

# Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT

Junyu Ren, Jinze Li, Huaxing Liu, and Tuanfa Qin\*

**Abstract:** With the rapid advancement of the Internet of Things (IoT), the typical application of wireless body area networks (WBANs) based smart healthcare has drawn wide attention from all sectors of society. To alleviate the pressing challenges, such as resource limitations, low-latency service provision, mass data processing, rigid security demands, and the lack of a central entity, the advanced solutions of fog computing, software-defined networking (SDN) and blockchain are leveraged in this work. On the basis of these solutions, a task offloading strategy with a centralized low-latency, secure and reliable decision-making algorithm having powerful emergency handling capacity (LSRDM-EH) is designed to facilitate the resource-constrained edge devices for task offloading. Additionally, to well ensure the security of the entire network, a comprehensive blockchain-based two-layer and multidimensional security strategy is proposed. Furthermore, to tackle the inherent time-inefficiency problem of blockchain, we propose a blockchain sharding scheme to reduce system time latency. Extensive simulation has been conducted to validate the performance of the proposed measures, and numerical results verify the superiority of our methods with lower time-latency, higher reliability and security.

**Key words:** wireless body area networks (WBANs), healthcare IoT; software-defined networking (SDN); fog computing; blockchain; task offloading; blockchain sharding

## 1 Introduction

With the advancement of wireless sensor networks (WSNs), the Internet of Things (IoT) has undergone

- Junyu Ren is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, China; Guangxi University, Xingjian College of Science and Liberal Arts Nanning 530004, China, and also with Guangxi Key Laboratory of Multimedia Communications and Network Technology, Guangxi University, Nanning 530004, China. E-mail: junyuren@yeah.net.
- Jinze Li and Tuanfa Qin are with Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China. E-mail: li\_jinze@126.com; tfqin@gxu.edu.cn.
- Huaxing Liu is with the Faculty of Earth Sciences & Geography, Trinity College, University of Cambridge, Cambridge, CB21TN, UK. E-mail: harris@cambridge.social.

\* To whom correspondence should be addressed.

Manuscript received: 2021-05-25; accepted: 2021-07-08

rapid development and played a vital role in many aspects of society. By providing autonomous support for communications and operations in the real world, it has initiated extensive novel services in industry and academic fields. It has promised to bring prominent advantages through increased connectivity to cyber-physical systems<sup>[1]</sup>. The IoT has boosted the emergence of new trends, such as smart healthcare, smart grids, smart cities, and smart nations in recent years<sup>[2, 3]</sup>. As a typical application of the IoT in the field of smart healthcare, wireless body area networks (WBANs) based healthcare has been rapidly developed by the IoT and has gained wide-spread attention from all sectors of society. Despite the great progress it has achieved, the IoT suffers from potential bottlenecks, such as resource limitations, mass data processing, lack of a central controller and cyber-attacks<sup>[4]</sup>, which calls for novel network paradigm.

Because of the high time-sensitivity of human

physiological parameters gathered by WBANs, a practical healthcare IoT system should have high capability in real-time service provision, especially in critical situations. If the emergency data cannot be processed timely, the rapid diagnosis and decision-making of the doctors will be impacted, thereby bringing great risk to the health and safety of the patients and even endangering their lives in severe cases. This situation has posed a great challenge to the low-latency implementation of the smart healthcare system. Additionally, because of the rigid security demands of smart healthcare applications, powerful measures should be explored to protect the privacy and the security of physiological data. In fact, a novel network paradigm with features such as high confidentiality, privacy, flexibility, scalability, reliability, and energy-efficiency, as well as low-latency is required for smart healthcare system.

The challenge of resource limitations and low-latency mass data processing can be alleviated by fog computing, which is a form of edge computing to extend the cloud computing and storage capacity to the network edge. By computation offloading, fog computing can provide computationally intensive task processing with low latency for time-sensitive healthcare IoT applications<sup>[5-7]</sup>.

On the other hand, by leveraging the new networking paradigm of software-defined networking (SDN), all the network infrastructures can be combined and managed by the centralized controller responsible for decision-making, policy enforcement, and intelligent management in a flexible and dynamic matter. Benefiting from the global view of the whole network, the SDN controller can provide optimal network services, such as higher-level security, intelligent management, and optimal resource scheduling, and has become a promising solution to manage and secure large-scale IoT networks<sup>[8]</sup> that can be well explored in a healthcare IoT system to eliminate the challenge of lacking a central network entity.

Regarding the rigid security demand of smart healthcare systems, the powerful security measure of blockchain can be used to protect data confidentiality, privacy, and resource availability against untrusted users<sup>[9]</sup>. Blockchain is essentially a decentralized hyper-ledger that can realize the distributed and secure storage of data based on peer-to-peer (P2P) technology without the need for third-party trust entities, thereby efficiently preventing data tampering and realizing traceability, integrity, confidentiality, and secure sharing of data.

By employing distributed consensus algorithms, such as proof-of-work (PoW), the consistency of the data can be well ensured. Furthermore, blockchain can also guarantee data privacy through access control rules to ensure that only those with authority view information or make changes<sup>[10]</sup>. Blockchain has gained widespread popularity in IoT applications, and is a promising solution to the pressing challenges of trust, confidentiality, integrity, and privacy for the healthcare IoT system<sup>[10]</sup>.

Inspired by these developments, in this work, we first recommend a new network framework leveraging fog computing and the novel networking paradigm of SDN to address the mentioned pressing challenges of the healthcare IoT system. In particular, we have proposed a centralized decision-making algorithm executed by the SDN controller for task offloading by resource-constrained healthcare IoT edge devices. Next, a comprehensive blockchain-based two-layer and multidimensional security scheme is designed to well ensure the security of the SDN and fog-empowered smart healthcare system. Furthermore, to tackle the inherent time-inefficiency problem of blockchain, the blockchain sharding strategy is proposed for the fog layer blockchain (BottomChain). The main contributions of this paper can be summarized as follows.

(1) To address the pressing challenges of the healthcare IoT system, we first recommend a hierarchy network framework with centralized control and distributed computing for the promising smart healthcare IoT applications based on WBANs, which is composed of three layers, viz., the control layer, the fog layer, and the data layer, wherein the control layer can provide centralized and optimal network control and management and resource scheduling, the fog layer incorporates with the other two layers to provide the capacity of mass data and computationally intensive task processing with low latency, and the data layer composed of healthcare IoT edge devices (WBANs gateway devices) is responsible for aggregating human physiological data captured by the body sensors.

(2) We propose a task offloading strategy with a low-latency, secure and reliable decision-making algorithm with emergency handling capacity (LSRDM-EH) to determine the optimal fog node for task offloading by jointly considering the time-efficiency, security, and reliability demands of WBANs-based healthcare IoT systems, and make full use of the powerful and centralized control ability of SDN controllers to diminish

the challenge of resource-constrained edge devices in processing computationally intensive tasks. On the basis of the dynamic information collected from the network, the SDN controllers can intelligently make globally optimized decisions on scheduling the optimal fog node for reliable, secure, and low-latency task processing. Because of the resource limitations, when having computationally intensive tasks to offload, the edge devices initiate service requests to the corresponding controller to allocate optimal fog nodes for task processing.

(3) We propose a comprehensive blockchain-based two-layer and multidimensional security scheme with one TopChain (Fig. 1) deployed in the control layer to secure the vital decision-making results and the SDN inter-domain signaling, and numerous BottomChains in the fog layer to ensure the security of task-respective information and intra-domain signaling. In addition, to further improve the system security and efficiency, we also consider the potential misbehaviors of edge devices. In particular, we design a trust evaluation method for the edge devices implemented by the SDN controller, and a corresponding blacklist scheme stored and secured by the TopChain.

(4) To solve the inherent time-inefficiency problem of blockchain, we propose to use the effective blockchain sharding approach within the BottomChain. Differing from prior works, we shard the BottomChains by the organization (SDN domain) in case of privacy disclosure.

(5) Extensive simulation has been conducted to validate the performance of the proposed strategies,

namely, the decision-making algorithm LSRDM-EH, the blockchain-based two-layer and multidimensional security mechanism, and the proposed blockchain sharding scheme. Numerical results prove the effectiveness and superiority of the methods in time-efficiency, reliability, and security.

The remainder of this paper is organized as follows. In Section 2, we review the related works, and in Section 3, we present the system model and formulate the problem. Section 4 details the proposed centralized decision-making algorithm of the SDN controller for task offloading, and the blockchain-based two-layer and multidimensional security strategy is illustrated in Section 5. Numerical simulations and results are presented in Section 6, and finally, Section 7 concludes the paper.

## 2 Related Works

A few state-of-the-art works adopting the advanced solutions of fog computing, SDN, and blockchain have been conducted in the field of healthcare. In this section, we review and discuss the prior works on fog-cloud-assisted WBANs, blockchain-empowered WBANs, and SDN-enabled healthcare.

### 2.1 Fog-cloud-assisted WBANs

Great effort has been devoted to adopting cloud computing to assist the storage<sup>[11, 12]</sup>, analysis, and processing of human physiological big data<sup>[13, 14]</sup>. Moulik et al.<sup>[15]</sup> proposed to realize the effective allocation of cloud resources by using game theory

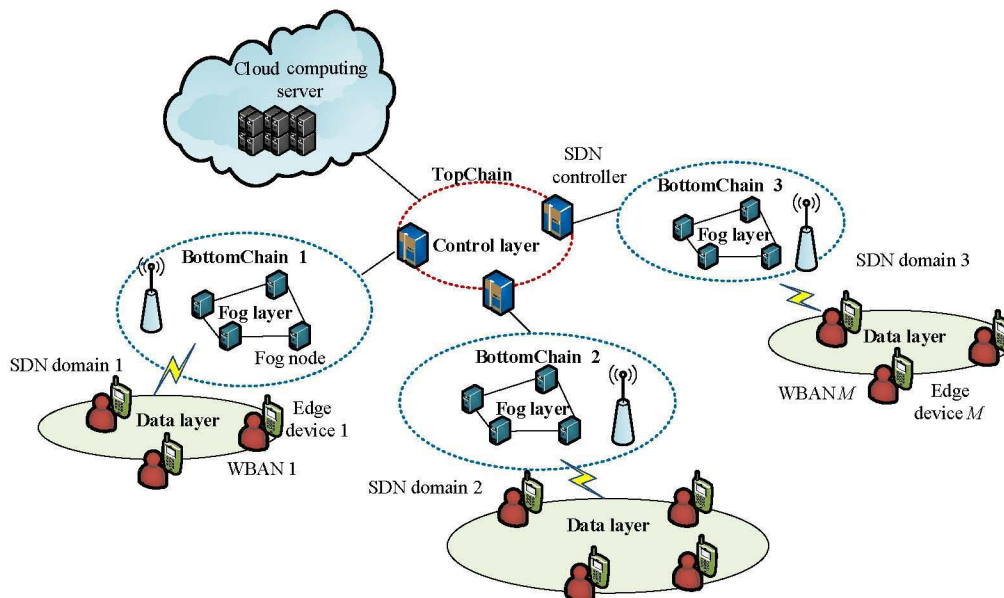


Fig. 1 Network model.

and price mechanisms in a WBANs environment. Almashaqbeh et al.<sup>[16]</sup> proposed a cloud-based telemedicine monitoring system enabling patients to track their physical health status conveniently without affecting their normal daily life. Regarding the high latency of cloud computing, fog computing is introduced to meet the low-latency requirement of delay-sensitive IoT applications<sup>[17]</sup>. Existing studies have attempted to combine cloud and fog computing to solve problems of healthcare applications, such as Ref. [18], wherein the authors focused on improving the system time efficiency, especially for critical patients. According to the critical value of human physiological parameters, the local processing unit adopts game theory to determine whether to transmit data to the cloud or the fog. Gia et al.<sup>[19]</sup> studied the feature extraction problem of human physiological parameters, whereby fog computing is integrated into the smart gateway for ECG feature extraction to obtain faster system response, and mathematical analysis indicates that with the number of real-time applications increasing, the fog computing paradigm outperforms traditional cloud computing in terms of time-latency, energy efficiency, CO<sub>2</sub> emission and cost<sup>[5]</sup>.

## 2.2 Blockchain-empowered WBANs

The security-by-design nature of blockchain makes it extremely powerful in immutability, non-repudiation, and anti-tamper capacity; therefore, it can be well explored to ensure system security. Some state-of-the-art works use blockchain to secure data storage, e.g., Zhang and Lin<sup>[20]</sup> explored both privated and consortium blockchains to ensure secure sharing of human health data. Wang et al.<sup>[10]</sup> employed blockchain to provide secure storage and transmission of medical data for the WBANs-based eHealthcare systems. Xiao et al.<sup>[21]</sup> proposed the use of a private chain to store the registration data of sensor nodes and the physiological data of WBANs. Although they all consider the secure storage of health data using blockchain, while none of these works is designed for the SDN-based healthcare IoT systems; therefore, they are not applicable to the proposed SDN-based networking framework, where not only the human data but also the vital SDN inter- and intra-control signaling and other crucial information, including the task-respective information and decision-making results, should also be secured to ensure the security of the entire system. Furthermore, none of these works considers the inherent time-inefficiency problem

of blockchain, such as in our work.

## 2.3 SDN-enabled healthcare

The challenge of lacking a centralized control entity in traditional IoT systems can be alleviated by employing the novel network framework of SDN to provide centralized and flexible control and management of the IoT devices<sup>[9]</sup>. Cicioğlu and Cihan<sup>[22]</sup> incorporated SDN into WBANs to exploit the centralized SDN controller to reduce the workload of WBANs gateway devices. For the network control inefficiency problem and to provide priority support for emergency data, Hasan et al.<sup>[23]</sup> proposed novel SDN-based network architecture to efficiently manage application-specific traffics in WBANs. Cicioğlu and Cihan<sup>[24, 25]</sup> developed an efficient routing mechanism using SDN in WBANs. Varadharajan et al.<sup>[26]</sup> presented an SDN-based framework for secure monitoring of patients in hospital environments. The proposed approach can provide fine granular security policies for communications and can well track the locations of patients with wandering behavior. Confronted with the potential security issues of SDN, Meng et al.<sup>[27]</sup> applied trust-based method to resist insider attacks in SDN-based medical environments. Although the proposed approach can effectively detect malicious healthcare devices, it is not designed for WBANs-based systems, and only works well for resisting network insider attacks but not for outsider attacks. Few pioneering works employ both SDN and blockchain to tackle security and other issues. Yazdinejad et al.<sup>[28]</sup> explored SDN and blockchain to balance the need for security and energy-efficiency of IoT networks, while this study is not for smart healthcare and offloading scenarios, in contrast to our work.

## 3 System Model and Problem Formulation

### 3.1 Network model with blockchain security

Suppose there are  $N$  fog nodes,  $M$  WBANs and multiple SDN controllers in the healthcare IoT system, as shown in Fig. 1. The whole network is composed of three layers, namely, the data layer, the fog layer, and the control layer.

(1) **Data layer:** For the convenience of monitoring the physical conditions, as well as gathering the physiological parameters of the human body, each patient is equipped with a WBAN comprising diverse body sensors implanted in, placed on or around



the human body to capture physiological parameters, such as temperature, pulse rate, blood oxygen levels, blood pressure, electrocardiogram (ECG), and electroencephalogram (EEG)<sup>[29]</sup>. The collected health data are then sent to the data layer WBANs gateway (edge) devices that are typically mobile phones for data aggregation, preprocessing, and fusion. When the resource-constrained devices have computationally intensive tasks to offload, they first request the corresponding SDN controller in the domain to assign the optimal fog node for task processing. Note that, the WBANs edge devices are also lightweight nodes in the BottomChains that only initiate and verify transactions (services) without participating in the resource-consuming consensus processes because of their limited resources.

**(2) Fog layer:** The fog layer is partitioned into distinct SDN domains, each comprising numerous fog nodes possessing powerful computation and storage resources cooperating with the SDN controllers and the data layer edge devices to provide real-time and low-latency mass data and computationally intensive task processing capacities, and serve as the blockchain peers in the corresponding BottomChain to ensure secure storage of human health data and task-respective information, as well as SDN signaling. Each SDN domain under the management of one or more SDN controllers should be affiliated with one organization, such as a hospital, a rehabilitation center, or a sanatorium, to ensure system security in the scenario of healthcare IoT, as organizations are reluctant to share their privacy-sensitive human health data in case of privacy disclosure. To simplify analysis and make the work more concentrated, we suppose that each domain is only equipped with one controller. Without loss of generality, the scheme could be easily extended to more application scenarios, e.g., to further enhance system time-efficiency, consensus peers in each domain could be further divided into multiple subdomains by department or other policies, whereby there would be multiple SDN controllers in one organization, and the controllers elected as representatives of the domain can then act as consensus peers in the TopChain. Additionally, the fog nodes subordinated to the same domain are also the consensus peers of the corresponding BottomChain, i.e., there is a one-to-one map between an SDN domain and a BottomChain.

**(3) Control layer:** The controller of each domain makes up the control layer. By continuously monitoring

and scanning the overall network information, the SDN controller possesses the global view of the network and can optimize network resource scheduling to improve system efficiency. The updated information collected is stored in the relevant database of the controller and would be refreshed periodically or as needed in an inquire-response manner greatly benefiting the system to adapt to the dynamic network environment. According to the distinct service requirements initiated by the data layer edge devices, the controller would command the fog layer for service provisions.

### 3.2 Problem formulation

Constrained by limited energy and computational resources, healthcare IoT edge devices process big data and execute computationally intensive tasks with great difficulty, so we leverage fog computing having powerful computation and storage capacity to diminish the challenge. Specifically, when the edge device has computationally intensive tasks to process, it would initiate service requests to the SDN controller to assign fog nodes for task processing. Therefore, the decision-making scheme of the controller plays a vital role in the design that greatly impacts the network performance. Hayajneh et al.<sup>[30]</sup> proposed a data delivery protocol for fog-assisted WBANs, wherein the WBANs devices aim to select fog nodes with low delay and high reliability for delivering data while neglecting the high delay-sensitivity of healthcare IoT, especially on emergency occasions, causing the method not applicable for emergency situations, especially those with rigid task deadlines. Differing from that, in this work, based on joint optimizing the system-reliability and time-efficiency, we also fully consider the critical task deadline when conducting the decision-making process on the optimal target fog node, especially in emergency cases.

On the other hand, despite the great benefits SDN brings, it also incurs problems, such as the severe single-point failure owing to the vital role the SDN controller plays, making it more vulnerable to malicious attacks. Moreover, SDN cannot generally prevent insider attacks on the system<sup>[31]</sup>. To address these challenges, we explore the powerful security method of blockchain to ensure the security of the entire system. Specifically, we have designed the TopChain in the control layer to tackle the severe single-point failure problem of SDN and to protect the security of the cross-domain signaling and the decision-making results of the SDN controllers.

Furthermore, we also design BottomChains in the fog layer to protect the security of the intra-domain signaling and task-respective information. Additionally, to resist the potential misbehaviours of fog nodes, we also use the nodes' reputation value, which can well reflect their historical behavior in the long run, to readily recognize and exclude misbehaving nodes to guarantee the network efficiency and security, and to further diminish security risks of insider attacks.

Despite the great advantages of blockchain, it suffers from the inherent problem of time-inefficiency, which should be fully considered for time-sensitive healthcare IoT applications. Most recently, some pioneering works exploited blockchain sharding to tackle the problems of time-inefficiency and poor throughput to improve the scalability of a blockchain system<sup>[32,33]</sup>. However, these methods are mostly designed for the blockchain-enabled currency<sup>[32,33]</sup>; therefore, they cannot be directly applied to SDN-based healthcare IoT systems. Moreover, the blockchain peers are usually randomly distributed into different sub-blockchains under the schemes<sup>[32-34]</sup>, which cannot be applied to the SDN-based healthcare IoT system as proposed in our work. Because the fog nodes deployed by the same organization or operator are logically assigned to one same SDN domain, randomly dividing them into different blockchains is obviously not applicable. Liu et al.<sup>[34]</sup> also employed the blockchain sharding approach in an SDN-based system, whereas they merely applied blockchain to the control layer and only focused on tackling the blockchain inefficiency problem of the SDN control layer rather than that of the data layer.

Differing from the above works, we employ blockchain in the control layer and data layer to well ensure the security of the entire system, and apply the blockchain sharding technique in the fog layer blockchain (BottomChain) to tackle the time-inefficiency problem. Furthermore, to balance the conflicts between efficient network management and the data security of different SDN domains, the BottomChain is further divided into multiple BottomChains, and the consensus peers of each BottomChain are no longer randomly distributed but assigned according to their affiliation (different SDN domains), i.e., nodes that are subordinated to the same organization should be divided into the same BottomChain. Similarly, when the number of consensus nodes in one organization is too large to affect the system performance, the system should continuously run a sharding algorithm, i.e., these

consensus peers could be further divided according to a certain policy, such as by department.

## 4 Proposed Decision-making Algorithm for Task Offloading

In this section, we illustrate the task-offloading strategy in detail, including the system initialization procedure, the system working flow, and the proposed centralized decision-making algorithm implemented by the SDN controller.

### 4.1 System initialization

(1) The SDN controller initializes the resource information database  $DBS_F: \{F_j | F_j = (B_W^j, f_{CPU}^j, P_s^j, L_F^j, \varepsilon_\mu^j, S_F^j, \sigma^2 \{(C_j^l, \varepsilon_j^l) | l = 1, 2, \dots, L\} | j = 1, 2, \dots, N)\}$  for each fog node with inquiry-response manner, where  $B_W^j$  denotes the remaining bandwidth of the  $j$ -th fog node  $F_j$ .  $f_{CPU}^j$  denotes the computational capacity of  $F_j$  in Hz.  $P_s^j$  and  $L_F^j$  denote the transmitting power and the location information of  $F_j$ , respectively.  $\{(C_j^l, \varepsilon_j^l) | l = 1, 2, \dots, L\}$  indicates that a total of  $L$  tasks are queuing in  $F_j$ , each demanding the CPU resource  $C_j^l$ , with the actual allocated value being  $\varepsilon_j^l$ .  $\varepsilon_\mu^j$  denotes the CPU ratio allocated for the upcoming task, and  $S_F^j$  and  $\sigma^2$  denote the remaining storage and the background noise power of  $F_j$ , respectively.

(2) The SDN controller also establishes the WBANs edge device information database  $DBS_H: \{H_i | H_i = (p_H^i, L_H^i(t), \{I_i(k) | k = 1, 2, \dots, \Lambda\}, |i = 1, 2, \dots, M)\}$ , where  $p_H^i$  and  $L_H^i(t)$  denote the transmitting power and the location information of the  $i$ -th HUB  $H_i$ , respectively.  $I_i(\cdot)$  is an indicator function to indicate the trustworthiness of the edge device  $H_i$  assessed by the fog node based on the device's  $k$ -th service request as follows:

$$I_i(k) = \begin{cases} 1, & \text{trustworthy;} \\ 0, & \text{untrustworthy} \end{cases} \quad (1)$$

(3) The controller periodically requests the fog nodes and data layer devices to update information, and the fog nodes and the healthcare IoT edge devices respond by signaling messages.

### 4.2 System working flow

(1) Because the edge devices are resource-constrained, when the  $i$ -th edge device  $H_i$  determines to offload the task, it first broadcasts a HELLO  $(H_i, e_i, T_{exp}^i, \theta)$  message, where  $T_{exp}^i$  and  $\theta$  denote the task deadline and its acceptable price index for the requested service,

respectively.  $e_i$  is an indicator variable to indicate whether the task is urgent as defined below:

$$e_i = \begin{cases} 1, & \text{emergency;} \\ 0, & \text{non-emergency} \end{cases} \quad (2)$$

(2) On receiving the message, each fog node would first check  $\theta$  to ensure that it is acceptable, then measures the received signal strength indicator (RSSI), whereafter it sends the ECHO ( $F_j$ ,  $\text{RSSI}_j$ ,  $\pi_j$ ,  $\Omega_j$ ) message to  $H_i$ , where  $\pi_j$  and  $\Omega_j$  denote the afforded service price and the supported task scheduling policy by the  $j$ -th fog node  $F_j$ , respectively. Note that, to balance the need for performance improvement of the global system and to meet the rigid task deadline, especially on emergency occasions, different task scheduling strategies are adopted depending on the delay requirements of certain tasks. Specifically, when  $e_i = 1$  denotes the task being in an emergency situation, preemptive task scheduling is supported. Otherwise, the first-come-first-served (FCFS) strategy is followed by the fog nodes.

(3) When receiving ECHO,  $H_i$  would first establish the feasible fog set  $S_f$  comprising the fog nodes having responded previously, and record the corresponding message arrival time  $T_a^j$ . Then, it compares  $T_{\text{exp}}^i$  with  $T_a^j$  and removes the  $F_j$  with  $T_a^j > T_{\text{exp}}^i$  to update  $S_f$ . Next, it checks  $\text{RSSI}_j$  and removes  $F_j$  with  $\text{RSSI}_j < \text{RSSI}_{\text{th}}$  from  $S_f$  to ensure that the received signal strength is strong enough to guarantee the communication reliability of the network, where  $\text{RSSI}_{\text{th}}$  is the minimum threshold value for RSSI. Furthermore, it checks to ensure that  $\pi_j$  and  $\Omega_j$  are acceptable. Finally,  $H_i$  sends an REQ ( $e_i$ ,  $C_i$ ,  $D_i$ ,  $T_{\text{exp}}^i$ ,  $S_f$ ) message to the corresponding SDN controller in the domain requesting fog node assignment for task processing, where  $C_i$  is the CPU cycles needed and  $D_i$  is the data amount of the task.

(4) On receiving REQ, the controller would first retrieve the database to ensure that  $H_i$  is not blacklisted to reduce the security risk from malicious devices. Then, via QUE message, the controller would inquire the fog nodes in  $S_f$  for node information update and the fog nodes reply with REPE.

(5) After the above steps, the controller begins to proceed with the decision-making process on the target fog node  $F_t$  for task offloading with the centralized decision-making algorithm LSRDM-EH, as will be detailed in the following section. Additionally, according to the decision result, it generates the TopChain smart contract  $\text{SCT}_1$  consisting of the flow table before broadcasting it among the TopChain peers. When

consensus is reached,  $\text{SCT}_1$  will be automatically executed, and the flow table is distributed to the respective fog nodes, whereafter  $\text{SCT}_1$  is securely stored in the TopChain.

(6) On the other hand, on receiving the flow table,  $H_i$  will generate a BottomChain smart contract SCB containing the task-respective information ( $e_i$ ,  $C_i$ ,  $D_i$ ,  $T_{\text{exp}}^i$ ,  $F_t$ ,  $A_i$ ), with  $A_i$  indicating the account information of  $H_i$ , and send it to  $F_t$  to request a service provision.

(7) After verifying the transaction in  $\text{SCT}_1$ ,  $F_t$  would broadcast it within the corresponding BottomChain peers, and when consensus is reached, SCB is securely saved in the BottomChain.

(8) SCB is executed automatically with the terms of the transaction being met, i.e., with the transaction payment being received by  $F_t$ , whereafter  $F_t$  begins to process the offloaded task.

### 4.3 Trust evaluation method

As mentioned earlier, to resist security risks from cyber-attacks of the data layer edge devices and to further ensure the global security of the system, we also design a trustworthiness evaluation method herein. Specifically, when  $F_t$  has finished the task processing, it begins to initiate the trust evaluation process to determine the trustworthiness of the device according to the task information, the task processing result, and the service attributes requested. If the device is evaluated as trustable, it feeds back the EVAL message with  $I_i(k) = 1$  to the controller, otherwise with  $I_i(k) = 0$ . When receiving EVAL, the controller extracts  $I_i(k)$  and stores it in the database. Meanwhile, it computes the trustworthiness of the device  $H_i$  during the  $\lambda$ -th time interval as follows:

$$\Theta_i = \frac{\sum_{j=1}^N \sum_{k=1}^{\Lambda} I_i(k)}{\sum_{i=1}^M \sum_{j=1}^N \sum_{k=1}^{\Lambda} I_i(k)} \quad (3)$$

where  $\Lambda$  denotes the total number of evaluations fed back by the fog nodes during the  $\lambda$ -th time window toward  $H_i$ . Then, the controller computes the global trustworthiness  $\tilde{\Theta}$  of  $H_i$  as below:

$$\tilde{\Theta}_i = (1 - \varrho)\Theta_i + \varrho\Theta_{i-1} \quad (4)$$

where  $\Theta_{i-1}$  denotes the trustworthiness evaluated during the previous time interval that can well reflect the historical behavior of  $H_i$ , and  $\varrho$  is the history factor indicating the relative importance of the history trust of

the device satisfying  $0 < \varrho < 1$ . Then, the controller compares  $\tilde{\Theta}_i$  with the pre-defined trust threshold  $\Theta_{th}$  to determine the trustworthiness of the device as below:

$$I_i(\Theta) = \begin{cases} 1, & \tilde{\Theta} > \Theta_{th}; \\ 0, & \tilde{\Theta} < \Theta_{th} \end{cases} \quad (5)$$

Finally, if the device is assessed as untrustworthy, the controller backlists it for resisting the potential insider attack, meanwhile, it generates another TopChain smart contract  $SCT_2$  to securely store the ID of the blacklisted device in case of being tampered with to well ensure system security. To further clarify the system working process, we summarize it in Fig. 2.

#### 4.4 Centralized decision-making algorithm

As discussed above, the resource-constrained healthcare IoT edge devices would offload computationally intensive tasks to the fog layer for real-time and low-latency data processing after signaling interactions. The decision-making algorithm on the optimal target fog nodes is implemented by the SDN controller of the

corresponding SDN domain. In this section, we illustrate the specific decision-making procedures.

(1) The SDN controller would first compare the remaining storage space  $S_F^j$  of the  $j$ -th fog node in  $S_f$  with the data amount  $D_i$  of the task to be offloaded to ensure that the remaining storage space of the fog node is sufficient for storing the task data, and will remove the fog node with  $S_F^j < D_i$  to update  $S_f$ . Next, it computes the overall time cost of each fog node in  $S_f$  for task processing as below:

$$T_j^i = (1 - e_i) \sum_{l=1}^L \frac{C_j^l}{\varepsilon_j^l f_{CPU}^j} + \frac{D_i}{r_j^i} + \frac{C_i}{\varepsilon_\mu^{(1-e_i)} f_{CPU}^j} \quad (6)$$

where  $r_j^i$  denotes the data rate of  $H_i$  to  $F_j$  computed as follows. Note that, the return time of the task processing result is too short to consider herein.

$$r_j^i = B_W^j \cdot \log_2 \left( 1 + \frac{p_H^i \cdot H_i^j}{\sigma^2 + \sum_{k \in S_f, k \neq i} p_H^k \cdot H_k^j} \right) \quad (7)$$

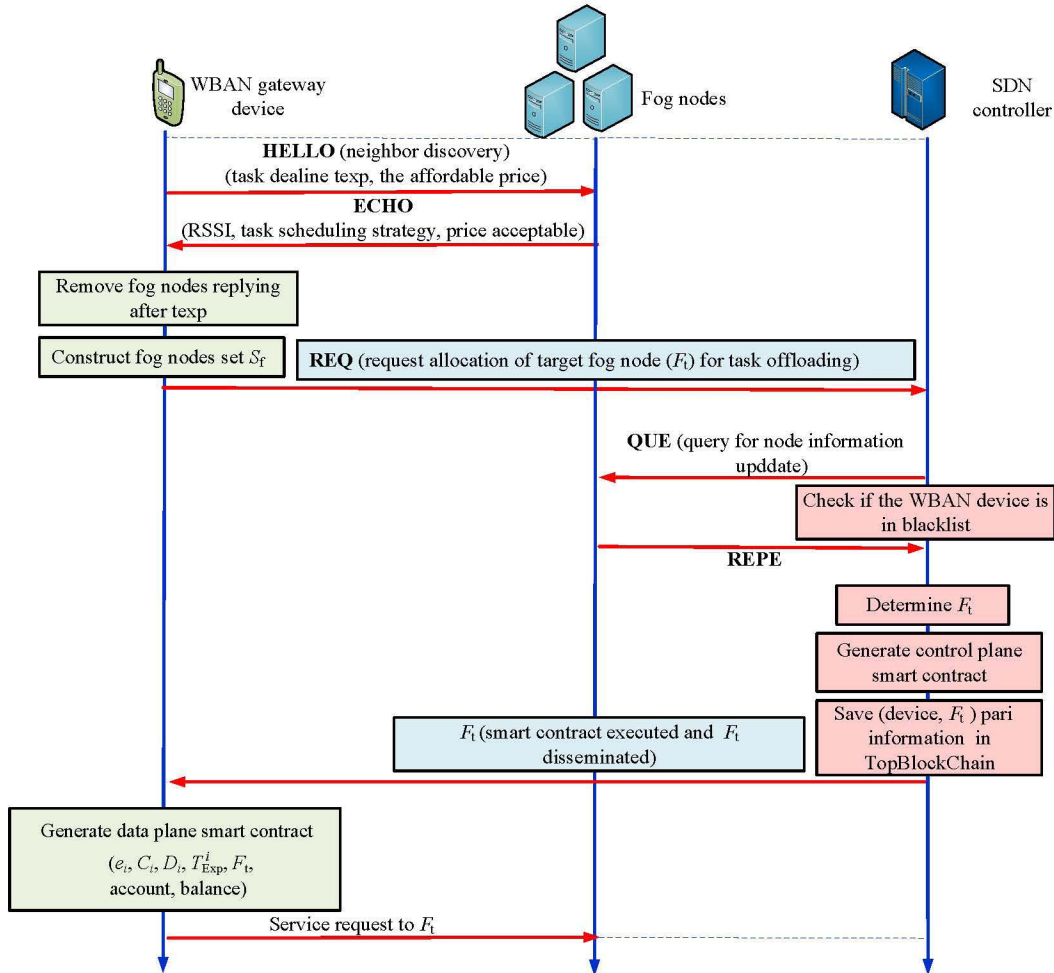


Fig. 2 Flow chart of the system signaling.



where  $H_i^j$  denotes the channel gain between  $H_i$  and  $F_j$  as below:

$$H_i^j = \mathcal{E}^j d_{ij}^{-\Gamma}, \quad d_{ij} \leq d_{\max} \quad (8)$$

where  $\mathcal{E}$  denotes the small-scale attenuation coefficient,  $d_{ij}$  denotes the distance between  $H_i$  and  $F_j$ ,  $\Gamma$  is the channel attenuation factor, and  $d_{\max}$  is the maximum communication distance of the edge device.

(2) The controller compares the total time cost  $T_j^i$  of each fog node in  $S_f$  with the task deadline  $T_{\text{exp}}$  to ensure that the total time cost of the fog node for task processing is lower than the task deadline, and removes the fog node with  $T_j^i > T_{\text{exp}}$  to update the feasible node set  $S_f$ . Next, it searches the first  $N$  minimum values, followed by a normalization step of each element as follows.

$$T_j^{i*} = \frac{T_j^i - T_{\min}}{T_{\max} - T_{\min}} \quad (9)$$

where  $T_{\min}$  and  $T_{\max}$  are the minimum and maximum values of  $T_j^i$ , respectively. Meanwhile, it updates  $S_f$  with the corresponding  $N$  fog nodes.

(3) The controller retrieves the database to obtain the reputation value  $R_j$  of each  $F_j$  in  $S_f$ , then normalizes each element as below:

$$R_j^* = \frac{R_j - R_{\min}}{R_{\max} - R_{\min}} \quad (10)$$

(4) The controller computes the fitness function of each  $F_j$  in  $S_f$  as below:

$$\begin{aligned} f(j) &= \alpha T_j^{i*} + \beta(1 - R_j^*), \\ \text{s.t. } &\alpha + \beta = 1 \end{aligned} \quad (11)$$

where  $\alpha$  and  $\beta$  are weight parameters indicating the relative importance of each decision factor. The larger the weight is, the more important the corresponding index is. Then, the controller can decide on the optimal target fog node ( $F_t$ ) as follows:

$$F_t = \arg \min_j f(j) \quad (12)$$

(5) Then, the controller can build the flow table consisting of  $H_i$ ,  $F_t$ , and the other  $N - 1$  fog nodes in  $S_f$  in order of the fitness value from smallest to largest, and distribute the table to the relative nodes, including the edge device  $H_i$  that has initiated the service, the target optimal fog node  $F_t$  for service provision and the other  $N - 1$  fog nodes to prepare as candidate nodes.

## 5 Blockchain-Based Security

In this section, we first analyze the security challenges of the system, then we illustrate the proposed comprehensive blockchain-based two-layer and multidimensional security strategy.

### 5.1 Challenge

Although authentication-based<sup>[35]</sup> approaches can be used to address security issues of the fog layer, they do not work well in cross-domain communication scenarios under the framework of SDN. Moreover, because of the curious nature of the fog nodes and the high-security sensitivity of human health data, great challenges have been posed on system security and data privacy, and how to ensure signaling and data integrity and prevent them from being tampered with should also be fully considered. Furthermore, the healthcare IoT edge devices may be untrusted or malicious such that they may selfishly initiate false claims to obtain better services, and abuse network resources and ruin the system security by launching cyber-physical attacks; therefore, effective security measures should be designed to ensure the security of the entire system.

### 5.2 Security strategy

To well address the pressing security challenges discussed above, we explore the advantage of blockchain and propose a comprehensive blockchain-based two-layer and multidimensional security strategy as indicated in Fig. 1. Benefiting from strong security power, such as non-repudiation and anti-tampering of blockchain, the confidentiality, privacy, and integrity of the body data can well be ensured. In the following, we analyze and summarize the proposed blockchain-based security measure.


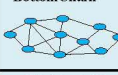

On one hand, regarding the control layer, we have designed a three-fold blockchain security mechanism, viz., TopChain, to ensure security, whereby potential malicious behaviors of the SDN controllers can be effectively resisted to ensure the control layer security. In particular, when completing the decision-making process, the SDN controller would disseminate the decision result to the respective fog nodes of the corresponding control domain including the optimal target fog node ( $F_t$ ), to process the offloaded task and other candidate fog nodes to securely store the results in the TopChain after consensus is reached. Next, we have designed a blacklist scheme to resist the potential threats from untrusted and malicious data layer edge devices, whereby the TopChain is used to secure the blacklist from tampering. Specifically, when a WBANs device initiates a service (task-offloading) request, the SDN controller (TopChain consensus peer) would first check to ensure that it is not blacklisted to resist the potential security risk. Furthermore, cross-domain signaling under

the SDN framework can also be well secured by the TopChain.

On the other hand, with regard to the fog layer, a blockchain-based three-fold security mechanism, viz., BottomChain, is designed, whereby not only the original task and data information but also the task processing results would be securely stored to resist tampering attack and nodes repudiation. Additionally, the security of the intradomain signaling is also well guaranteed by the BottomChains. Accordingly, we can conclude that the proposed security scheme is comprehensive and powerful in immutability, non-repudiation, and anti-tamper capability and in resisting outsider and insider attacks. To make the security strategy clearer, we summarize it in Fig. 3.

### 5.3 Blockchain sharding

Although the proposed blockchain-based system can provide powerful security, it also suffers from the inherent time-inefficiency problem. By experiments, we find that the number of consensus peers greatly impacts the system’s time-efficiency. Generally, the larger the number of peers is, the higher the time delay is; therefore, we propose to use a blockchain sharding strategy in the fog layer to reduce the number of peers of each blockchain to effectively reduce the system time latency. This approach is highly feasible with the SDN paradigm because of the way that the entire network is organized by disparate control domains. In this context, when implementing blockchain sharding, we just need to divide different BottomChains according to different SDN domains. This is greatly beneficial because, in the real-world implementation of a healthcare IoT, the system usually is composed of infrastructures of independent medical organizations; therefore, dividing the SDN domain by organization in case of privacy disclosure of the highly privacy-sensitive human health data is realistic and feasible.

 <p>TopChain</p>	<p>(1) Ensure security of the decision result of the SDN controllers. (2) Consensus on the blacklist of WBAN devices.</p>
 <p>BottomChain</p>	<p>(1) Ensure security of the task information from the WBAN devices. (2) Ensure secure storage of the task processing results.</p>
 <p>Light weight nodes</p>	<p>(1) Initiate service requests. (2) Generate smart contracts.</p>

**Fig. 3 Proposed blockchain-based two-layer and multidimensional security mechanism.**

We give an example herein to clarify the idea. Assume a total of 70 fog nodes are in the fog layer that may be deployed by different organizations. Great challenges exist if we design only one BottomChain in the fog layer with the 70 fog nodes as consensus peers, as not only the data privacy of distinct organizations faces great risk but also the potential long time-latency owing to the numerous of consensus peers. In contrast, if we use blockchain sharding in this case, it is natural to divide the fog nodes into different BottomChains according to the different organizations, with the fog nodes of the same organization serving as the corresponding BottomChain peers, to well ensure the data privacy and confidentiality of each organization. For example, if there are 3 organizations each with 10, 30, and 30 fog nodes deployed, then there would be a total of 3 disparate BottomChains in the fog layer with a maximum number of consensus peers of 10, 30, and 30, respectively, under the blockchain sharding scheme, which is remarkably lower than the total node number of 70 when without blockchain sharding. Note that, as mentioned earlier, we simply assume that all the fog nodes of an SDN domain participate in the consensus processes of the corresponding BottomChain for the feasibility of analysis and comparison in our work.

On emergency occasions, the blockchain sharding can be continued within one organization (SDN domain) to further decrease time-latency. In this case, the original BottomChain of one domain can be further divided into multiple ones according to certain criteria such as by department or using certain schemes, such as in our prior work<sup>[36]</sup>, where the K-means clustering algorithm is used to automatically divide the peers into different sub-blockchains.

Note that, although the system efficiency can efficiently be improved with the blockchain sharding strategy, it also brings about the potential problem of performance decline in system security, which is owing to the reduced cost to attackers for tampering. Accordingly, it becomes crucial to well balance and tradeoff the system performances of security and efficiency.

## 6 Evaluation Results and Analysis

In this section, we first evaluate the performance of the proposed decision-making algorithm LSRDM-EH in terms of time-efficiency, reliability, and network throughput through extensive simulation using Matlab.



In the simulation, the 70 fog nodes are equally distributed within a quadrangular wireless area of  $5000\text{ m} \times 3000\text{ m}$  and the WBANs edge devices can roam randomly. Experiments were conducted by changing the weight parameters  $\alpha$  and  $\beta$ , the task parameters, including  $C_i$ ,  $D_i$ , and task deadline  $T_{\text{exp}}$ . Then, we validate the performance of the blockchain-based security strategy, including the capacity of resisting a tampering attack and time-efficiency, and the simulation parameters used are listed in Table 1.

## 6.1 Evaluation of the centralized decision-making algorithm

### 6.1.1 Time-efficiency

Extensive simulation is conducted to evaluate the time-efficiency of the system, as shown in Fig. 4, where the time delay with respect to the weight parameter  $\alpha$  of the ordinary fog nodes and the optimal target fog

node ( $F_t$ ) with and without LSRDM-EH is illustrated. As observed from Fig. 4, because of the powerful emergency handling capacity of the proposed LSRDM-EH, the time cost is much lower with LSRDM-EH for either the ordinary fog nodes or the optimal target fog node. Specifically, with LSRDM-EH, when the edge device is in an emergency situation, the associated fog node in service would not only adopt preemptive task scheduling but also allocate all the CPU resources to the offloaded emergent task, further benefiting the low-latency service provision. Without LSRDM-EH, the fog nodes may routinely follow the manner of FCFS, potentially resulting in longer task queue, leading to considerably longer latency owing to the longer queuing time of the task. Additionally, the assignment of only part of the fog's CPU resource to the task further worsens the overall time-efficiency in that case. Figure 4 also shows that, as  $\alpha$  increases from 0 to 1, the time cost under  $F_t$  decreases with or without LSRDM-EH because fog nodes with lower time delay will be given higher priority to be associated with, which also reflects the role of the two decision factors of time delay and security. Specifically, if we increase the delay weight  $\alpha$ , the time cost of the nodes gradually dominates the performance, while when we increase the reputation weight  $\beta$  (decrease  $\alpha$ ), the security metric gradually dominates. That is,  $\alpha$  and  $\beta$  imply a tradeoff between system performance of latency and security, and when  $\alpha$  decreases to 0, the time delay under  $F_t$  appears comparable to or even higher than that of the ordinary fog nodes because the time delay index has lost control over the entire decision-making process with only the security index considered in this case.

Furthermore, we also verify the effect of the data volume ( $D_i$ ) and the required CPU cycles ( $C_i$ ) of the tasks on the system time latency, as shown in Fig. 5, whereby the increase in  $D_i$  and  $C_i$  incurs the increase in the system time latency with or without LSRDM-EH, and under the same condition, the time delay regarding the optimal target fog node and the ordinary fog nodes are much lower with LSRDM-EH. Meanwhile, the time cost of the target fog node is substantially lower than that of the ordinary fog nodes, manifesting the superiority of the proposed LSRDM-EH scheme.

As discussed above, we conclude that the decision-making scheme of LSRDM-EH performs well in low-delay service provision with a powerful emergency handling capacity that can well satisfy the real-time and low-latency requirements of the healthcare IoT

Table 1 Simulation parameters.

Symbol	Description	Value
$R_s$	Search space range	$5000\text{ m} \times 3000\text{ m}$
$N$	Total number of fog nodes	70
$M$	Total number of WBANs devices	1000
$D_i$	Task data volume	0–1200 MB
$C_i$	Task CPU cycles	0–1200 GHz
$f_{\text{CPU}}$	Frequency of the fog nodes	4–6 GHz
$B_W$	Bandwidth of the fog nodes	0.1–100 MHz
$\Gamma$	Channel attenuation coefficient	4
$\mathcal{E}$	Small scale attenuation coefficient	0.5
$p_H$	Transmitting power of WBANs gateway devices	0.2–1.0 W
$\sigma^2$	Noise power	–100 dBm
$T_{\text{exp}}$	Task deadline	25–200 s
$\alpha, \beta, \varrho$	Weight parameters	0–1

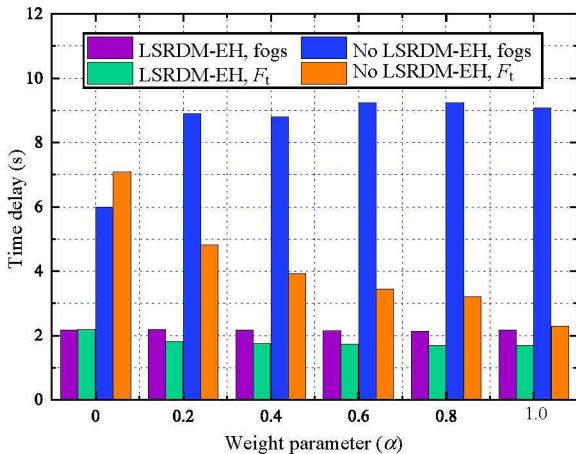
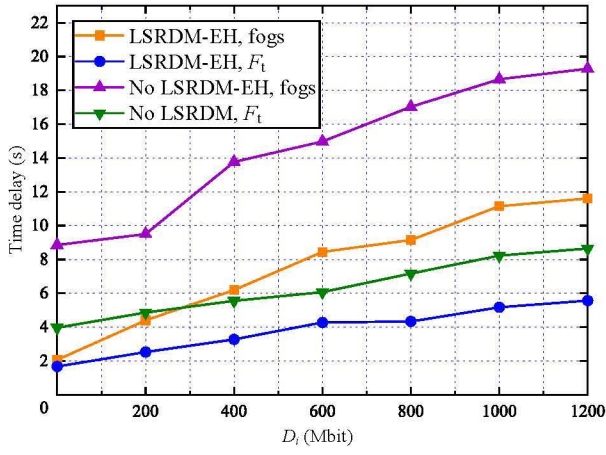
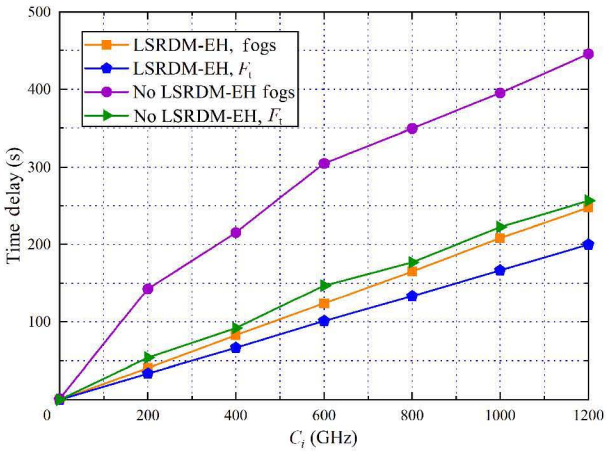


Fig. 4 Time delay against weight parameter  $\alpha$ .



(a)



(b)

Fig. 5 Time delay against  $D_i$  and  $C_i$ .

applications.

### 6.1.2 System security and reliability

An experiment was conducted for evaluating the system reliability by adjusting the weight parameter  $\beta$  to observe the key reliability index of the task success ratio (TSR) of the system, as shown in Fig. 6, where the TSR of the target fog node improves gradually with the increase in  $\beta$  with or without LSRDM-EH because the system security performance gradually dominates in this case, i.e., nodes with higher reputation value are gradually given higher priority to be associated with, leading to the gradual increase of the system security and reliability. Additionally, under the same condition, the TSR of the target fog node is much higher than that of the ordinary fog nodes, indicating the higher reliability of the system with LSRDM-EH. To further verify the system security, we also present the corresponding reputation values of the fog nodes as shown in Fig. 7, where the reputation value of the target fog node is remarkably

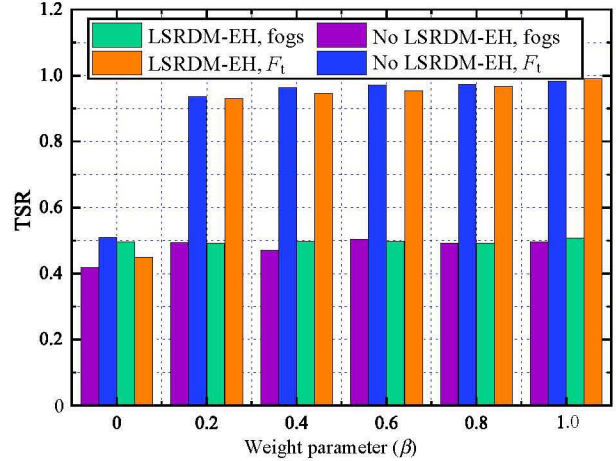


Fig. 6 Task success ratio (TSR) against weight parameter ( $\beta$ ).

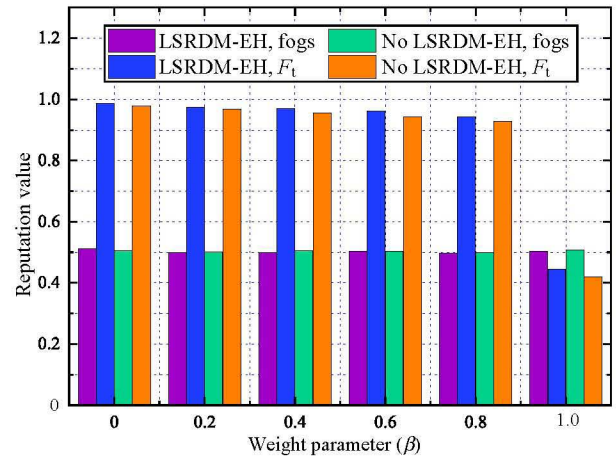


Fig. 7 Node reputation value against the weight parameter ( $\beta$ ).

higher than that of the ordinary fog nodes under the proposed scheme verifying the effectiveness of the decision making algorithm.

### 6.1.3 System throughput

Simulation has also been conducted to verify the effect of the task deadline on system throughput, as shown in Fig. 8, wherein too low a task deadline  $T_{exp}$  (less than 50 s) leads to an almost zero system throughput, while the gradual increase in  $T_{exp}$  to approximately 75 s incurs a sharp rise in the throughput to roughly the maximum value, with slight variation thereafter, implying the threshold of  $T_{exp}$  being approximately 75 s. This result is consistent with intuition because an undersized  $T_{exp}$  causes no fog nodes to meet the criteria. Moreover, as Fig. 8 shows, the system throughput regarding the target fog node is significantly higher than that of the ordinary fog nodes because of the even lower time delay of the former compared to that of the latter.



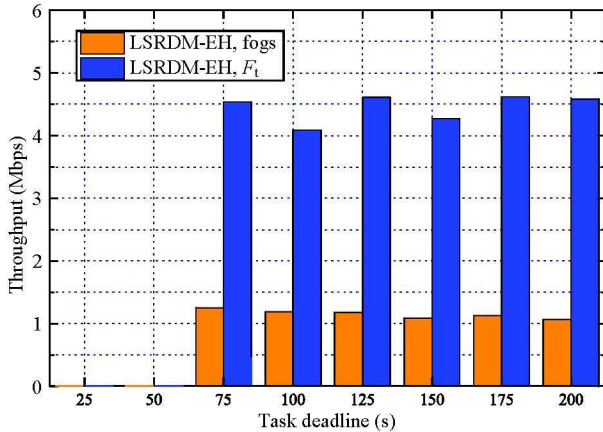


Fig. 8 System throughput against task deadline  $T_{exp}$ .

## 6.2 Blockchain-based system performance evaluation

As discussed above, to ensure system security, we have proposed a blockchain-based two-layer and multidimensional security scheme, viz., the control layer TopChain and the data layer BottomChains, to well resist diverse cyber-physical attacks, such as non-repudiation, DDoS, and tampering attacks, whereby crucial information including inter- and intra-SDN control signaling, human health parameters, original task information and the corresponding task processing results, and the blacklist of the edge devices are secured, benefiting from the powerful, secure storage capacity of the blockchains. Furthermore, not only the human data but also node behaviors can be well traced under the blockchain-based security mechanism. Moreover, the inherent problem of single-point failure of SDN can also be effectively eliminated with TopChain.

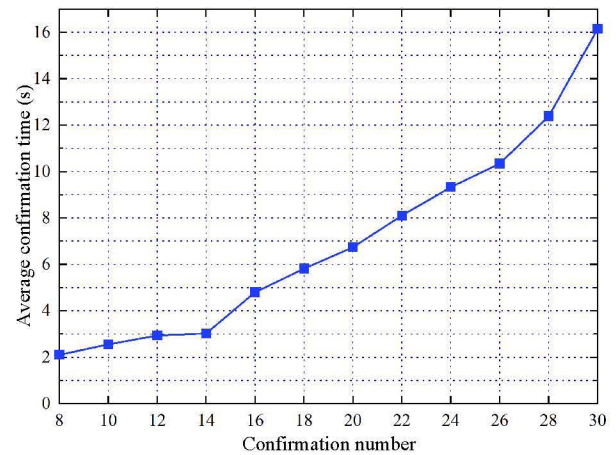
In this part, we first conduct a simulation-based evaluation to validate the superiority of the proposed security strategy. Next, because of the delay-sensitivity of practical smart healthcare applications, the time-efficiency of the proposed security method with blockchain sharding is also simulated by adjusting the number of consensus peers between 10 and 70 and difficulty bits between 3 and 27 to verify the efficiency and effectiveness of the recommended strategy. Note that, because of the resource-constrained nature of the healthcare IoT edge devices, they just serve as lightweight nodes that purely initiate and verify transactions (services) without participating in the energy-consuming consensus processes of the blockchains in the design.

### 6.2.1 Evaluation of system security

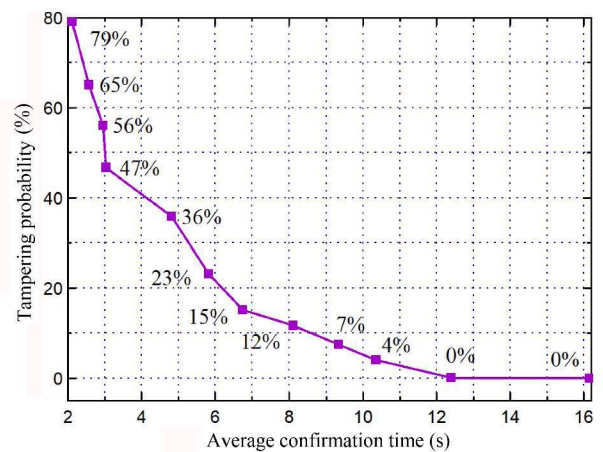
To validate the security performance of the proposed

strategy, we have conducted extensive simulations using Python, where the number of consensus nodes is 30, and the number of difficulty bits is 18. Each simulation has been run for 50 rounds for statistical validation, and the results are shown in Fig. 9.

Figure 9a shows that the confirmation number of a new block significantly affects its average confirmation time. The larger the confirmation number of the block is, the higher the performance of system security is, and the longer the average block confirmation time is, which implies a tradeoff between the time efficiency and the security of the blockchain-based system. This finding is intuitive because a larger number of confirmations to a new block would significantly reduce the security risk of tampering attacks in blockchain, as indicated in Fig. 9b, whereby the tampering probability of the blockchain decreases almost exponentially as the average confirmation time increases. Specifically, when



(a)

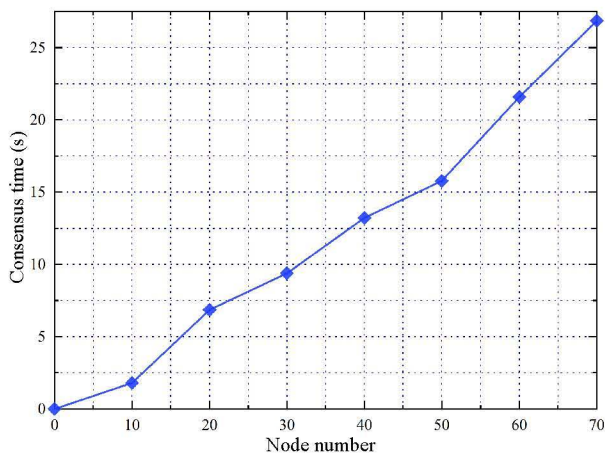


(b)

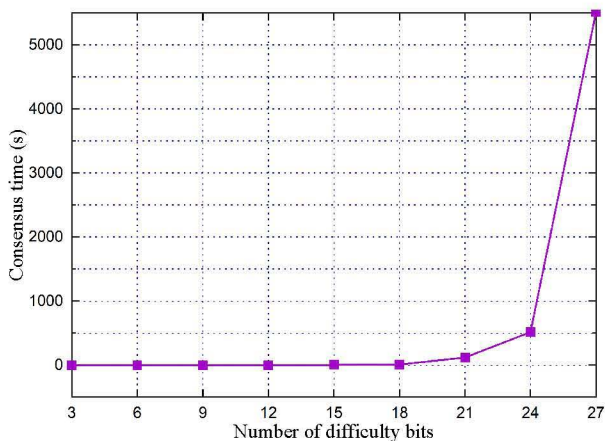
Fig. 9 Relationship of block confirmation number and confirmation time, and tampering probability against block confirmation time.

the confirmation ratio is 8/30, the probability of the system suffering tampering is approximately 79%, as the confirmation ratio increases to 20/30, the tampering risk is reduced to only approximately 15%, and when the confirmation ratio rises above 28/30, the tampering probability gradually reaches the minimum value of 0, enabling the system with absolute power of anti-tampering.

Although the proposed blockchain-based system can provide powerful security as discussed above, it suffers from an inherent time-inefficiency problem. To solve this problem, we have conducted extensive simulations to determine that the number of consensus peers and the number of blockchain difficulty bits have a vital impact on the system time efficiency, as indicated in Fig. 10. Figure 10a shows that the consensus time remarkably increases as the number of consensus nodes increases; therefore, we can conclude that given the total number of consensus peers, we can divide them



(a)



(b)

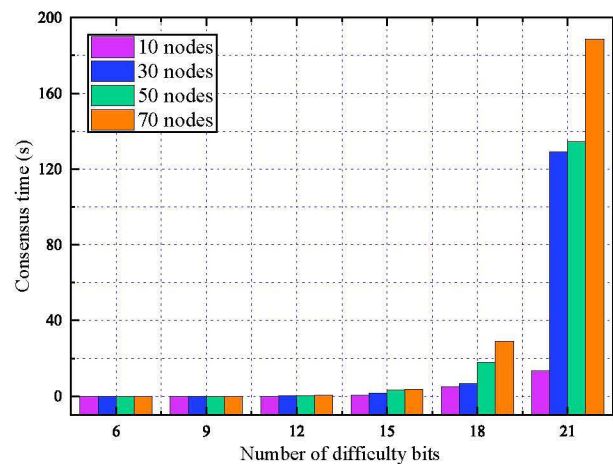
**Fig. 10** Consensus time against nodes number, and consensus time against number of difficulty bits.

into different sub-blockchains to reduce the number of peers participating in the consensus process for reducing the system time latency. This finding also validates the superiority of our strategy, whereby the innovative method of BottomChain-based sharding is used to decrease the number of consensus peers of a blockchain to improve the system’s time efficiency.

Figure 10b shows that the consensus time remains almost unchanged as the number of difficulty bits varies between 3 and 18. Moreover, when the number of difficulty bits rises above 21, the consensus time appears to increase noticeably, and when it increases to above 27, the time latency becomes too large to accept. This is because the fact that the larger the number of difficulty bits is, the greater the mining difficulty of the blockchain verifiers is, and the higher the system latency is. Consequently, we conclude that the service latency could be effectively adjusted by changing the number of difficulty bits. Specifically, when we need to reduce the service latency, we should decrease the difficulty bits.

**6.2.2 Evaluation of time-efficiency**

According to the above discussion, when we employ the advantage of blockchain sharding and the strategy of decreasing the number of blockchain difficulty bits, the service latency can be remarkably reduced, as indicated in Fig. 11, whereby 6, 9, 12, 15, 18, and 21 difficulty bits with 10, 30, 50, and 70 peers are experimented, respectively. As Fig. 11 shows, lower difficulty bits combining with fewer peers yield a shorter consensus time. Specifically, when the number of difficulty bits is 6, 9, and 12, the consensus time differs little and is almost zero with a different number of nodes, and when the number of difficulty bits is 15, the consensus time slightly increases as the nodes number increases. Then,



**Fig. 11** Time cost in various conditions.



as the difficulty bit continues to increase, the consensus time rises approximately exponentially, leading to a large performance gap under a different number of peers. This result shows that the consensus time is no more than 10 s with 10 peers while sharply increasing to approximately 180 s with 70 peers, causing the system latency to be too high to meet the low-latency requirement of the healthcare IoT system. Nevertheless, by using the proposed blockchain sharding strategy, the number of peers of one blockchain can be readily reduced to well meet the challenge.

In a real-world implementation, the specific number of consensus peers and difficulty bits should be determined according to the requirements of the practical applications, and because of the tradeoff between the difficulty bits and the system security performance, a compromise between these aspects should be used.

## 7 Conclusion

The WBANs-based healthcare IoT has gained widespread attention from industry and academia. To address the pressing challenges, the advanced solutions of SDN, fog computing, and blockchain are leveraged in this paper. Distributed near the edge devices, fog computing can provide real-time and low-latency mass data processing capacity. Through task-offloading, the resource-constrained edge devices can offload computationally intensive tasks to the fog nodes for task processing. In particular, we have designed a centralized decision-making algorithm LSRDM-EH to optimize the decision-making process for assigning target fog nodes for task processing with time-efficiency and reliability jointly considered. Benefiting from a global view of the entire network, the SDN controller can provide dynamic and flexible network control and management and optimized resource scheduling capability to ensure high system efficiency and scalability. Additionally, we have designed a comprehensive blockchain-based two-layer and multidimensional security strategy to ensure the security of the entire system. On the basis of this strategy, we propose a blockchain sharding mechanism for the fog layer blockchain to tackle the inherent time-inefficiency problem of blockchain. Extensive simulation has been conducted to validate the efficiency and effectiveness of the proposed mechanisms, and numerical results show that the system performances, including efficiency, reliability, and security, are significantly improved, verifying the superiority of our scheme.

## Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 61761007) and the Scientific Research Project of Guangxi University Xingjian College of Science and Liberal Arts (No. Y2021ZK03).

## References

- [1] J. J. Hu, M. Reed, N. Thomos, M. F. Ai-Naday, and K. Yang, Securing SDN controlled IoT networks through edge-block chain, *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2102–2115, 2021.
- [2] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective, *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8421–8434, 2019.
- [3] K. Kaur, S. Garg, G. Kaddoum, S. H. Ahmed, and M. Atiqzaman, KEIDS: Kubernetes-based energy and interference driven scheduler for industrial IoT in edge-cloud ecosystem, *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4228–4237, 2020.
- [4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, 2017, pp. 618–623.
- [5] S. Sarkar, S. Chatterjee, and S. Misra, Assessment of the suitability of fog computing in the context of Internet of Things, *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 46–59, 2018.
- [6] M. Mukherjee, S. Kumar, M. Shojafar, Q. Zhang, and C. X. Mavromoustakis, Joint task offloading and resource allocation for delay-sensitive fog networks, in *53<sup>rd</sup> IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 618–623.
- [7] W. S. Shi, J. Cao, Q. Zhang, Y. H. Z. Li, and L. Y. Xu, Edge computing: Vision and challenges, *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
- [8] G. S. Aujla, R. Chaudhary, N. Kumar, R. Kumar, and J. J. P. C. Rodrigues, An ensemble scheme for QoS-aware traffic flow management in software defined networks, presented at 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1–7.
- [9] M. Ojo, D. Adami, and S. Giordano, A SDN-IoT architecture with NFV implementation, presented at 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 2016, pp. 1–6.
- [10] J. C. Wang, K. N. Han, A. Alexandridis, Z. Y. Chen, Z. Zilic, Y. Pang, G. Jeon, and F. Piccialli, A blockchain-based eHealthcare system interoperating with WBANs, *Future Generation Computer Systems*, vol. 110, pp. 675–685, 2020.
- [11] D. Kim, J. Son, D. Seo, Y. Kim, H. Kim, and J. T. Seo, A novel transparent and auditable fog-assisted cloud storage

- with compensation mechanism, *Tsinghua Science and Technology*, vol. 25, no. 1, pp. 28–43, 2020.
- [12] Y. Z. Wu, Y. Lyu, and Y. C. Shi, Cloud storage security assessment through equilibrium analysis, *Tsinghua Science and Technology*, vol. 24, no. 6, pp. 738–749, 2019.
- [13] A. Botta, W. D. Donato, V. Persico, and A. Pescapé, Integration of cloud computing and internet of things: A survey, *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.
- [14] S. Ahmed, M. Saqib, M. Adil, T. Ali, and A. Ishtiaq, Integration of cloud computing with internet of things and wireless body area network for effective healthcare, presented at 2017 International Symposium on Wireless Systems and Networks (ISWSN), Lahore, Pakistan, 2017, pp. 1–6.
- [15] S. Moulik, S. Misra, and A. Gaurav, Cost-effective mapping between wireless body area networks and cloud service providers based on multi-stage bargaining, *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1573–1586, 2017.
- [16] G. Almashaqbeh, T. Hayajneh, and A. V. Vasilakos, Qosaware health monitoring system using cloud-based WBANs, *Journal of Medical Systems*, vol. 38, no. 10, pp. 1–21, 2014.
- [17] Y. Z. Zhou, D. Zhang, and N. X. Xiong, and B. J. Mohd, Post-cloud computing paradigms: A survey and comparison, *Tsinghua Science and Technology*, vol. 22, no. 6, pp. 714–732, 2017.
- [18] A. Roy, C. Roy, S. Misra, Y. Rahulamathavan, and M. Rajarajan, CARE: Criticality-aware data transmission in CPS-based healthcare systems, pretended 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1–6.
- [19] T. N. Gia, M. Z. Jiang, A. M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, Fog computing in healthcare internet of things: A case study on ECG feature extraction, presented at 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 2015, pp. 356–363.
- [20] A. Q. Zhang and X. D. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, *Journal of Medical Systems*, vol. 42, no. 8, p. 140, 2018.
- [21] L. J. Xiao, D. Z. Han, X. W. Meng, W. Liang, and K. C. Li, A secure framework for data sharing in private blockchain-based WBANs, *IEEE Access*, vol. 8, pp. 153956–153968, 2020.
- [22] M. Cicioğlu and A. Clhan, SDN-enabled wireless body area networks, presented at 2018 6<sup>th</sup> International Conference on Control Engineering and Information Technology, Istanbul, Turkey, 2018, pp. 1–5.
- [23] K. Hasan, K. Ahmed, K. Biswas, M. S. Islam, and O. A. Sianaki, Software defined application-specific traffic management for wireless body area networks, *Future Generation Computer Systems*, vol. 107, pp. 274–285, 2020.
- [24] M. Cicioğlu and A. Clhan, SDN-based wireless body area network routing algorithm for healthcare architecture, *ETRI Journal*, vol. 41, no. 4, pp. 452–464, 2019.
- [25] M. Cicioğlu and A. Clhan, Energy-efficient and SDN enabled routing algorithm for wireless body area network, *Computer Communications*, vol. 160, pp. 228–239, 2020.
- [26] V. Varadharajan, U. Tupakula, and K. Karmakar, Secure monitoring of patients with wandering behavior in hospital environments, *IEEE Access*, vol. 6, pp. 11523–11533, 2018.
- [27] W. Meng, K.-K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, Towards bayesian-based trust management for insider attacks in healthcare software-defined networks, *IEEE Transactions on Network & Service Management*, vol. 15, no. 2, pp. 761–773, 2018.
- [28] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. K. R. Choo, An energy-efficient SDN controller architecture for IoT networks with blockchain-based security, *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625–638, 2020.
- [29] L. Wang, G. Z. Yang, J. Huang, J. Y. Zhang, L. Yu, Z. D. Nie, and D. R. S. Cumming, A wireless biomedical signal interface system-on-chip for body sensor networks, *IEEE Transactions on Biomedical Circuits & Systems*, vol. 4, no. 2, pp. 112–117, 2010.
- [30] T. Hayajneh, K. Griggs, M. Imran, and B. J. Mohd, Secure and efficient data delivery for fog-assisted wireless body area networks, *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1289–1307, 2019.
- [31] R. Hasan, S. Zawoad, S. Noor, M. M. Haque, and D. Burke, How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis, presented at 2016 IEEE 40<sup>th</sup> Computer Software & Applications Conference, Atlanta, GA, USA, 2016, pp. 417–422.
- [32] M. Zamani, M. Movahedi, and M. Raykova, Rapidchain: Scaling blockchain via full sharding, presented at 2018 ACM SIGSAC Conference, Toronto, Canada, 2018, pp. 931–948.
- [33] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, OmniLedger: A secure, scale-out, decentralized ledger via sharding, presented at 2018 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2018, pp. 583–598.
- [34] L. Liu, W. Feng, C. Chen, Y. R. Zhang, D. P. Lan, X. M. Yuan, and S. Vashisht, BSIoT: Blockchain based software defined network framework for internet of things, presented at *IEEE INFOCOM 2020–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, Canada, 2020, pp. 496–501.
- [35] M. Azrou, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, New enhanced authentication protocol for internet of things, *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, 2021.
- [36] J. Z. Li, Z. H. Wang, M. H. Li, and T. F. Qin, spectrum sharing management method for the small-area blockchain based on district partition (in Chinese), *Journal of Xidian University (Nat. Sci.)*, vol. 47, no. 6, pp. 122–130, 2020.





**Junyu Ren** received the MS degree in communication and information system from Guilin University of Electronic Science and Technology, Guilin, China, in 2005. She is currently pursuing the PhD degree in information and communication engineering with the School of Electronic and Information Engineering, South China

University of Technology, Guangzhou, China. Her current research interests include wireless body area network, Internet of Things, fog computing, blockchain, and trust management.



**Jinze Li** is currently pursuing the MS degree with the School of Computer, Electronics and Information, Guangxi University, Nanning, China. His research interests include cognitive radio network and blockchain.



**Huaxing Liu** received the PhD degree from University of Cambridge, Cambridge, UK, in 2018, and he is now with the Faculty of Earth Sciences & Geography, Trinity College, University of Cambridge, Cambridge, UK. His research interests include multimedia communication and remote sensing.



**Tuanfa Qin** received the PhD degree from Nanjing University, Nanjing, China, in 1997. Since 1991, he has been with the School of Computer, Electronic and Information, Guangxi University, Nanning, China, where he became an associate professor in 1997 and a professor in 2000. He is also the laboratory director

of Guangxi Key Laboratory of Multimedia Communications and Network Technology. He has authored more than 200 academic papers and participated in writing 2 monographs. He has obtained 12 authorized Chinese invention patents in the field of communication, and 7 utility model patents, and more than 20 copyrights of computer software registration. He has sponsored over 5 projects of National Natural Science Foundation of China, over 2 National Innovation Fund Projects for small and medium-sized enterprises, and over more than 10 provincial and ministerial projects. His general research interests include wireless body area network and wireless multimedia communication.