IEEE Access
SPECIAL SECTION ON MOBILE SERVICE COMPUTING WITH INTERNET OF THINGS

Received March 31, 2019, accepted April 27, 2019, date of publication May 15, 2019, date of current version May 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2916345

Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving

WEI SHE[1,2,3], ZHI-HAO GU[1], XU-KANG LYU[4], QI LIU[1], ZHAO TIAN[1], AND WEI LIU[1,2]
[1]School of Software Technology, Zhengzhou University, Zhengzhou 450000, China
[2]Collaborative Innovation Center for Internet Healthcare, Zhengzhou 450000, China
[3]Water Environment Governance and Ecological Restoration Academician Workstation of Henan Province, Zhengzhou 450002, China
[4]School of Computer Software, College of Intelligence and Computing, Tianjin University, Tianjin 300354, China

Corresponding author: Wei Liu (wliu@zzu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602422 and Grant 61402328, in part by the National Key R&D Program of China under Grant SQ2018YFB1201403, in part by the Key Science and Technology Program of Henan Province under Grant 162102310536, and in part by the CERNET Innovation Project under Grant NGII20160705 and Grant NGII20180702.

ABSTRACT The relative low level of smart home system (SHS) device information security may threaten the privacy of users. In this paper, we propose a homomorphic consortium blockchain for SHS sensitive data privacy preserving (HCB-SDPP), which is based on the traditional smart home system. We add verification services, which are composed of verification nodes, to our model to verify working nodes and transactions in SHS. In order to record the SHS device information transaction, we propose a new block data structure based on homomorphic encryption (HEBDS). Using the HCB-SDPP model, we design an encrypted algorithm based on Paillier encrypted for privacy protection. To verify the validity of the HCB-SDPP model, we firstly encrypt sensitive data of all gateway peers and upload them to the consortium blockchain. Then, we validate the security of sensitive data after homomorphic encryption processing. In the experiment, we also design attack experiments to attack different types of peers on the consortium blockchain in the HCB-SDPP model. If these nodes are insecure, the influence on the whole model will be analyzed. The simulation result shows that the HCB-SDPP model can protect customer privacy more effectively than SHS.

INDEX TERMS Privacy preserving, smart home systems, consortium blockchain, homomorphic encryption.

I. INTRODUCTION

With the development and integration of the computer technology, the communication technology, and the Internet technology, the Internet of Things (IoT) [1] applications have been found in many fields [2]. IoT technology not only changes people's daily life [3], [4], but also creates new "ecological" environments [5]. IoT uses technologies like radio frequency identification technology, wireless communication technology, etc. to make real-time global information shared. In short, IoT involves interconnecting everything around us [6]. Things in IoT are smart devices that have the capability to "decide" the target to communicate (D2D) and to make computation. Data communication between devices in the IoT has always been a research hotspot [7]. Typical application of IoT can be found in the smart home system (SHS) [8], whose architecture is basically the IoT architecture [9].

The growth of smart devices has greatly increased the volume of individual health information, which is transmitted and stored by mobile phones, tablets, wireless sensors and wearable health devices in SHS [10].

If a large amount of personal information was hacked, it could cause a great influence harm to the whole society. Therefore, the network security of IoT in SHS has attracted the attention of many researchers. In [11], an SH-IoT architecture was provided to enable the interaction (communication) among various devices, and the possible risk for information security was explored under various scenarios. Reference [12] provided a solution to network-level security of SHS in the future. Such a flow-based monitoring in [9] can not only achieve most of the security advantages based on packet monitoring, but also reduce processing costs. In [13], Mehdi Nobakht *et al.* proposed an IoT-IDM framework that provided network-level protection for smart devices

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

deployed at home and monitored the malicious network activity. Healthcare devices in SHS generally record sensitive information such as blood pressure [14], heart rate [15], respiratory rate [16]. Therefore, in order to prevent sensitive data from being hacked, the security of network data is particularly important. Although the existing SHS can protect the privacy of users in some way, there are still some potential risks about information security. The above literatures have all adopt the central transaction data processing structure. These sensitive and privacy data of users are stored and processed centrally. If the centralized database system is attacked and the data is leaked, security and privacy of transaction data are difficult to guarantee.

The emergence of blockchain [17]–[19] and smart contract [20], [21] provided a new way for the protection and privacy of SHS. It is another type of cryptography system that integrates a consensus mechanism, distributed data storage, point-to-point transmission and encryption algorithms [22]. Now the technology continues to find novel applications in numerous areas such as digital asset transactions, equity clearing, cross-border payment, secure document storage and notarization. In [23], Madhusudan Singh *et al.* provided a blockchain network for IoT architecture and a distributed data share architecture. This literature discusses the combination of Blockchain technology and IoT environment, then puts forward the idea that blockchain is a solution of IoT security. In [24], Pascal Urien *et al.* provided a BIoT paradigm whose main idea was to insert sensor data in blockchain transactions, this literature uses BIoT paradigm to implement publication/duplication of sensor data in public and distributed ledgers, data authentication and non repudiation of data. Reference [25] constructed a trustworthy trading platform for IoT ecosystems by combining blockchain and IoT. It solves the trust problem in the ecosystem of IoT and the traceability problem of IoT equipment and related data. In [25], Bin Yu *et al.* proposed a solution using a local peer network to bridge the gap to address the problem of combining blockchain with IoT. The solution provides a way to resolve the difficulty of implementing blockchain point-to-point network on IoT devices which is caused by resource constraints. It also solves the problem that the current blockchain is hard to handle the speed of transaction generation due to the large number of devices in IoT. Therefore, summarize the above literatures, the problems in the privacy security and privacy protection of data from IoT can be solved through combining blockchain and IoT technologies. The anonymity of blockchain technology makes it impossible for one to match an account of others even if the user can see all transaction records about an account. The information of blockchain is highly transparent and tamper-resistant, which can effectively reduce the risk of privacy leakage. The emergence of Change [26] and CoinJoin [27] provided a safe and effective tool for data privacy. However, the Consortium Blockchain serves as a kind of blockchain framework. While containing the characteristics of blockchain, the Consortium Blockchain architecture will be more suitable for the fields that focus on privacy protection, transaction speed and internal supervision. The Consortium Blockchain realizes the blockchain technology to provide new support for the security and privacy protection of SHS based on the IoT architecture.

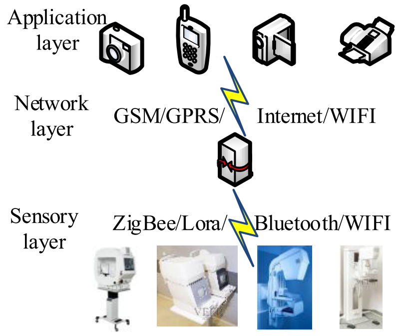

FIGURE 1. Schematic diagram of SHS.

This paper is structured as follows. In Sec. II, we introduce the concept of SHS, Consortium Blockchain and homomorphic encryption Paillier. Section III discusses the modified SHS and the HCB-SDPP model, then we design a new block data structure HEBDS of the latter. In Section IV, we present a deep analysis of examples result; to evaluate the data security of our model, Section V performs attack experiments and conducts comparative analysis to verify the characteristics for protecting privacy data of the HCB-SDPP model.

II. PRELIMINARIES

A. SMART HOME SYSTEM

Traditional SHS [28] takes the residences as one platform to inherit or control various furniture devices and forms an intelligent system that integrates the structure, service, system and management.

Fig. 1 shows the architecture of a traditional SHS and that architecture can be divided into three layers: application layer, network layer and sensory layer. The application layer mainly accesses, analyzes, processes data and issues control commands. That is, users can access mobile terminals through the GSM/GPRS/Internet/WIFI network. The sensory layer mainly collects data generated by real-world devices. The network layer mainly involves the problems of control terminal in the application layer and intelligent sensor device in the perception layer to access the network and data transmission. The home gateway is the core of the SHS. It is the only way to connect the external network with the home network (local network). It allows devices to access GSM/GPRS/Internet/WIFI network, and to collect all kinds of communication data of sensors through ZigBee/Lora/Bluetooth/WIFI network.

B. CONSORTIUM BLOCKCHAIN

At present, the blockchain technology [29] can be divided into Public Blockchain, Consortium Blockchain and Private Blockchain. Because SHS demand for huge privacy data

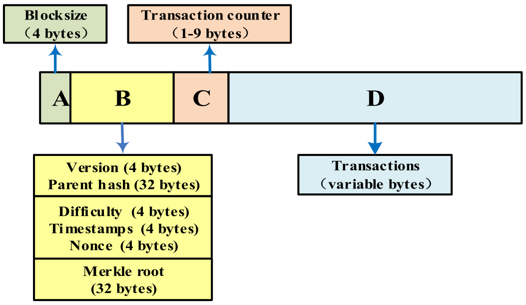

FIGURE 2. Blockchain block structure.

security, as well as the system within the sensor attached to the terminal each residential distribution characteristics, we need to rely on the Consortium Blockchain that has the characteristic of multi-blockchain structure, high scalability, high interoperability, and its system can be implemented more organizational governance, members of the cooperative Consortium Blockchain. The Consortium Blockchain can help us to provide new support for SHS security and privacy protection by taking advantages of the above characteristics of blockchain technology.

The multi-blockchain structure of Consortium Blockchain refers to multiple blockchains formed by the nodes that controlled by different entities. Each blockchain runs multiple nodes. The data in the Consortium Blockchain only allows nodes in different blockchains to read, write and send transactions, all nodes in blockchain jointly record the transaction data. Data exchange between different blockchains can be implemented using methods such as channels in Fabric (one of the Consortium Blockchain project). The construction of Consortium Blockchain also follows a whole set of consensus and protocol mechanism. The consensus process is not required to involve all nodes in blockchain like public blockchain, but controlled by some pre-selected nodes with large weights. The distributed ledger and distributed consensus of Consortium Blockchain solve the trust problem of the interaction among multiple participants.

The data structure of the Consortium Blockchain is generally divided into two parts [30]: 1) the block header, which mainly contains the hash value of the previous block and is used to connect the previous block to ensure the integrity of the blockchain; 2) the block body, containing the main information of the block (transaction information), which together with the hash value of the previous blocks and random numbers constitute the hash value of the block. The data structure of Consortium Blockchain is shown in Fig. 2.

Such this data structure enables the information of each block to be traced from the pre-selected nodes and to affect the information of the subsequent nodes. Its cryptographic method [31] ensures that malicious attacks cannot tamper with information, thus ensuring the security and integrity of data. For areas such as privacy protection, transaction speed and internal regulation, the Consortium Blockchain structure is more appropriate.

C. HOMOMORPHIC ENCRYPTION TECHNOLOGY

Homomorphic encryption [32], [33] is a form of encryption, which allows people to make specific algebraic operations on ciphertext to obtain still encrypted results. The result obtained by decryption is the same as that obtained by the same operation on plaintext. In other words, the technology allows people to perform operations such as retrieval, comparison and other operations in the encrypted data to get the correct results without having to decrypt the data in the whole process. The significance lies in the fundamental solution to the problem of confidentiality when data and its operation are entrusted to a third party, such as for various cloud computing applications.

Paillier encryption is a kind of homomorphic encryption [34]. This encryption system is the first additive homomorphic encryption cryptosystem based on the determination of composite residual problems. It was proposed by the scholar Paillier in 1999, and its security is based on the determination of composite residual problems. The additive homomorphism can not only process ciphertext data quickly, but also meet the high security requirement [35]. This means that, given only the public key and the encryption of m_1 and m_2, you can calculate the encryption of $m_1 + m_2$. The Paillier algorithm can be divided into the following steps:

Step 1. Key Generation from Paillier Function.
1)Randomly choose two large prime numbers p and q, if and only if, for $\forall p, q \in DPN$, where DPN is a large prime, and we get: $\gcd = (pq, (p-1)(q-1)) = 1$.
2)Calculate $\lambda(N) = lcm(p-1, q-1)$ and $N = pq$.
3)For $\forall g \in Z^*_{N^2}$,$\mu = \mathrm{mod} N/(L(g^{\lambda(N)} \bmod N^2))$ has to be satisfied. Among them, $L(x) = (x-1)/N$.
4)Public Key, $pk = (N, g)$.
5)Private Key, $sk = (\lambda(N), \mu)$.

Step 2. Encryption
For $\forall m \in Z_n$ randomly select $r \in Z^*_N$ to get CT $c = E_{pk}(m) = g^m r^N \bmod N^2$.

Step 3. Decryption
For $\forall c \in Z_n$, decrypt the PT
$m = D_{sk}(c) = L(c^{\lambda(N)} \bmod N^2) \cdot \mu \bmod N$.

Step 4. Analysis of homomorphism
For $\forall m_1, m_2 \in Z_n$, encrypted by the Encrypt function, we will get:
$E(m_1) = g^{m1} r_1^N \bmod N^2$, $E(m_2) = g^{m2} r_2^N \bmod N^2$
Then you can find:

$$E(m_1) \cdot E(m_2) = g^{m1} r_1^N \cdot g^{m2} r_2^N \bmod N^2 = E(m_1 + m_2)$$

III. SMS PRIVACY PROTECTION AND SECURITY SHARING MODEL

In this section, we will propose the HCB-SDPP model. First of all, we introduce the overall structure involved in the HCB-SDPP model in Sec. III-A. We add the idea of channel from Fabric in model and describe the topology of the whole model. In Sec. III-B, we construct a new block data structure. In Sec. III-C and Sec. III-D, we design the distributed

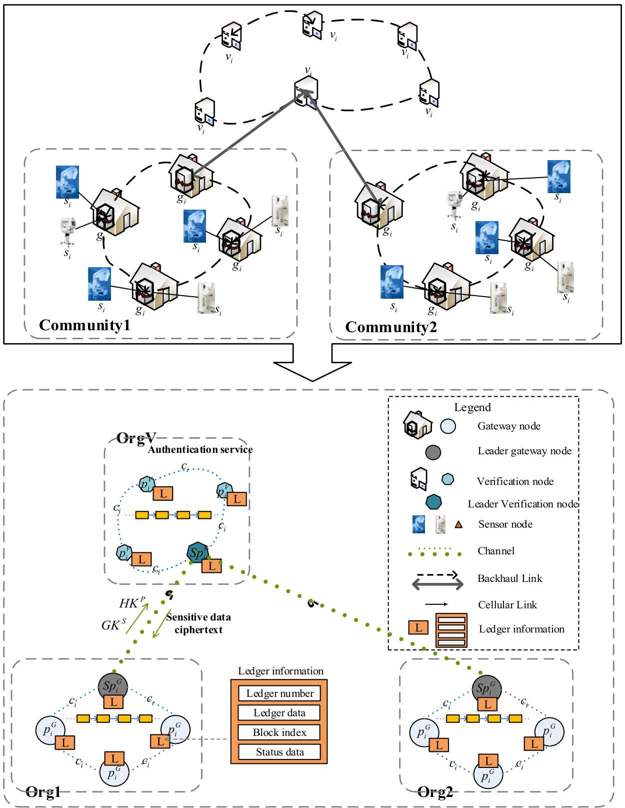

FIGURE 3. The structure of HCB-SDPP model.

consensus method, homomorphic data decryption of the model, the key generation, and update methods of the model. The working process of the model is given in Sec. III-E.

A. THE MODEL ARCHITECTURE

As shown in the top half of Fig. 3, different from the usual SHS [36] and to better manage its members and encrypt sensitive data within SHS, we consider adding verify nodes v_i into SHS and using homomorphic encryption to encrypt and protect sensitive data in SHS. We create a connection between the v_i and the smart gateway nodes g_i that has added in SHS through backhaul link. First of all, the v_i will generate the node key pair and the homomorphic encryption key pair, and v_i will distribute the secret keys to all g_i that connect with v_i. At the same time, sensor nodes s_i gather users' sensitive data in real time, and upload integrated data to the associated smart gateway g_i through cellular link; g_i collects all users' sensitive data uploaded by s_i in transmission range. Then g_i will use the node key and the homomorphic encryption key to encrypt sensitive data. Finally, the privacy sensitive data encryption protection is realized.

As shown in the lower part of Fig. 3, we map the new smart home system network into homomorphic Consortium Blockchain. There are four main types of nodes in the homomorphic Consortium Blockchain: smart gateway nodes, leader smart gateway node, verification nodes and leader verification node. The p_i^G is the smart gateway node, we integrated p_i^G from one common community into a common organization, and create one channel to make p_i^G from one common organization to joined in. Through this channel, all joined p_i^G will store the collected sensor sensitive data by consensus.

The p_i^V is the verification node, all p_i^V constitute members of the certification service. p_i^V provides digital certificate-based identity information to members of the homomorphic Consortium Blockchain community (Each p_i^G and the organization in the communication range is a consortium), and can generate or cancel a member's identity certificate. On the basis of clear membership, the organization can implement the management of authority control. p_i^V is served by the pre-selected p_i^G. It is mainly responsible for processing the smart contract, checking the legality of transaction data, and updating and maintaining the node data and the account status in blockchain organization. In particular, the generation of each block is determined by all pre-selected nodes and stored in homomorphic Consortium Blockchain.

The Sp_i^G is the leader smart gateway node and is also the anchor smart gateway node, because all nodes in blockchain are anonymous, they do not know the node information of each other. When the nodes outside blockchain need to communicate with the nodes inside blockchain, they need to elect a leader smart gateway node Sp_i^G and communicate with the outside through this node. The Sp_i^G can also be found by the external nodes as an anchor node. The Sp_i^V is the leader verification node and is also the anchor verification node. Both the Sp_i^G and Sp_i^V are responsible for communicating with outside world and the anchor nodes of other channels. Neither the Sp_i^G nor the Sp_i^V is fixed, the Sp_i^G is selected periodically and automatically by all p_i^G, as well as the Sp_i^V is also selected periodically and automatically by all p_i^V. The HCB-SDPP model will created V-G channel between the Sp_i^G and the Sp_i^V, the Sp_i^G communicates with the Sp_i^V as a representative. The node key, the homomorphic encryption key and the encrypted ciphertext of sensitive information will be transmitted between the Sp_i^G and the Sp_i^V through V-G channel.

Therefore, based on characteristics of modified SHS, the overall structure of the modified SHS can be mapped into the homomorphic Consortium Blockchain, we propose the homomorphic Consortium Blockchain for SHS sensitive data privacy preserving (HCB-SDPP). The HCB-SDPP model is formalized as follows:

Definition 1: HCB-SDPP is a 11-tuple.

$$(S, G, V, P, C, GK, HK, \delta, \psi, \sigma, \omega)$$

where:

1) $S = \{s_i | i \in \mathbb{N}^+\}$ is the finite set of sensor node s_i in the SHS.

2) $G = \{g_i | i \in \mathbb{N}^+\}$ is the finite set of smart gateway node g_i in the SHS.

3) $V = \{v_i | i \in \mathbb{N}^+\}$ is the finite set of verification node v_i.

4) $P = P^G \cup P^V$, $P^G = \{p_i^G | i \in \mathbb{N}^+\}$ is the finite set of smart gateway role p_i^G in Consortium Blockchain. Sp_i^G is the leader

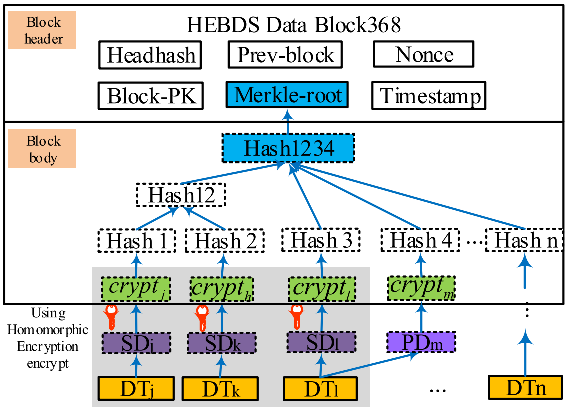

FIGURE 4. The data structure of HEBDS.

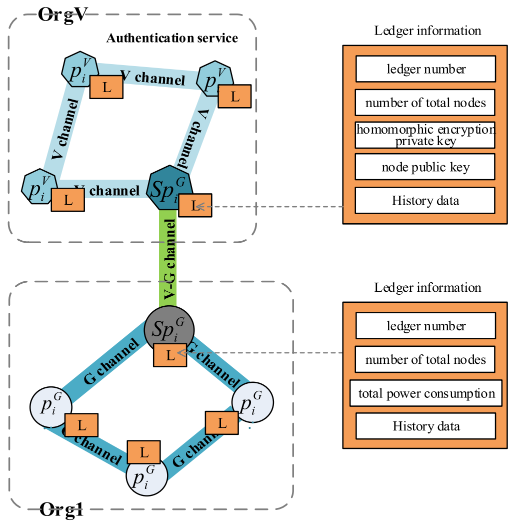

FIGURE 5. The schematic diagram of V-G channel.

smart gateway node and is also the anchor smart gateway node. $P^V = \{p_i^V | i \in \mathbb{N}^+\}$ is the finite set of verification role p_i^V in Consortium Blockchain. Sp_i^V is the leader verification node and is also the anchor verification node.

5) $C = \{c_i | i \in \mathbb{N}^+\}$ is the finite set of channel c_i in Consortium Blockchain.

6) $GK = GK^P \cup GK^S$, $GK^P = \{gk_i^P | i \in \mathbb{N}^+\}$ is the finite set of node public key, $GK^S = \{gk_i^S | i \in \mathbb{N}^+\}$ is the finite set of node private key.

7) $HK = HK^P \cup HK^S$, $HK^P = \{hk_i^P | i \in \mathbb{N}^+\}$ is the finite set of homomorphic encryption public key, $HK^S = \{hk_i^S | i \in \mathbb{N}^+\}$ is the finite set of homomorphic encryption private key.

8) $\delta : P \rightarrow C$ is the mapping from the finite set of Consortium Blockchain nodes P to the finite set of channel C.

9) $\psi : G \rightarrow P^G$ is the mapping from the finite set of smart gateway node G in SHS to the finite set of smart gateway node P^G in Consortium Blockchain.

10) $\sigma : V \rightarrow P^V$ is the mapping from the finite set of verification node V to the finite set of verification node P^V in Consortium Blockchain.

11) $\omega : GK^S \rightarrow G$ is the mapping from the finite set of node private key GK^S to the finite set of smart gateway node G.

B. THE BLOCKCHAIN DATA STRUCTURE OF HCB-SDPP

Different from the structure of data blocks in usual Consortium Blockchain, sensitive data need to be protected in HCB-SDPP. Therefore, this paper proposes a new block data structure based on Homomorphic Encryption (HEBDS), its structure is shown in Fig. 4. Compared with transaction data recorded by other Consortium Blockchain, the HEBDS proposed in this paper mainly records sensitive data of users, such as blood pressure, heart rate and breathing rate in personal health data, or power consumption and idle time in status data of smart devices.

The difference between HEBDS and other Consortium Blockchain block data structures is that, at some point t, after the smart gateway g_i collects message data $msg_i = \{cm_j, \cdots, cm_k\}$ from a group of sensors $(c_j, \cdots, c_k)$, g_i does not hash the message data directly, but divides the message data into public data (PD) and sensitive data (SD), $msg_i = msg_i^{PD} \cup msg_i^{SD}$. msg_i^{PD} is some publicly available data, msg_i^{SD} is private and sensitive data, it only visible to users, such as blood pressure and heart rate in personal health data, or power consumption in status data of smart devices. For data in msg_i^{SD}, it needs to be homomorphic encrypted with the homomorphic encryption public key hk_t^P related to the current time t. Then, the HEBDS uses the private key gk_i^S assigned to g_i to sign the entire data of msg_i ($crypt_j$-$crypt_k$ in Fig. 4), and hash the signed data (Hash1-Hash4 in Fig. 4). Finally, the HEBDS generates a unique merkle root to write into the block header.

C. DISTRIBUTED CONSENSUS METHOD AND HOMOMORPHIC DATA DECRYPTION

When data in HEBDS needs to be computed (such as accumulated or statistically), the verification node set V in the HCB-SDPP model take a distributed consensus to decide whether to respond to the request:

Take the calculation of household electricity consumption in the same community as an example.

Step 1. The leader smart gateway node Sp_i^G can obtain the homomorphic "electricity consumption" value in all blocks of this G channel chain, and calculate the total electricity consumption quantity (ciphertext state) by means of homomorphic accumulation method.

Step 2. After electricity consumption quantity (ciphertext state) is exchanged through V-G channel and received by the anchor node (the leader verification node Sp_i^V) of V channel, a transaction is initiated (translate the homomorphic ciphertext into plaintext).

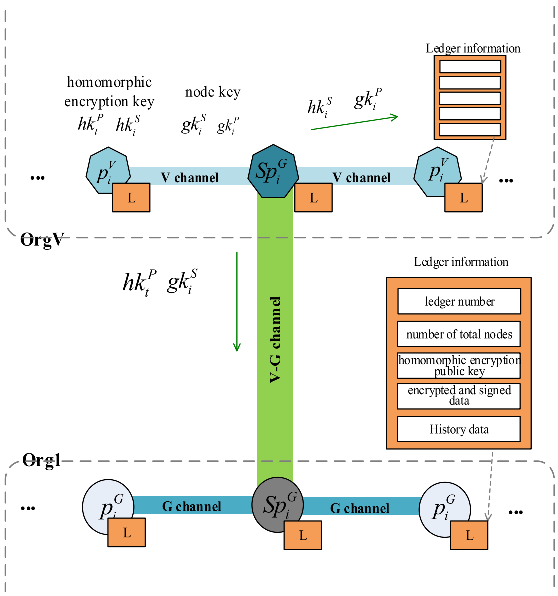

FIGURE 6. **The schematic diagram of V-G channel.**

This transaction needs to be verified by all verification nodes p_i^V. After the verification is passed, the accounting nodes will translate it. The translation process will be carried out through the homomorphic encryption private key corresponding to the corresponding timestamp of the given data. If there are multiple groups of data in different time stages, the chain code will search for the corresponding homomorphic encryption private key in different time stages. After that the chain code will decrypt the data and then summarize them.

D. KEY GENERATION AND UPDATA METHODS

When sensitive data in HEBDS needs to be encrypted, the homomorphic encryption key and the node key will be updated periodically.

When nodes in V channel conduct consensus, the p_i^V that obtain the bookkeeping right are selected by the PoW. These p_i^V are responsible for generating key pairs equal to the number of nodes in G channel. Through V-G channel and the leader smart gateway node Sp_i^G, the Sp_i^V will give each p_i^G in G channel a private key (directly replace), and will write the public key of this key pair group into the block of V channel.

In addition, the p_i^V that obtain the bookkeeping right will generate a pair of homomorphic encryption keys. The homomorphic private key should be recorded in the block of V channel, and the homomorphic public key should be published to G channel as a special transaction through the two anchor nodes on both channels and V-G channel.

E. THE WORKING PROCESS of MODEL

In order to describe the working process of the entire model more clearly, we briefly describe it, the HCB-SDPP model working process as follows:

Step 1. The formation of HCB-SDPP main chain and genesis block. In HCB-SDPP, multiple pre-selected nodes are selected according to the PoW consensus algorithm as the bookkeeping nodes of the whole network from p_i^G and p_i^V. These pre-selected nodes as bookkeeper, and the generation of each block is decided by all of them. (pre-selected nodes participate in the consensus process). In HCB-SDPP, in order to achieve information transmission, storage and query among multiple same nodes, we create V channel and G channel. We add all p_i^V into the V channel and add p_i^G from the same organization (community) into their respective G channel. The V channel is established before the G channel. The first transaction in HCB-SDPP is agreed by all bookkeeping nodes and written into a block, which is the creation block in HCB-SDPP and the first block in main chain of HCB-SDPP.

Step 2. Allocate the node key and the homomorphic encryption key. Firstly, *HK* and *GK* are generated by the p_i^V that obtain the bookkeeping right nodes in the V channel. These nodes save hk_i^S and gk_i^P into the block of the V channel. At the same time, they transmit hk_t^P and gk_i^S through V-G channel to G channel, G channel distributes gk_i^S to each p_i^G. And hk_t^P is treated as a special transaction, the corresponding bookkeeping node in G channel should record the homomorphic public key in the block.

Step 3. Publish the signed packet. When a certain smart network node p_i^G collects the information sent by sensor nodes, it will be processed as a "transaction": firstly, the data will be homomorphic encrypted (such as Paillier), and then the homomorphic encrypted data will be packaged into data package (DP), and the DP will be signed by gk_i^S. In this formula, d is the serial number of the DP. Finally, DP is published to the network by p_i^G.

$$DP_{\mathrm{d}} = \{Data_{gk_i^S} | \mathrm{d} \in \mathrm{N}^+, \mathrm{i} \in \mathrm{N}^+\}$$

Step 4. Produce block. All p_i^G select the bookkeeping nodes of the whole network according to PoW consensus algorithm, and the bookkeeping nodes write the all information in a period of time into block header in the form of Merkle tree, and they store ParentHash, Coinbase, TimeStamp, Merkle tree root, Number, Nonce and other parameters in block body. Among them, ParentHash and Nonce need to be calculated based on the parameters of the previous block such as nonce and hash value. Finally, they pack block header and block body into a new block which is linked at the end of main chain. These correct blocks are sequentially linked in time stamp to form a chain data structure, which ultimately forms a blockchain.

Step 5. Data query or summary. When the chain code running on a node needs to query or summarize the data

TABLE 1. The users privacy sensitive data of p_i^G.

Indicator	p_i^G_1	p_i^G_2	p_i^G_3	...	p_i^G_50
HR	79	79	95	...	102
BP	112	139	145	...	124
RR	18	18	16	...	19

in G channel, this node should join in G channel to obtain chain block data of the channel firstly, and then perform homomorphic calculation to obtain the ciphertext of statistical result.

IV. SIMULATION EXPERIMENT AND ANALYSIS

In usual SHS, sensitive privacy information collected by smart home devices often has the problems of weak non-anonymity, the risk of privacy leakage in the process of calculation and storage. To solve this problem, we carried out simulation experiment on HCB-SDPP model. We successfully deployed the HyperLedger Fabric 1.2.0 environment with multiple machines and nodes under the Ubuntu 16.04 operating system, we manually used configuration files to create multiple channels (V channel, G channel and V-G channel) and multiple nodes, and we added the corresponding nodes into the corresponding channels. With the above methods, we construct HCB-SDPP model.

The contents of simulation are as follows: There are about 100 gateway nodes p_i^G in community, and due to the limited computational force in simulated experimental environment, we randomly selected 50 gateway nodes p_i^G for the simulation experiment. Each users' personal health data or status data of smart devices are uploaded to the smart gateway node p_i^G. Each p_i^G collects three types of SHS private sensitive data: heart rate (HR), blood pressure (BP) and respiratory rate (RR). The plaintext of users' privacy data collected by each p_i^G is shown in TABLE 1.

In HCB-SDPP model, we create two channels, G channel and V channel, and we add these 50 p_i^G to G channel, the verification nodes p_i^V are all added in V channel. The HCB-SDPP model will use its own characteristics of the Consortium Blockchain architecture and the method of homomorphic encryption to encrypt and protect the users' privacy sensitive data. The data processed by p_i^G is encrypted into the form of TABLE 2 (only 2 types of p_i^G data are listed this paper), and broadcast to G channel composed of all p_i^G as a transaction. The bookkeeping node in G channel uses homomorphic calculation for statistics of all the obtained indicators, as shown in TABLE 3. At this point, the results of the homomorphic calculation are in ciphertext form, which can be interpreted as plaintext after obtaining the authorization of p_i^V, but only limited to the profile data. No node can know the original HR, BP, RR and other original data of user. The input values and results of this homomorphic computation are saved as a HEBDS block (as shown in TABLE 4), and linked to the main chain of the Consortium Blockchain, and synchronized

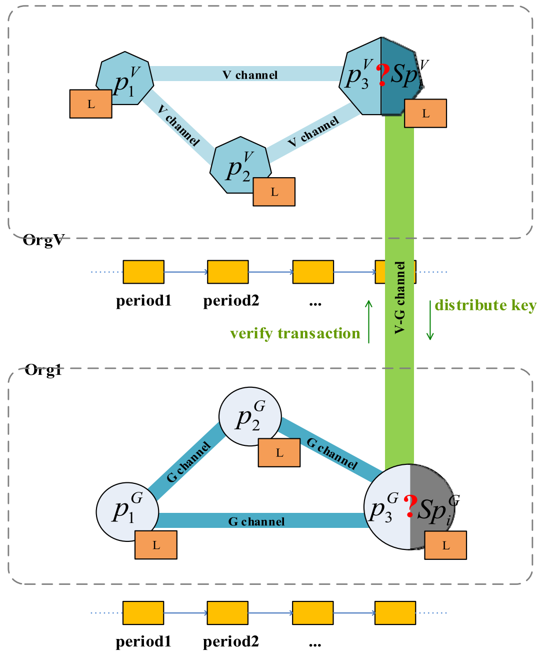

FIGURE 7. The design diagram of attack experiment.

to all p_i^G. The p_i^G with the permission of p_i^V in the same G channel and in the Consortium Blockchain can consult the statistics of these users' sensitive privacy data through the authorized hk_t^P and gk_i^S at any time, and it can also trace and accumulate the historical data along the blockchain. However, since the signature of p_i^G private key gk_i^S is added in the data preprocessing, any node cannot pry into the private data of other nodes before obtaining the p_i^V permission.

V. ATTACK EXPERIMENT AND PERFORMANCE ANALYSIS

A. ATTACK EXPERIMENTATION AND ANALYSIS

In this section, we will design an attack experiment. There are many gateway nodes in the community, and each users' personal health data or status data of smart devices is uploaded to the corresponding smart gateway node. The HCB-SDPP is used for managing these data uniformly. In the practical application of the HCB-SDPP model, the verification node p_i^V in V channel, periodically generates a pair of homomorphic encryption keys and n pairs of node keys. The homomorphic encryption private key hk_i^S and the n node public keys gk_i^P are stored in the blockchain of V channel, and the homomorphic encryption public key hk_i^P and the n node private keys gk_i^S are distributed to the smart gateway node p_i^G in G channel. In G channel, the smart gateway node p_i^G periodically encrypts the smart home sensitive data with the homomorphic encryption public key hk_i^P and the n node private keys gk_i^S. These data and the hk_i^P are stored in the blockchain of G channel. The Sp_i^G and Sp_i^V are selected periodically and automatically.

When the HCB-SDPP model is made into use, it will be attacked by malicious nodes or malicious programs. When the HCB-SDPP model is under network attack, and different types of nodes in the model are attacked and become insecure

TABLE 2. The ciphertext of p_i^G user privacy sensitive data indicators by homomorphic encryption.

p_i^G	Indicator	Corresponding ciphertext
1	HR: 79	7269101104738362791976471928211212827202493837328237781612667251124782736354682736382176352110294802838349111324352901928356231420928371345382021093821637282010393948476282203091829302029212353210200939792102792032101392732937193210319480816415216356310130351635163576352631567351403135163413436361631361436 43
	BP: 112	37355123523515323131472140095529000062922826358496576536420842471920502272785562539197196976074825808341557249303329312432428772925445733485271719231231195722767677419725589052231335108124981571231168846654793961456385774498759128895426331820234234224557381515945361278650772513027259112313134144115465474534 6
	RR: 18	28020142253836042406142119376196064946937080355579804183156090688604844988600838387270076722789810192367011636731362068376536310978255057452914624227351133463903464734867907869399107597707558289315669557488886985432733959471007242300902921192840725795129266461667448839853000676346593249156101845640783886347
...	...	......
50	HR: 102	11450311897153501235098210789756583153781512516727414485271250026045797881673102147262749418158810003471837217874238278518859269925876005458752801178622566417612581576188684893744883840716690781292495797894730382345437162100405660820313156402482546479273204051970915711785579892947483295154067032516197904923
	BP: 124	64869511005535921846042161832924354582480773484913257072697707868692150192381749868205878451615106585844715215684766100644773858685481342816790805855007636384326232120772204877743436744584961283884225206025505028618768382930724309229183210348172770361443556000840153354831057657094702051310902808422718490431
	RR: 19	14506505283628636420129741707000614503929027195962728163390428235406684366442054101214459855614453386646341763202943417989039059690557089108200000995001484583157645521246354954535571121248529995967870123344178974146275022929788049392548297210506660746988126483487631690740149372244558159371615694785044948 58

TABLE 3. The statistical results.

Avg	Encrypted avg
$\overline{HR} = 79$	49654592884641019846941536489781952495337461940268250362105487730847693038063739414588272205018850463321249940024872906060344869062987887372364544735777175484635963065617500347452615097805030506064433348118316175110497111875467269775062419954113578789102660153077071849149555840158486122393067966924549670567 1
$\overline{BP} = 111$	04096333332094362416804915628597275935684651514581067323744233356774178129139183251696231555028429675976213163304192715814068262857844827080473269018424506661285561627763774325999505707959418915446679956001071968750027102730399668360466333422482045979357091099498614684549050617178644948159809473419630366936
$\overline{RR} = 17$	29039485864634170789747428669205988213920228317569090570009950410556138341051260652664466050114528362863642012974596074671707051798359434006627544845195965521288405815937146482945299121445289399910820067849308344839231232969054453557054081607495145273541339004787224406622014499615694785041121248316768357 45

nodes, we analyze the influence of these insecure nodes on the entire model network and on the household privacy data stored in it. Here we analyze 8 cases of attacks:

Exp.1 Assume that p_3^G is Sp_i^G, and it is attacked as an insecure node. The following data will be leaked: 1. the homomorphic encryption public key hk_i^P and the n node private keys gk_i^S distributed by Sp_i^V; 2. all of the current n transaction sets which are smart home sensitive data encrypted and signed by homomorphic encryption; 3. the statistical and verifiable historical transaction data, which are all ciphertext. In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.2 Assume that p_3^G is not Sp_i^G, and it is attacked as an insecure node. The following data will be leaked: 1. the smart home terminal information collected by

TABLE 4. The information recorded in HEBDS in a certain period of time.

Various indicator				Data
asset	data	message	1	2947914223811727797250601156151127903547779382936475659722241901320012649743264995716460759720165252931184267768195375954031164133380724942486803237384111471731795611716916633983175960964550433361319160189326967883688796148228660273103142979171831514066120401830634352164554456894029713732828599416934540840 1
			2	3858448777736486951161832924354582480773484913251742098707269770761510658584473210348172771505535943121568476610064476854813426736121846042384816790807622043327484049612801309470205132520686869923884255050286187683212070583829307243092291803614435516255053354831057657868458600058784510221510902808422718490 0
			3	9485864634170789747213929029039057000995001145065052836286364201297417070535943417980061452735414936074633904286692059880478722442410556144533836644564484519596606622083157658357455212464829452991214452893995967879108200012329690557083441051264831462750229235408160776495411212483169988405815937161569478504
inputs	id			aa25fa630ab28e6b02cf9afd03e66d83dbe569bf5e9db93fc9375d0e4ae3628b
	owners_before			72xGFjhD9SMU6ZosgsfMKEDAP3EqmymXgJbNunMxa4an
	fulfills			null
	fulfillment			pGSAIFmmMD26Al62y5EV8Our3T8JNBx_NpULcFNuy8KnJO1rgUCtqbTMxR0LcLHSTUlE L3E2n-x1WKidc_6MI_bd5g5xQ2dAoNU8NT-hxpjR8-9wXCfAx73Ex-uRsjk4hqQ6dqEA
operation				CREATE
metadata				null
outputs	condition	public_key		72xGFjhD9SMU6ZosgsfMKEDAP3EqmymXgJbNunMxa4an
		details	type	ed25519-sha-256
			public_key	72xGFjhD9SMU6ZosgsfMKEDAP3EqmymXgJbNunMxa4an
		uri		ni:///sha-256;DEcoQmQ50eJvC1MGXVVbSKdfYbZZ3Y6QLEiVYwh43Oo?fpt=ed25519-sha-256&cost=131072
	amount			3
version				2.0

p_3^G itself; 2. the previous block information, which records previously encrypted smart home sensitive data that cannot be decrypted.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.3 Assume that p_2^V is Sp_i^V, and it is attacked as an insecure node. The following data will be leaked: 1. the homomorphic encryption public key hk_i^P and the n node private keys gk_i^S distributed by Sp_i^V; 2. the authenticated homomorphic encrypted data that Sp_i^G requests; 3. with the key leaked by Sp_i^V, data on the Sp_i^G can also be decrypted and obtained, but these data are the result data of homomorphic encryption, and the sensitive data on the other p_i^G will not be leaked; 4. the data stored on the blockchain from time 0 to time $n-1$ in the past (the homomorphic encryption private key hk_i^S and the n node public keys gk_i^P). However, Sp_i^V cannot initiate a request to query the content of the previous data block in G channel blockchain.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.4 Assume that p_2^V is not Sp_i^V, and it is attacked as an insecure node. The following data will be leaked: the previous homomorphic encryption private key hk_i^S and the n node public keys gk_i^P.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.5 Assume that p_3^G is not Sp_i^G, p_2^V is not Sp_i^V, and they are all attacked as insecure nodes at the same time. Combining the experiment results of Exp 2 and Exp 4, the following data will be leaked: 1. the smart home terminal information collected by p_3^G itself; 2. the previous encrypted block information in G channel blockchain and the previous he homomorphic encryption private key hk_i^S and the n node public keys gk_i^P in V channel blockchain. However, the p_2^V cannot initiate a request to query the content of the previous data block in G channel blockchain.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.6 Assume that p_3^G is not Sp_i^G, p_2^V is Sp_i^V, and they are all attacked as insecure nodes at the same time. Combining the experiment results of Exp 2 and Exp 3, the following data will be leaked: 1. except the pair of homomorphic encryption key and n pairs of node key generated by the current cycle; 2. the

TABLE 5. The user privacy sensitive data can be accessed by insecure nodes.

Indicator	Threatened nodes	Threatened nodes sensitive data	Data form	Threatened G channel sensitive data	Data form
Exp 1	$\underline{\underline{Sp_i^G}}$, other all p_i^G	1. the current n transaction sets of home sensitive data 2. historical transaction data	ciphertext	historical transaction data in G channel	ciphertext
Exp 2	$\underline{\underline{p_3^G}}$	the smart home terminal information of p_3^G	plaintext	the previous block transaction information in G channel	ciphertext
Exp 3	$\underline{\underline{Sp_i^V}}$, Sp_i^G, other all p_i^G	1. the current n transaction sets of home sensitive data 2. historical transaction data	ciphertext	historical transaction data in G channel	null
Exp 4	$\underline{\underline{p_2^V}}$	null	null	null	null
Exp 5	$\underline{\underline{p_3^G}}$, $\underline{\underline{p_2^V}}$	the smart home terminal information of p_3^G	ciphertext	the previous block transaction information in G channel	ciphertext
Exp 6	$\underline{\underline{p_3^G}}$, $\underline{\underline{Sp_i^V}}$, Sp_i^G, other all p_i^G	1. the current n transaction sets of home sensitive data 2. historical transaction data 3. the smart home terminal information of p_3^G	ciphertext	the previous block transaction information in G channel	ciphertext
Exp 7	$\underline{\underline{Sp_i^G}}$, $\underline{\underline{p_2^V}}$, other all p_i^G	1. the current n transaction sets of home sensitive data 2. historical transaction data	ciphertext	all block transaction information in G channel	ciphertext
Exp 8	$\underline{\underline{Sp_i^G}}$, $\underline{\underline{Sp_i^V}}$, other all nodes	all transaction data in all nodes	plaintext	all block transaction information in G channel	plaintext

previous encrypted block information in G channel blockchain; 3. the previous homomorphic encryption private key hk_i^S and the n node public keys gk_i^P in V channel blockchain; 4. the smart home terminal information collected by p_3^G itself and the previous encrypted block information in G channel blockchain are also leaked. However, these data are encrypted.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.7 Assume that p_3^G is Sp_i^G, p_2^V is not Sp_i^V, and they are all attacked as insecure nodes at the same time.

Combining the experiment results of Exp 1 and Exp 4, the following data will be leaked: 1. the all encrypted block information in G channel blockchain; 2. the homomorphic encryption public key hk_i^P and the n node private keys gk_i^S of current period; 3. all key data in V channel blockchain. However, these available data are also encrypted.

In this case, the attack has no effect on the sensitive smart home data protected in this model.

Exp.8 Assume p_3^G is Sp_i^G, p_2^V is Sp_i^V, and they are all attacked as insecure nodes at the same time.

Combining the experiment results of Exp 1 and Exp 3, by using the homomorphic encryption key and the node keys of all time periods (the intruder will use other means of communication in the network to enable p_3^G and p_2^V to communicate and transmit the important key), all encrypted block information and all the encrypted smart home sensitive data in G channel blockchain can be decrypted. However, the probability of this situation is extremely low. The reason is that, on the premise of the security protection of blockchain itself, the HCB-SDPP will carry out stricter supervision on all verification nodes p_i^V and V channel.

In this case, the attack has very weak influence on the sensitive smart home data protected in this model.

Based on the discussion above, once the model is attacked, resulting in the nodes being captured and becoming insecure, different keys will be disclosed under different attack conditions. What's worse, these insecure nodes can pose a threat to other normal nodes. There is a certain probability for insecure nodes to obtain privacy and sensitive data on other nodes and G channel blockchain. According to above analysis of Exp 1-8, insecure nodes are serious threats to normal nodes safety. Users' data obtained by insecure nodes are now summarized in TABLE 5, in which the attacked set of nodes in design Exp 1-8 are highlighted by underscores.

B. MODEL PERFORMANCE ANALYSIS

In this section, we analyze the performance of the HCB-SDPP from five aspects based on the attack experiments.

1) DATA SECURITY

In the experiment, the smart gateway p_i^G performs Paillier encryption, and private key signature on the collected local source data. Then it forwards them in the form of ciphertext packets in blockchain network. If the key is intercepted during distribution, it is difficult for an external network attack to obtain p_i^G privacy information, because it cannot pass the verification of verification node p_i^V. However, for an intranet attack, such as when p_i^G is captured by a malicious program, there are two situations: 1) if it is an ordinary p_i^G, privacy information cannot be obtained because the original p_i^G cannot be obtained; 2) if it is a p_i^V, the consensus of p_i^V set must be completed before it can be obtained. According to the Byzantine consensus mechanism, this consensus needs to be supported by more than 2/3 of the nodes, meaning that an attack must conquer 2/3 of p_i^V, which is almost impossible in terms of probability. Therefore, the method in this paper can largely guarantee the security of data.

2) DATA AVAILABILITY

This paper uses HEBDS structure for block organization. Since Consortium Blockchain technology has the characteristics of tamper-proof, permanent, decentralized and open, each p_i^G can obtain this permanent database by synchronizing the chain block after the block is formed. Among them, PD data can be directly obtained and calculated from the chain block. The SD data involving privacy can be counted, accumulated and other homomorphic calculations. Corresponding results can be obtained after authorization without damaging the privacy of data set.

3) COMPUTABILITY AND SHARABILITY

In the above experiments, all kinds of privacy data processed by Paillier algorithm are distinguished according to different families and different indicators. The encrypted result set is refined to the index level in terms of data granularity, which can be used to select subsets for nodes that need data processing and calculation, or to conduct statistical calculation according to different purposes. Since ciphertext data does not involve personal privacy, sharing, copying and distribution of data will not affect the disclosure of privacy.

4) SYSTEM ROBUSTNESS

As the model is supported by the Consortium Blockchain technology, when one node fails, other nodes will not be affected. Single point failure is avoided by spreading the workload to the network. In addition, the decentralized storage, non-tampering, strong timing and public verification features of Consortium Blockchain enable each p_i^G to participate in calculation and verification process of the whole system. This improves the computational power of the system, and also enhances the robustness of the system

5) STORAGE SECURITY

The HCB-SDPP creates G channel among the various smart gateway p_i^G, and p_i^G join G channel. A common ledger in G channel constitutes a blockchain, which is maintained by all p_i^G that join G channel. The information collected by the smart gateway node p_i^G is packaged into blocks and stored in this blockchain. The p_i^G added to G channel can query and access the data, and the nodes outside G channel cannot do anything with the data inside it.

Verification nodes are mainly responsible for the management (distribution, revocation, etc.) of all certificates in HCB-SDPP network, and provide identity information based on digital certificates to all nodes in the network. The verification nodes can generate or cancel identity certificate of the member node. On the basis of the clear identity of the member node, addition of p_i^V service can realize the management function of authority control for HCB-SDPP model, allowing new nodes to join the organization or allowing new nodes or organizations to join the network.

In addition, the block header part of the HEBDS adds an information compared with the original blockchain pk_b. This information mainly records public key used by the block in DT Paillier encryption, so that the real information can be viewed later. This method of first encrypting and then hashing enhances the protection of privacy data and further prevents the disclosure of privacy data.

VI. CONCLUSION

In this paper, we constructed a modified SHS model. Based on this model, we mapped this model to the consortium blockchain architecture. We also proposed the HCB-SDPP model. By performing Paillier encryption on the users' personal health data or status data of smart devices, privacy protection was provided for the modified SHS under the Consortium Blockchain framework. We verified the effectiveness of this scheme by analysis of simulation results, and the security of the scheme by performing attack experiments and analysis. However, there is still a need for considerable further research in this area. For example, the smart contract in the HCB-SDPP model needs to be further extended to meet the higher requirements of the more prevalent SHS. In the future, we will do more in-depth research on these aspects.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their critical and constructive comments and suggestions.

REFERENCES

[1] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *Proc. Int. Symp. Consum. Electron. (ISCE)*, Jun. 2015, pp. 1–2.

[2] T. Qiu, R. Qiao, D. O. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[3] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018. doi: 10.1016/j.jii.2018.01.005.

[4] P. Yadav, A. Mittal, and H. Yadav, "IoT: Challenges and issues in Indian perspective," in *Proc. 3rd Int. Conf. Internet Things (IoT-SIU)*, Feb. 2018, pp. 1–15. doi: 10.1109/IoT-SIU.2018.8519869.

[5] T. Qiu, X. Liu, K. Li, Q. Hu, A. K. Sangaiah, and N. Chen. "Community-aware data propagation with small world feature for Internet of vehicles," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 86–91, Jan. 2018.

[6] Y.-F. Kung, S.-W. Liou, G.-Z. Qiu, B.-C. Zu, Z.-H. Wang, and G.-J. Jong, "Home monitoring system based Internet of Things," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 325–327. doi: 10.1109/ICASI.2018.8394599.

[7] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.

[8] B. Y. Su, G. J. Wang, and J. Zhang, "Smart home system based on Internet of Things and Kinect sensor," *J. Sci. Technol.*, vol. 44, pp. 181–184, Oct. 2013.

[9] A.R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A smart home energy management system using IoT and big data analytics approach," *IEEE Trans. Consum. Electron.*, vol. 63, no. 4, pp. 426–434, Nov. 2017. doi: 10.1109/TCE.2017.015014.

[10] R. A. Ramlee, M. A. Othman, M. H. Leong, M. M. Ismail, and S. S. S. Ranjit, "Smart home system using Android application," in *Proc. Int. Conf. Inf. Commun. Technol. (ICoICT)*, Mar. 2013, pp. 277–280.

[11] D. Geneiatakis, I. Kounelis, R. Neisse, I. N. Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2017, pp. 1292–1297.

[12] A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman, and A. Vishwanath, "Low-cost flow-based security solutions for smart-home IoT devices," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Nov. 2016, pp. 1–6.

[13] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Sep. 2016, pp. 147–156.

[14] C. H. Kuo, C. J. Wu, H. C. Chou, G. T. Chen, and Y. C. Kuo, "Development of a blood pressure measurement instrument with active cuff pressure control schemes," *J. Healthcare Eng.*, vol. 2017, Mar. 2017, Art. no. 9128745.

[15] M. Salai, I. Vassányi, and I. Kósa, "Stress detection using low cost heart rate sensors," *J. Healthcare Eng.*, vol. 2016, Mar. 2016, Art. no. 5136705.

[16] Y. Fang, Z. Jiang, and H. Wang, "A novel sleep respiratory rate detection method for obstructive sleep apnea based on characteristic moment waveform," *J. Healthcare Eng.*, vol. 2018, Jun. 2018, Art. no. 1902176.

[17] M. Pilkington, *Blockchain Technology: Principles and Applications*. Rochester, NY, USA: Social Science Electronic Publishing, 2016.

[18] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://nakamotoinstitute.org/bitcoin

[19] M. Swan, *Blockchain: Blueprint for A New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

[21] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, Sep. 2017. doi: 10.1109/MC.2017.3571045.

[22] F. M. Ametrano, *Bitcoin, Blockchain, and Distributed Ledger Technology*. Rochester, NY, USA: Social Science Electronic Publishing, 2016.

[23] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 51–55. doi: 10.1109/WF-IoT.2018.8355182.

[24] P. Urien, "Blockchain IoT (BIoT): A new direction for solving Internet of Things security and trust issues," in *Proc. 3rd Cloudification Internet Things (CIoT)*, Jul. 2018, pp. 1–4. doi: 10.1109/CIOT.2018.8627112.

[25] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Aug. 2018. doi: 10.1109/MCC.2018.043221010.

[26] T. C. Shen, *Blockchain Development Guide*. Thiruvanmiyur, India: Machinery Industry Press, 2017, pp. 6–8. [Online]. Available: https://www.ionixxtech.com/blockchain-guide

[27] F. K. Maurer, T. Neudecker, and M. Florian, "Anonymous CoinJoin transactions with arbitrary values," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 522–529.

[28] Y. Pang and G. M. Li, "Study on smart home based on Zigbee," (in Chinese), *Comput. Eng. Des.*, vol. 35, no. 5, pp. 1547–1550, 2014.

[29] N. Zhang, Y. Wang, C. Q. Kang, J. G. Cheng, and D. W. He, "Blockchain technique in the energy Internet: Preliminary research framework and typical applications," in *Proc. CSEE*, Aug. 2016, pp. 4011–4022.

[30] Y. Yuan and F. Y. Wang, "Blockchain: The state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, Apr. 2016.

[31] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Newton, MA, USA: O'Reilly Media, 2014.

[32] C. Gentry, "Fully homomorphic encryption using ideal lattices," *STOC*, vol. 31, no. 9, pp. 169–178, May 2009.

[33] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–179, 1978.

[34] S. D. Li, J. W. Dou, and D. S. Wang, "Survey on homomorphic encryption and its applications to cloud security," *J. Comput. Res. Develop.*, vol. 52, no. 6, pp. 1378–1388, 2015.

[35] P. Paillier, "Public-key cryptosystems based on composite degree Residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Apr. 1999, pp. 223–238.

[36] G. Zhao, L. Xing, Q. Zhang, and X. Jia, "A hierarchical combinatorial reliability model for smart home systems," *Int. Qual. Reliability Eng.*, vol. 34, no. 1, pp. 37–52, Feb. 2018.

WEI SHE received the B.S. degree in control engineering from Air Defence Academy of PLA, in 2000, the M.S. degree in software engineering from Hunan University, in 2008, and the Ph.D. degree in computer software and theory from Zhengzhou University, China, in 2013, where he is currently an Associate Professor with the Software College. His research interests include information security, the energy Internet, and the Internet healthcare.

ZHI-HAO GU received the B.S. degree from Zhengzhou University, China, in 2016, where he is currently a Graduate Student. His research interest includes information security.

XU-KANG LYU received the Ph.D. degree in computer science from the University of Memphis, Memphis, TN, USA, in 2011. He was a System Specialist at the Advanced Computing Center for Research and Education, Vanderbilt University, from 2012 to 2013. He is currently an Assistant Professor with Tianjin University. His research interests include big data, cloud computing, AI/ML, high-performance networking, and transport protocols.

QI LIU received the B.S. degree from Zhengzhou University, China, in 2016, where she is currently a Graduate Student. Her research interests include information security and Petri net theory.

ZHAO TIAN received the B.S. degree in information and computing science from Huazhong Agricultural University, in 2008, the M.S. degree in computer software and theory from Zhengzhou University, in 2011, and the Ph.D. degree in safety technology and engineering from Beijing Jiaotong University, in 2016. He is currently a Lecturer with the Software College, Zhengzhou University. His research interests include information security, artificial intelligence, and intelligent transportation.

WEI LIU received the B.S. and M.S. degrees in information engineering from Zhengzhou University, China, in 2003 and 2008, respectively, and the Ph.D. degree from Tohoku University, Japan, in 2013. He is currently an Associate Professor with the Software College, Zhengzhou University. His research interests include information security, wireless mesh networks, and the Internet healthcare.