological data by accessing the hub node’s database.

C. BLOCKCHAIN-BASED BLIND SIGNATURE PROTOCOL
1) PROTOCOL MODEL
This section proposes a blind signature protocol based on Blockchain, which can verify the authenticity of Blockchain’s Signer nodes and Collector nodes as well as effectively reduce the cost burden of nodes in key management. The protocol model consists of three parts, namely public key generator (PKG), Signer node and Collector node. PKG is a semi-trusted third-party center, mainly used for node registration and distribution of some keys. Both the Signer node and the Collector node are nodes in the Blockchain. The Signer node is responsible for signing messages. Collector node is mainly used to Collect and broadcast WBAN information transmitted from supernodes. Only when the signature is valid and the identity of the Collector node is legal, the information collected by the Collector node will be broadcast to other nodes in the Blockchain.

Elliptic curve encryption technology has the characteristics of high security, fast processing speed, small key among others, and is widely used in the fields of identity authentication and digital signature. In this section, the expression of an elliptic curve \( E_p(a, b) \) with finite field \( F_p \) is defined as \( y^2 = x^3 + ax + b \), where \((a, b) \in F_p\), satisfying \(4a^3 + 27b^2 \neq 0\). \( G_q \) is an additive cyclic group with an upper order \( q \) of elliptic curve \( E_p(a, b) \), \( P \) is a generator of \( G_q \), satisfying \( qP = O_\infty \), \( O_\infty \) is an infinity point on \( E_p(a, b) \). Assuming \( a, b \in Z_q^* \), the security of ECC technology is mainly due to the following two problems:

1) Elliptic Curve Discrete Logarithm Problem (ECDLP):
Let \( P \) be the generator of \( G_q \), \( Q = aP \), it is difficult for an attacker to calculate the value of \( a \) through \((P, Q)\) in polynomial time.

2) Elliptic curve Computation Diffie-Helman (ECCDH):
Let \( P \) be the generator of \( G_q \). Knowing \( P, aP, bP \), it is difficult for an attacker to calculate the value of \( abP \) in polynomial time.

Blind signature is a unique digital signature technology. In the process of blind signature, the requester generates blind factor information \( r \) and then uses \( r \) to blindly process the information \( m \) and send it to the Signer. Signer sends the message \( m^r \) to the requester after signing. Next, the requester removes the blind factor \( r \) of \( m^r \) to retrieve the signature of the message \( m \). The blind signature technology has the following two characteristics: (1) When the Signer signs the information, the Signer cannot know the content of the information, (2) The signed message is not traceable, and the Signer cannot know when and why the information was signed.

Algorithm 3 Creating and Adding the New Blocks to the Private Blockchains

**Input:** A set of \( HN \) in the cloud server layer, A set of Blockchains \( B \) including \( D_B \) and \( R_B \), The new blocks generated in time \( \Delta t \)

**Output:** The newly created blocks \( d_b_n \) and \( r_b_n \)

1. **Initialize an empty block group** \( G \)
2. **While** transaction time \(<\Delta t\) **do**
3. \( d_b_n \leftarrow \text{create block (record data)}; \)
4. \( \text{block group } G \leftarrow \text{add block } (d_b_n); \)
5. \( t_h_n \leftarrow \text{hash func } (d_b_n); \)
6. \( n+ = 1; \)
7. **end while**
8. \( h \leftarrow \text{hash func } (\sum d_h_n); \)
9. \( r_b_n \leftarrow \text{create block } (h); \)
10. **end for**
11. **broadcast data pack** \((G, r_b_n); \)
12. \((G, r_b_n) \leftarrow \text{verify received packets}; \)
13. **for each** \( h \in HN \) **then**
14. **if** (Successful verification)
15. \( D_B' \leftarrow D_B + G; \)
16. \( R_B' \leftarrow R_B + r_b_n; \)
17. **else**
18. regenerate \( G \) and \( r_b_n; \)
19. **end if**
20. **end for**
2) BLOCKCHAIN-BASED BLIND SIGNATURE PROTOCOL
The blind signature protocol based on Blockchain proposed is composed of 6 stages, namely setup, partial private key extraction, set secret value, set public key, Blind signature generation, and Verification. The symbol description of the protocol is shown in the following Table 2.

1) Setup. PKG selects the additive cyclic group \( G_q \) with generator \( P \), and \( qP = O_\infty \). Then PKG selects a master key \( x_A \in \mathbb{Z}_q^* \) and hash function \( H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \), \( f_1 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2} \), \( f_2 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1} \), and then calculate the PKG public key \( Y_A = x_A P \). Finally, PKG sends the information \( E, G_q, P, Y_A, H_1, F, f_1, f_2, l_1, l_2 \) to the Signer node and Collector node.

2) Partial private key extraction. For each \( ID_i \) node, PKG will calculate and assign the following information. First, PKG selects a random number \( x_{Bi} \in \mathbb{Z}_q^* \), and then calculates \( Y_{Bi} = x_{Bi} P \), \( h_i = H_1(ID_i, Y_{Bi}, Y_A) \), \( s_i = (x_{Bi} + x_A h_i) \mod q \), and \( C_i = (s_i, Y_{Bi}) \). Then PKG sends information \( \{C_i\} \) to the nodes in the WBAN environment.

3) Set secret value. Signer node verifies the authenticity of \( \{C_i\} \) by calculating \( s_i P = Y_{Bi} + Y_A H_1(ID_i, Y_{Bi}, Y_A) \). If it is true, the Signer node randomly selects the secret value \( x_C \in \mathbb{Z}_q^* \) and \( x_D \in \mathbb{Z}_q^* \), and then the Signer node calculates \( Y_C = x_C P \), \( Y_D = x_D P \), \( Z_1 = x_C^{-1} Y_C \) and \( Z_2 = x_D^{-1} Y_D \), and then sends the information \( \{ s_i, Y_{Bi}, Y_C, Y_D, Z_1, Z_2 \} \) to the Collector node.

4) Set public key. Signer node then calculates \( Y_C = x_C P \), \( Y_D = x_D P \), \( Z_1 = x_C^{-1} Y_C \) and \( Z_2 = x_D^{-1} Y_D \), and then sends the information \( \{ s_i, Y_{Bi}, Y_C, Y_D, Z_1, Z_2 \} \) to the Collector node.
5) Blind signature generation. Collector node selects a point \( A(x_1, y_1) \) on elliptic curve \( E_p(a, b) \), and selects message \( m \). Then the Collector node calculates \( r_1 = x_1 \text{mod } q, r_2 = y_1 \text{mod } q \), then selects \( x_E \in Z_q^* \) and calculates \( M_1 = f_1(m) \parallel (f_2(f_1(m) \oplus Y_{B1}) \parallel m), Y_E = x_E P, Q = H_1(m, x_{E} P, Z_1 Y_{D} + Z_2 Y_{C} + r_2 M_1 P + s_1 r_1 P), M_2 = F(I D_i, Q), g = M_2 \oplus M_1 \text{ and } m' = Q - r_1 \), and sends the information \( \{m', Y_E\} \) to the Signer node. After receiving the message \( \{m', Y_E\} \), the Signer node calculates \( s'' = (x_E + x_D) - (m' s_1 + Y_E) \) and sends \( \{s''\} \) to the Collector node. The Collector node calculates \( s'' = (s' + r_2 M_1) \) after receiving the message \( \{s''\} \). So \( \{g, s'', Q\} \) is the blind signature in \( m \).

6) Verification. The verification node calculates \( \{Q'\} = H_1(m, s_1 P_E, s' P + Q s_1 P + Y_E P), M_2' = F(I D_i, Q'), M_1' = g \oplus M_2', \text{ and } m' = \{M_1' \parallel f_2(I D_i) \parallel M_1' \parallel Y_{B1}\} = m \), the signature information and the authenticity of the Collector node are successfully verified. The proof process is as follows:

\[
Q = H_1(m, s_1 P_E, Z_1 Y_D + Z_2 Y_C + r_2 M_1 P + s_1 r_1 P) = H_1(m, s_1 P_E, x_E P + x_D P + r_2 M_1 P + s_1 r_1 P) = H_1(m, s_1 P_E, (x_E + x_D) P + r_2 M_1 P + s_1 r_1 P) = H_1(m, s_1 P_E, (s' + m' s_1 + Y_E) P + r_2 M_1 P + s_1 r_1 P) = H_1(m, s_1 P_E, s' P + m' s_1 P + Y_E P + r_2 M_1 P + s_1 r_1 P) = H_1(m, s_1 P_E, s' P + m' s_1 P + Y_E P + s_1 r_1 P) = H_1(m, s_1 P_E, s' P + Q s_1 P + Y_E P + s_1 r_1 P) = H_1(m, s_1 P_E, s' P + Q s_1 P + Y_E P + s_1 r_1 P)
\]

\( = Q' \)

The blind signature protocol based on Blockchain proposed in this section uses \( m' = Q - r_1 \) to blind the message \( m \). The Signer node cannot obtain the blind factor information, so the Signer node cannot know the content of the message \( m \). And the Signer node cannot track the signed information \( m \) according to \( \{s_1, Y_{B1}, Y_C, Y_D, Z_1, Z_2, m', Y_E, s'\} \), since the Signer cannot know the value of \( \{x_E, r_1, r_2\} \), so the proposed protocol has the characteristics of message blindness and untraceability. The blind signature protocol is shown in Figure 6.

IV. SECURITY AND PRIVACY ANALYSIS

In this section, the security of the hub node and private consensus mechanism are analyzed. The network structure limits the centralized WBANs, and the failure of a single server node will cause the cloud server layer to crash. The scheme proposed in this article utilizes two sets of private Blockchains at the WBANs cloud server layer to ensure the security of sensor node registration data and patient physiological data.

A. INFORMAL SECURITY ANALYSIS

1) HUB NODE STOLEN DATABASE ATTACK

The attacker can steal the registration data \( E_{k_S}(i d_{SN}, i d_N, \alpha) \) of the sensor node stored in the private Blockchain inside the hub node, and the sensor node’s symmetric key \( k_N \) encrypts the registration data. Even if the attacker obtains the encrypted registration data, he cannot obtain the registration data because he cannot obtain the symmetric key \( (i d_{SN}, i d_N, \alpha) \). Hub node uses Blockchain technology to protect the security of registration data is to protect the security of the session key \( k_S \). The attacker can also steal patient physiological data stored in a private Blockchain. However, the data is encrypted by the user’s key. The attacker cannot obtain the user’s key, and therefore cannot obtain the patient’s physiological data, and therefore, the network architecture of WBANs can effectively defend against hub node stealing database attacks.

2) DOS ATTACKS

DoS attack refers to that the attacker consumes hub node resources and preventing it from providing standard services. The cloud server layer of centralized two-hop WBANs has only one hub node. When an attacker uses the DoS attack, it is easy to make the hub node unable to provide services. The cloud server layer built using Blockchain technology consists of multiple hub nodes, each of which has the same permissions, and the private Blockchain of database storage is the same. Even if a local hub node in a specific area cannot provide access services, the sensor node in that area can perform authentication and key agreement with the hub node in other areas. Users can also access patient physiological data in the hub node private Blockchain across regions. The cloud server layer built using Blockchain technology makes WBANs have strong system stability and reliability.

3) SENSOR NODE IDENTITY PRIVACY PRESERVATION

The Blockchain is a public ledger, and the more decentralized the Blockchain system, the easier it is to add new members.
Every member of the Blockchain can easily access the contents of the Blockchain record, which will have the security problem of data leakage. Any disclosure on the identity of the sensor node will result in the disclosure of data details of that node. Therefore, the way how to protect the security of the sensor node identity in the Blockchain is essential. The Blockchain-based WBANs systems proposed in this article use private Blockchain, since the system administrator authorizes the hub node during the system initialization phase. Moreover, only the hub node authorized by the system administrator can become a new member of the maintenance private Blockchain, since the attacker cannot pretend to be a hub node. In this case, the attacker can only obtain the identity information of the sensor node by stealing the hub node’s database, but this method is also invalid.

**4) TRANSACTIONAL PRIVACY PRESERVATION AMONG HUB NODES**

Every node in the Blockchain needs to ensure the consistency of the ledger after the transaction is completed. Failure to consider privacy protection will result in the disclosure of transaction data. Thus, it is necessary to design a flexible and effective consensus mechanism to ensure that the data recorded in the new blocks are not leaked when new blocks are added to the Blockchain. In the scheme proposed, the registration data of the first set of private Blockchain record maintained by the hub node is encrypted by the symmetric key $k_N$. When new blocks containing the ciphertext is transmitted at the cloud server layer, it cannot cause the registration data to leak even if stolen by the attacker. The second set of private Blockchain records patient physiological data. The hub node uses the user’s key to encrypt patient physiological data collected by the sensor node. Therefore, data recorded in the new blocks are also ciphertext. The private Blockchain will not cause the leakage of patient physiological data when adding new blocks. Therefore, the proposed scheme achieves data privacy protection while ensuring the consistency of many hub node storage private Blockchain.

**B. FORMAL SECURITY VERIFICATION USING AVISPA TOOL**

This section uses the Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool to verify the security of the blind signature protocol [26]. The role-based formal language High-Level Protocol Specification Language (HLPSL) has a rich semantic expression module that selects the intruder’s mode and formulates the security goals of the protocol. The translator will automatically translate the HLPSL language into the intermediate formal language Intermediate Format (IF), which can be used directly by the test terminal.

Security Protocol Animator (SPAN) software provides an interactive graphical interface for the AVISPA simulation tool and able to animate the security protocol and construct a message sequence diagram from the data exchange between the various roles in the protocol, and shown in Figure 7 the complete execution process of the protocol in the presence of an intruder. It is used in this section two back-ends to verify the security of the protocol, whereas the report output from the back-end records whether the protocol is SAFE or UNSAFE. As shown from the experimental results, the blind signature protocol is secure under specific security goals.

**V. PERFORMANCE EVALUATION**

**A. CALCULATION COST**

Python is a simple and powerful scripting language, very popular in the field of scientific computing researches, and an increasing number of researchers have adopted Python for high-performance computing [27]. Python provides a large number of extension libraries, and includes hashlib for hash function calculations. As a simulation environment, Python version 3.7.3 is installed in a server equipped with an AMD 1600 CPU for performance testing of six hash functions.
MD5, SHA-1, SHA224, SHA256, SHA384 and SHA512 in generating block hash function value. First, assuming that the size of each block is 1024 byte, the experiment aims at finding the processing time required by different hash functions for the block hash function values, and the results are shown in Figure 8.

Next, assuming that the hash function values of 10000 blocks are calculated, the processing time required by different block sizes are tested, which results are shown in Figure 9. Results obtained from calculations indicate that, the processing time of MD5 and SHA-1 is approximately the same, SHA224 and SHA256 approximately the same, and SHA384 and SHA512 approximately the same, and thus, only the processing time of SHA-1, SHA256 and SHA512 hash functions are shown. By analyzing these results, it can be seen that the processing time of SHA-1 is the minimum and that of SHA256 is the maximum.

The block of authentication private Blockchain is used to record the hash function value of the block group in data private Blockchain, and the size of each block group is related to the number of internal blocks and the size of each block. Take the set of private Blockchain that records patient physiological data as an example. The size of each block depends on the amount of physiological data of a single patient in a unit time and which hash function is used. The length of other parameters in the block is relatively small, so it is not considered. The number of blocks in the block group depends on the number of patients whose physiological data is recorded by the private Blockchain within the unit time.

In order to simplify the calculation, the hash function value of block group is not the hash function value of all the data recorded in the block, despite the fact that the hash function value of all blocks in the block group is hashed again. Assuming that the size of the data that can be recorded in each block is 1024 bytes, experimentations with different hash functions calculations on the time cost of the hash function value of the block group with different numbers of blocks are depicted and shown in Figure 10. It can be seen that, even though SHA384 and SHA512 have a computing advantage is continuously calculating the hash function value of a block and calculating a hash function of a larger block, the highest calculation time is required in calculating a block group. Due to the fact that each block uses a different hash function to retrieve a different hash function value, the block group hash function value is affected by the input size. The private Blockchain with a higher security level should choose a hash function with a large amount of calculation, which will not support the attacker to tamper with the data recorded in the private Blockchain.

B. STORAGE OVERHEAD

The number of transactions that the Blockchain can process every second is one of the main challenges restricting its development. In different application scenarios, the requirements for the number of transactions that the Blockchain are potentially different. In the Bitcoin network, a maximum of seven transactions (theoretical) are processed [28], while in the transaction network and email network, at least 500,000 to 2,100,000 transactions must be processed each second.
In WBANs, millions of patients upload physiological data within a specific given period of time, which puts high demands on the scalability of the Blockchain. Therefore, it is simulated in this research the changes in the size of a set of private Blockchain data with time through the number of times the patient uploads physiological data per unit time, using the calculation formula adopted in [17] and then compared with the scheme proposed. The formula for calculating the size of the Blockchain is $M \times B \times T$, where $M$ defines the number of transactions sent per second, $B$ defines the size of a block, and $T$ defines the running time of the Blockchain.

In the data private Blockchain, the size of block size and time stamp is 4 Bytes, respectively. The size of block identity is 32 Bytes, and 512 Bytes for the transactions, respectively. This private Blockchain uses SHA512, and the size of the block hash value is 64 Bytes, so thus, the total size of a block is 616 Bytes. In the authentication private Blockchain, the size of block size and time stamp is 4 Bytes, the size of block identity is 8 Bytes, and the size of transactions is 32 Bytes. This private Blockchain uses SHA256, and 32 Bytes the size of the block hash value. Thus, the total size of a block is 80 Bytes. As depicted in Table 3, the result of the size of private Blockchain changing with transaction and time.

| Transaction | Pre Second | Pre Day |
|-------------|------------|---------|
| $R_B$ | $D_B$ | $[17]$ | $R_B$ | $D_B$ | $[17]$ |
| 2000 | 156.25 KB | 1.17 MB | 1.29 MB | 12.87 GB | 99.13 GB | 108.84 GB |
| 10000 | 781.25 KB | 5.87 MB | 6.47 MB | 64.37 GB | 495.67 GB | 545.91 GB |
| 15000 | 1.14 MB | 8.81 MB | 9.71 MB | 96.26 GB | 743.51 GB | 819.28 GB |
| 500000 | 38.15 MB | 293.73 MB | 323.77 MB | 3.14 TB | 24.20 TB | 26.68 TB |
| 2100000 | 160.22 MB | 1.20 GB | 1.33 GB | 13.20 TB | 101.65 TB | 112.22 TB |

| Transaction | Pre Year | Pre 10 Years |
|-------------|---------|-------------|
| $R_B$ | $D_B$ | $[17]$ | $R_B$ | $D_B$ | $[17]$ |
| 2000 | 4.59 TB | 35.34 TB | 38.79 TB | 45.89 TB | 353.36 TB | 387.90 TB |
| 10000 | 22.95 TB | 176.68 TB | 195.95 TB | 229.45 TB | 1.73 PB | 1.95 PB |
| 15000 | 34.42 TB | 265.02 TB | 292.03 TB | 334.18 TB | 2.59 PB | 2.92 PB |
| 500000 | 1.12 PB | 8.63 PB | 9.74 PB | 11.20 PB | 86.17 PB | 97.40 PB |
| 2100000 | 4.71 PB | 36.23 PB | 40.96 PB | 47.06 PB | 361.33 PB | 409.60 PB |

### VI. CONCLUSION

WBANs can not only effectively improve the medical service experience of patients, but also reduce the burden on the medical system, reserving a functional space for development in the future medical field. The security challenges of centralized WBANs can be solved by blockchain technology. In this article, the disadvantages of centralized WBANs are first presented, so then a scheme to build a cloud server layer is proposed using private blockchain technology in WBANs, and a new WBANs architecture model is designed. The hub node in the cloud server layer establishes two groups of private Blockchains, which are used to store the registration data of the sensor node and supernode and physiological data of patients, respectively. The private blockchain storage of registration data and physiological data can effectively reduce the complexity of regional data management. In addition, the working mode of the private blockchain consensus mechanism is described in detail. On this basis, a blind signature protocol in the blockchain network is designed. The experiments evaluate the computation cost and storage overhead of the cloud server layer for private Blockchain. The security of the blind signature protocol is verified using the AVISPA simulation tool. Experimental results show that the proposed scheme is up-and-coming and effective. In future work, we will continue to engage in authentication research and store vast amounts of data in WBANs based on Blockchain technology.

### ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their advice on technical issues examined and comments.

### REFERENCES

[1] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, “An industrial network intrusion detection algorithm based on multifeature data clustering optimization model,” IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2063–2071, Mar. 2020.

[2] X. Wang, L. T. Yang, Y. Wang, L. Ren, and M. J. Deen, “ADTT: A highly-efficient distributed tensor-train decomposition method for IIoT big data,” IEEE Trans. Ind. Informat., early access, Jan. 20, 2020, doi: 10.1109/TII.2020.2967768.

[3] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, “A novel smart card and dynamic ID based remote user authentication scheme for multi-server environment,” Math. Comput. Model., vol. 58, no. 12, pp. 85–95, 2013.

[4] M. Hagh, K. Thurow, and R. Stoll, “Wearable devices in medical Internet of Things: Scientific research and commercially available devices,” Healthcare Inform. Res., vol. 23, no. 1, pp. 4–15, 2017.

[5] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, “Secured data collection with hardware-based ciphers for IoT-based healthcare,” IEEE Internet Things J., vol. 6, no. 1, pp. 410–420, Feb. 2019.

[6] W. Liang, W. Huang, J. Long, K.-C. Li, and D. Zhang, “Deep reinforcement learning for resource protection and real-time detection in IoT environment,” IEEE Internet Things J., vol. 7, no. 7, pp. 6392–6401, Jul. 2020.

[7] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” Egyptian Inform. J., vol. 18, no. 2, pp. 113–122, 2017.
[8] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Zomaya, “Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection,” IEEE Trans. Emerg. Topics Comput., early access, May 11, 2020, doi: 10.1109/TETC.2020.2993032.

[9] N. Elisa, L. Yang, F. Chao, and Y. Cao, “A framework of blockchain-based security and privacy-preserving E-government system,” Wireless Netw., vol. 2018, pp. 1–11, Dec. 2018.

[10] X. Li, J. Niu, J. Liao, and W. Liang, “Crytpanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update,” Int. J. Commun. Syst., vol. 28, no. 2, pp. 374–382, Jan. 2015.

[11] H. U. Rahman, G. Wang, M. Z. A. Bhuiyan, and J. Chen, “Towards in-network generalized trustworthy data collection for trustworthy cyber-physical systems,” in Proc. 5th Int. Conf. Dependability Sensor, Cloud, Big Data Syst. Appl., Guangzhou, China, Nov. 2019, pp. 54–66.

[12] X. Meng, J. Xu, W. Liang, and K.-C. Li, “An anonymous mutual authentication and key agreement scheme in WBAN,” in Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput., (HPSConf); IEEE Int. Conf. Intell. Data Secur. (IDS), May 2019, pp. 31–36.

[13] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “McDS-Share: Trustless medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14757–14767, 2017.

[14] P. Zhang, H. Wang, C. Hu, and C. Lin, “On denial of service attacks in software defined networks,” IEEE Netw., vol. 30, no. 6, pp. 28–33, Nov./Dec. 2016.

[15] IEEE Standard for Local and Metropolitan Area Network-Part 15. 6 Wireless Body Area Networks, IEEE Standard 802.15, IEEE Standard Association, Piscataway, NJ, USA, Feb. 2012.

[16] X. Li, M. H. Ibrahim, S. Kumari, and R. Kumar, “Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors,” Telecommun. Syst., vol. 67, no. 2, pp. 323–348, Feb. 2018.

[17] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” Information, vol. 8, no. 2, pp. 44, Apr. 2017.

[18] A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain,” J. Med. Syst., vol. 42, no. 8, pp. 1–18, Aug. 2018.

[19] S. Amofa, E. B. Sifah, K. O. Ageyem, S. Abba, Q. Xia, J. C. Gee, and J. Gao, “A blockchain-based architecture framework for secure sharing of personal health data,” in Proc. IEEE 20th Int. Conf. E-Health Netw., Appl. Services (Healthcom), Sep. 2018, pp. 1–6.

[20] S. Wang, X. Wang, and Y. Zhang, “A secure cloud storage framework with access control based on blockchain,” IEEE Access, vol. 7, pp. 112713–112725, 2019.

[21] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, “Secure data storage and recovery in industrial blockchain network environments,” IEEE Trans. Ind. Informat., vol. 16, no. 10, pp. 6543–6552, Oct. 2020.

[22] X. Wang, L. T. Yang, L. Song, H. Wang, L. Ren, and J. Deen, “A tensor-based multi-attributes visual feature recognition method for industrial intelligence,” IEEE Trans. Ind. Informat., early access, Jun. 4, 2020, doi: 10.1109/TII.2020.2999901.

[23] R. Li, D. T. H. Lai, and W. Lee, “A survey on biofeedback and actuation in wireless body area networks (WBANs),” IEEE Rev. Biomed. Eng., vol. 10, pp. 162–173, 2017.

[24] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” Appl. Innov., vol. 2, nos. 6–10, p. 71, 2016.

[25] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, “A novel secret protocol for wireless sensor networks with cooperative communication,” Computers, vol. 9, no. 1, p. 4, Jan. 2020.

[26] A. Armando, D. Basín, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielisma, P. C. Heám, O. Kouchkarenko, J. Mantovani, S. Mødersheim, D. von Oheimb, M. Rustinowitch, J. Santiago, M. Turunni, L. Viganò, and L. Vigneron, “The AVISPA tool for the automated validation of Internet security protocols and applications,” in Computer Aided Verification, LNCS 3576, 2005, pp. 281–285.

[27] J. Demšar, T. Curk, A. Erjavec, C. Gorup, T. Hocevar, M. Milutinovic, M. Možina, P. Polajnar, M. Toplak, A. Staric, and M. Štajdohar, “Orange: Data mining toolbox in Python,” J. Mach. Learn. Res., vol. 14, no. 1, pp. 2349–2353, 2013.

[28] L. Lau, V. Narayanay, k. Baweja, C. Zheng, S. Gilbert, and P. Saxena, “SCP: A computationally-scalable byzantine consensus protocol for blockchains,” IACR Cryptol. ePrint Arch., vol. 2015, p. 1168, 2015.