Permissioned blockchain and deep reinforcement learning enabled security and energy efficient Healthcare Internet of Things

LONG LIU\textsuperscript{1} and ZHICHAO LI\textsuperscript{2}

\textsuperscript{1}School of Political Science and Public Administration, East China University of Political Science and Law, Shanghai, 200042, China
\textsuperscript{2}School of International and Public Affairs, Shanghai Jiao Tong University, Shanghai, 200030, China

Corresponding author: Zhichao Li (e-mail: yizhiqingcao@163.com).

This work was funded by the National Natural Science Foundation of China [Grant No. 71974057, and Grant No. 72071031]; and the Ministry of Education through the Humanities and Social Science project [Grant No. 19YJC630104].

\begin{abstract}
Recently, the Healthcare Internet of Things (H-IoT) has been widely applied to alleviate the global challenge of the coronavirus disease 2019 (COVID-19) pandemic. However, security and limited energy capacity issues remain the two main factors that prevent the large-scale application of the H-IoT. Therefore, a permissioned blockchain and deep reinforcement learning (DRL)-empowered H-IoT system is presented in this research to address these two issues. The proposed H-IoT system can provide real-time security and energy-efficient healthcare services to control the propagation of the COVID-19 pandemic. To address the security issue, a permissioned blockchain method is adopted to guarantee the security of the proposed H-IoT system. As for handling the limited energy constraint, we employ the mobile edge computing (MEC) method to offload the computing tasks to alleviate the computational burden and energy consumption of the proposed H-IoT system. We also adopt an energy harvesting method to improve performance. In addition, a DRL method is employed to jointly optimize both the security and energy efficiency performance of the proposed system. The simulation results demonstrate that the proposed solution can balance the requirements of security and energy efficiency issues and hence can better respond to the COVID-19 pandemic.
\end{abstract}

\begin{keywords}
Blockchain, Deep Reinforcement Learning, Mobile Edge Computing, Energy Harvesting, Healthcare Internet of Things, COVID-19
\end{keywords}

I. INTRODUCTION

As a huge global public health crisis, the outbreak and spread of the coronavirus disease 2019 (COVID-19) pandemic has hugely impacted the traditional healthcare industry. An increasing amount of advanced information and communication technologies (ICTs) have been adopted in the healthcare sector to mitigate the impact of the COVID-19 pandemic. The Healthcare Internet of things (H-IoT), which is one of the most dominant and promising applications of IoT responding to the COVID-19 pandemic, has developed rapidly in recent years [1], [2]. From a clinical perspective, the H-IoT can be employed widely for sensing, communication, data analytics, and inference in future healthcare areas [3]. In addition, emerging advanced ICTs have been employed in the H-IoT in recent years, including machine learning, fog and edge computing, big data, blockchain, and software-defined networks (SDNs). These technologies can accelerate the applications of H-IoT in healthcare areas [2], especially applications related to COVID-19 prevention and treatment. In this context, a framework based on disruptive ICTs to restrict the spread of the COVID-19 pandemic is presented in [4]. These technologies include artificial intelligence (AI), 5G, blockchain, Industry 4.0, the Internet of Things (IoT), the Internet of Medical Things (IoMT), big data, and drones. Such emerging technologies can enable COVID-19 pandemic-related digital transformation, research and development, and service delivery.

Clearly, the COVID-19 pandemic has accelerated the ap-
applications of the H-IoT in the healthcare industry. For example, one review summarizes the changes brought about by ICTs in the healthcare industry, where the IoT, cloud and fog computing, and big data have reformed the whole ecosystem of the healthcare industry [5]. Because IoT-based healthcare applications have the potential to improve the efficiency of healthcare delivery systems to alleviate the challenges of the COVID-19 pandemic [6], an increasing number of IoT applications have been employed in the healthcare industry in recent years. For example, advanced digital technologies, including the IoT, big data analytics, AI, and blockchain, have already been applied to alleviate the impact of the COVID-19 pandemic, such as by effectively monitoring, detecting, and preventing the spread of COVID-19 [7]. Furthermore, the IoT platform can be employed to develop intelligent COVID-19 pandemic prevention and control, including symptom diagnosis, quarantine monitoring, contact tracing, social distancing, outbreak forecasting, and mutation tracking [8]. To prevent the spread of COVID-19, the IoT can help with remote diagnostics and detection [9]. In addition, an empirical study investigating the staff of healthcare manufacturing companies in South Korea demonstrates that digital healthcare technologies, including AI and IoT, can improve the performance of supply chains in the healthcare industry in response to the pandemic [10]. However, due to the limited computing and communication resources of H-IoT systems, security and limited energy capacity issues have become two main issues preventing the large-scale and widespread application of H-IoT. For example, in [2], the performance challenges of H-IoT in the healthcare industry are reviewed, including low latency, low power operation, security, and real-time operational challenges, as well as the scalability, service availability, interoperability, and the regulatory policies [2]. In addition, a blockchain-based energy-efficient data collection system is presented to address the security and energy-efficient challenges of IoT applications [11]. In summary, as the research on the H-IoT in the COVID-19 pandemic is still in its initial stages, efforts addressing both the security and energy efficiency issues of the H-IoT are still lacking. Therefore, in this study, we introduce a permissioned blockchain and deep reinforcement learning (DRL)-enabled H-IoT system to improve both the security and energy efficiency of the H-IoT system.

To address the security issue, the permissioned blockchain method is used to protect the security of the proposed H-IoT system. An increasing number of related studies employ blockchains to ensure the security and auditability of IoT applications [12]. In addition, blockchains can improve the interoperability, privacy, security, reliability, and scalability of IoT systems [13]. The blockchain method not only plays a strategic role in the healthcare sector but can also improve the clinical practice when dealing with the COVID-19 pandemic [14]. Therefore, the blockchain method is adopted in this research to guarantee the security of the H-IoT system. However, the permissionless blockchain methods commonly employed by most of the current research cannot fit the limited computing and communication resources of the H-IoT system. Hence, the permissioned blockchain method is chosen in this study due to its limited energy and computational resources.

To address the limited energy capacity issue, mobile edge computing (MEC) and energy harvesting methods are adopted. It is worth noting that an increasing number of studies have employed the MEC method to offload computing tasks to the edge server in order to improve the performance of the IoT system [15]. Therefore, in this study, the MEC method is used to alleviate the computing burden and the energy consumption of the H-IoT. In addition, some researchers have adopted the energy harvesting method to capture energy from external sources to prolong the running time of IoT [16]. Therefore, we also deploy an energy harvesting method to improve the energy efficiency of the proposed H-IoT system.

Furthermore, a joint optimization method is employed that takes into account both the security requirements and the energy efficiency performances of the H-IoT system. Considering the complex and dynamic nature of the blockchain-based and MEC-enabled H-IoT system, we model the system as a discrete Markov decision process (MDP) problem [17], to explore the maximized system reward. Since the dynamic state of H-IoT system cannot be defined in advance, a DRL method is adopted in this study for the joint optimization task. In particular, an asynchronous advantage actor critic (A3C) algorithm is adopted for joint optimization of the throughput of a permissioned blockchain system and the energy efficiency of the H-IoT system.

This study is organized as follows: Section II presents the review of related studies regarding H-IoT applications dealing with the COVID-19 pandemic. Section III introduces the system model and the problem formation to address the security issue of the H-IoT system in COVID-19. Section IV describes the details of the proposed DRL method for the joint optimization of the H-IoT system. Section V presents extensive simulation results to evaluate the proposed H-IoT systems. Section VI and Section VII consist of the discussion and conclusions. The abbreviations frequently employed in this study are listed in Table 1.

II. RELATED WORKS

The related research described in this section contains three components: the H-IoT-related applications in the COVID-19 pandemic, the security issue of such H-IoT applications, and the limited energy capacity issue of these H-IoT applications.

A. H-IOT-RELATED APPLICATIONS IN THE COVID-19 PANDEMIC

The H-Iot, as an important and emerging application of IoT in the healthcare industry, has developed rapidly with the advancement of ICTs and the widespread use of wearable smart IoT devices in recent years [1], [2]. A comprehensive review of future H-IoT applications is presented in [2], including machine learning, fog and edge computing, big data, blockchain, and SDNs. A review of the H-IoT from
a clinical perspective is presented in [3] with the focus on three technologies, namely, sensing, communication, and data analytics and inference. In [18], a comprehensive review summarizes the integration of IoT and cloud computing in the healthcare industry, offers a complete IoT and cloud computing framework in the healthcare industry, and classified them briefly. The study also addresses threats, vulnerabilities, and attack risks of IoT in the healthcare industry.

The COVID-19 pandemic has accelerated the application of advanced ICTs in healthcare areas [7]. For example, [7] summarizes the applications of IoT, big data, AI, and blockchain technologies for tracking during the COVID-19 pandemic and for mitigation of the pandemic’s indirect negative impacts. In addition, a comprehensive review summarizes the advanced ICTs applied to alleviate the impact of the COVID-19 pandemic, including IoT, unmanned aerial vehicles (UAVs), blockchain, AI, and 5G [19]. In [8], another review summarizes the IoT platform for COVID-19 prevention and control and discusses the details of the fog and cloud combined IoT platform in the COVID-19 pandemic prevention and control process. This includes symptom diagnosis, quarantine monitoring, contact tracing, social distancing (during the COVID-19 pandemic prevention period), and outbreak forecasting and mutation tracking (in the COVID-19 pandemic control stage). In addition, a novel remote diagnostic and detection COVID-19 pandemic system based on AI and IoT is presented in [9]. This system not only helps doctors reduce direct contact with patients but also stops the spread of the virus. The study presented in [20] discusses the applications of IoT and AI in healthcare in different South American countries during the COVID-19 pandemic. Another study presents the state-of-the-art literature on machine learning-based techniques for big data analytics in IoT smart healthcare areas and discusses their strengths and weaknesses [21]. Furthermore, a comprehensive review summarizing the potential roles of machine learning in H-IoT within healthcare areas is presented in [22]; these potential roles include diagnosis, prognosis and spread control, assistive systems, monitoring, and logistics.

Although an increasing number of studies have combined advanced digital technologies or ICTs to prevent and treat the COVID-19 pandemic in recent years, there are still many challenges for the large-scale application of the H-IoT in practice. For example, in [2], the main challenges of the H-IoT are summarized, which include low latency, low power operation, security, real-time operation, scalable deployment, networking solutions, service availability, interoperability, and regulatory policy challenges [2]. Considering the characteristics of the H-IoT system, the security challenge and limited energy capacity challenge are two main issues that affect the system’s performance in the COVID-19 pandemic. Furthermore, there is not enough research to address both the security and the limited energy capacity issues of the H-IoT, especially in the dynamic environments of the COVID-19 pandemic. Therefore, the permissioned blockchain and DRL methods are employed in this research to address the security issue and the limited energy capacity issue of the H-IoT to improve the performance in response to the COVID-19 pandemic.

### B. THE SECURITY OF H-IoT APPLICATIONS IN THE COVID-19 PANDEMIC

An H-IoT system must deal with many personal data [23], such as heart and breath data [2], personal medical information [24], and personal living information, such as details of real-time location and travel [25]. Because this information is private and should be secure [26], an increasing number of studies have adopted blockchain systems to enhance the security of the H-IoT systems. For instance, some comprehensive surveys have summarized the research issues, applications, and challenges of blockchain technologies in IoT fields [13], [27], [28]. In addition, [14] demonstrated the strategic role of blockchain in healthcare areas. It shows that blockchains can not only be applied to safely share information between different groups of persons but can also improve COVID-19 pandemic-related clinical practice. [13] discusses the integration of blockchain technology with IoT and describes the research issues concerning blockchains for next-generation networks. Furthermore, blockchain technologies are already widely employed to guarantee security in industrial settings [29], [30] and large-scale IoT applications [31]. There are three main types of blockchains: public or permissionless blockchains, private or permissioned blockchains, and consortium or federated blockchains [12]. In light of their limited computing and energy capacities, an increasing number of H-IoT applications choose the private or the permissioned blockchain in practice [32].

Although a growing number of studies employ blockchains to ensure the security of the H-IoT, these blockchain-based H-IoT systems would also be vulnerable to malicious security attacks. For instance, [33] summaries the blockchain-related solutions for IoT security. In addition, [34] lists the security challenges for smart contracts in IoT systems. Moreover, [35] reports the research challenges
involving the performance evaluation of blockchain-based security and privacy systems for IoT. However, most current research only focuses on the applications of blockchain systems in IoT scenarios, only few of them discuss the security threats and attacks in blockchain-supported IoT systems. Therefore, we employ the practical Byzantine fault tolerance (PBFT) consensus mechanism to address the security threat and attacks imposed by malicious nodes in the proposed permissioned blockchain system. Further, we note in this context that there is still not enough research dealing with the throughput of blockchain systems in the H-IoT system. Therefore, our research not only adopts the permissioned blockchain system but also optimizes the throughput of the permissioned blockchain used in our H-IoT system.

C. THE LIMITED ENERGY CAPACITY ISSUE OF H-IOT APPLICATIONS IN THE COVID-19 PANDEMIC

Although the proposed permissioned blockchain system can reduce the computing burden compared with the public blockchain system, it also brings extra computing tasks and energy consumptions to the H-IoT system. To reduce the energy consumption, the MEC method is often employed to offload the tasks to the edge servers [36]. For example, a DRL-based decentralized and efficient structure was presented in [37] for blockchain-enabled IoT systems to reduce transaction delays and transmission power consumption, which can improve the efficiency and reliability of blockchain-enabled IoT systems. In addition, related studies have adopted the MEC method to enhance the capability and reduce the energy consumption of IoT systems [15], [16], [36], [38], [39]. Therefore, we also employ the MEC system to offload computing tasks to reduce the energy consumption of the proposed H-IoT system. Furthermore, the proposed H-IoT system can determine whether to offload computing tasks to MEC servers based on real-time situations, which can cover both the partial offloading and binary offloading scenarios [40].

Energy harvesting in IoT, which can harvest energy from natural or artificial environmental resources for IoT networks, can alleviate their dependence on batteries and prolong the duration of IoT networks [41]–[43]. There has been increasing research employing energy harvesting methods to improve the lasting performance of IoT systems in recent years [15], [16], [38], [39]. The linear energy harvesting model [38] was also employed in this study to prolong the duration of H-IoT in response to the COVID-19 pandemic.

Although several studies address the energy efficiency problems of H-IoT systems, most of them focus only on how to improve the energy efficiency while neglecting the security issues of H-IoT systems, which is indispensable for H-IoT applications to respond to the COVID-19 pandemic. Therefore, in our research, both security and energy efficiency issues are jointly addressed to help deploy the H-IoT in complex environments.

The DRL method, which combines deep learning and reinforcement learning, is often used to address the real-time complex decision problems of IoT applications [44]. It can effectively address issues related to the dynamic environment [45]. Considering the special characteristics of blockchain-enabled IoT systems, DRL methods are widely employed to address the dynamic environment and to obtain the optimal solutions of blockchain-empowered IoT systems [46]. Therefore, a DRL method is employed in our study to optimize both the throughput of the proposed permissioned blockchain system and the energy efficiency of H-IoT systems. The details of the proposed deep reinforcement learning method are described in Sections III and IV.

III. SYSTEM MODEL AND PROBLEM FORMULATION

In this section, the system model is introduced. We then demonstrate the MEC system and the energy management model. Subsequently, the permissioned blockchain and throughput model are described. Finally, the problem formulation process is presented.

A. H-IOT SYSTEM FRAMEWORK

Although an increasing number of H-IoT applications are employed to respond to the COVID-19 pandemic, the limited energy and computing capability of H-IoT restrict their large-scale application in practice. Fortunately, the MEC system can significantly increase the computing capability of the H-IoT system, while the energy harvesting system can surpass the current limits on battery capacity to prolong the running time of the H-IoT system. These two methods can improve performance and broaden the applications of the H-IoT in the COVID-19 pandemic. Accordingly, in this research, a secure and energy-efficient H-IoT system is presented in Figure 1.

As illustrated in Figure 1, the proposed H-IoT system consists of an MEC network that includes several MEC server devices, a permissioned blockchain system deployed on the MEC network, and several H-IoT devices with an
energy harvesting module and computing module, which can process the computing tasks at local devices or offload them to MEC server devices. The details of the proposed H-IoT system are presented in the following sub-sections.

### B. PERMISSIONED BLOCKCHAIN SYSTEM AND THROUGHPUT MODEL

Considering the limited computing and energy resources of the H-IoT system, a permissioned blockchain model is deployed on MEC servers to guarantee the security of the proposed H-IoT system, which can prevent the security threat and attacks of malicious nodes in the proposed H-IoT system during COVID-19 pandemic.

According to [47], the proposed permissioned blockchain systems in this research contain two main steps: Generating a block and appending the block to the blockchain. Generating a block consists of collecting, validating, and packaging the transactions into a block, while appending the block to the blockchain including both broadcasting the generated block to other block produces and appending the block to the local blockchain after the consensus of the new block is reached by the consensus mechanism.

Considering there may be some malicious nodes in the proposed H-IoT system, the proposed blockchain mainly deal with manipulation-based attacks [27], which means the malicious node may send incorrect or false information to the blockchain system [47]. Hence, the PBFT consensus protocol has been employed in this study to guarantee the security of the H-IoT system. The whole consensus of PBFT includes five steps: Request, Pre-prepare, Prepare, Commit, and Reply [47]. In the PBFT consensus mechanism, every transaction will be validated by every other node in the blockchain system, then the final consensus decision is following a majority rule that can prevent some malicious Byzantine replications proposed by dishonest or malicious nodes [33]. In a nutshell, the PBFT can achieve a robust consensus as long as the malicious replicas are less than a fraction (1/3) [48].

Given q consensus nodes in the proposed permissioned blockchain system, which can be defined as $Q = \{1, 2, ..., q\}$. In the beginning, the H-IoT system sends the consensus requirement of the new block to the blockchain system. Then the blockchain system randomly chooses a primary node and assigns all other nodes as replica nodes. In terms of [47], [49], there are three main steps of the PBFT consensus in H-IoT. Firstly, the primary node verifies the signature and the message authentication code (MAC) of the new block, then the primary node generates a MAC and broadcasts them to all other replica nodes. Secondly, each replica node verifies the received new block and MAC, then generate a MAC and broadcasts them to other replica nodes, which means each node will verify these MACs and new blocks from all other nodes. Finally, any node that received more than $2L$ (where $L = (q - 1)/3$) correct messages will send one correct reply message to the master node, if the master node receives more than $2L$ correct reply message, the consensus process can be recognized as successful. Based on the PBFT consensus mechanism, the proposed system can filter out the security threat and attacks of malicious nodes in the H-IoT system.

As a robust and famous consensus protocol adopted by the Hyperledger, PBFT employs a replication algorithm to tolerant Byzantine failures [33], moreover, since the PBFT can support the smart contracts of the Hyperledger platform, growing research adopts the PBFT consensus protocol as the foundation of current blockchain application [50]. Therefore, based on the PBFT consensus protocol, the proposed framework in this study not only can support the blockchain system in the H-IoT system but also can be integrated with the current blockchain framework.

Following related studies [17], [30], [47], the transactional throughput of a permissioned blockchain system relies on two parameters, namely, the block size and block interval. Here, $T_b$ denotes the block interval, and the transactional throughput $\Omega$ of the permission blockchain system can be modelled as follows:

$$\Omega = \frac{S_b}{T_b}$$  \hspace{1cm} (1)

where $S_b$ represents the block size and $\chi$ denotes the average transaction size [17], [30], [47].

### C. MEC SYSTEM AND ENERGY MANAGEMENT MODEL

To guarantee the security, the permissioned blockchain system has to add some extra computing tasks of the proposed H-IoT system. Therefore, both MEC system and energy management model are used in this study to improve the performance of the proposed H-IoT system.

Given an MEC system consisting of $M$ H-IoT devices and $N$ mobile edge servers, similar to that in related studies [36], [38], and given a fixed constant slot duration of time $k$ (where $k \in \{1, 2, 3, ..., \}$), the H-IoT system generates a computing task of $C_i(k)$ bits at time slot $k$ [38]. Following related research [36], the computing task can be partitioned into $\lambda$ parts. Then, the H-IoT system can decide whether to process the computing task using local computing devices or to offload the task to mobile edge servers. In detail, $B_i(k)$ represents the radio link transmission rate of the H-IoT system to offload some tasks to the selected mobile edge device $i$ (where $1 \leq i \leq N$) at time slot $k$, and $x_i(k)$ (where $0 \leq x_i(k) \leq 1$) is the offloading rate of the H-IoT system. If $x_i(k) = 0$, the H-IoT system executes all the computing tasks using local devices, and if $x_i(k) = 1$, the H-IoT system offloads all the computing tasks to the selected mobile edge devices $i$. When $0 < x_i(k) < 1$, the H-IoT system executes $(1 - x_i(k))C_i(k)$ tasks on local devices while offloading $x_i(k)C_i(k)$ tasks on selected mobile edge devices $i$. In a nutshell, the value of $x_i(k)$ can represent both the partial offloading and binary offloading decisions of proposed H-IoT system [40]. In addition, the key notations are listed in Table 2.
3) Energy harvesting and energy consumption

Assume that the H-IoT is equipped with an energy harvesting module that can capture energy from energy resources, including solar, wind, and RF signals, and that the harvested energy can be stored in the battery to support both the local computing and offloading energy consumption. Suppose \( \rho^{(k)} \) represents the amount of energy harvested during time slot \( k \) as in [36]. Let \( E^{(k)} \) denote the total energy consumption during time slot \( k \). It can be defined as follows:

\[
E^{(k)} = E_{i}^{(k)} + E_{i}^{(k)}
\]

According to [38], the battery level at the beginning of time slot \( k \) can be modelled as follows:

\[
b^{(k+1)} = \max \left\{ 0, b^{(k)} - E^{(k)} + \rho^{(k)} \right\}
\]

If the battery charge is insufficient, for example, when \( b^{(k+1)} = 0 \), the H-IoT devices will drop the computing task [51].

**D. PROBLEM FORMULATION**

To improve the security and energy efficiency of the proposed H-IoT system, the system needs to simultaneously maximize the blockchain throughput and minimize the energy consumption. Therefore, similar to related studies [17], [30], the total objective function of the H-IoT system is modelled as follows:

\[
O^{(k)} = w_{1} \Omega - (1 - w_{1}) w_{2} E^{(k)}
\]

where \( w_{1}(0 < w_{1} < 1) \) is a weight parameter that can combine two objective functions into a single function, and \( w_{2} \) is a mapping factor that can ensure two objective functions at the same level.

1) Discrete MDP problem

Similar to related research on MEC computing in the IoT, we model this joint optimization problem as a discrete MDP problem. The optimization problem can be formulated as a four-tuple \( < S, A, P, r > \), where \( S \) denotes the state of the H-IoT system, \( A \) represents the discrete action space set of the H-IoT system, \( P \) is the state transition probability, and \( r \) is the reward function of the optimization problem.

2) System state space and transition probability

At each epoch, the DRL agent learns the experience from the state space and updates the decision policy based on the observed state. The state space at epoch \( t \) can be represented as follows:

\[
S(t) = [b^{(k)}(t), C^{(k)}(t), \rho^{(k)}(t), \chi(t)]
\]

### TABLE 2. List of key notations

| Notation | Description |
|----------|-------------|
| \( C^{(k)} \) | The volume of computing task during time slot \( k \) |
| \( A \) | The partition number of computing task |
| \( B_{i}^{(k)} \) | The radio transmission rate between the H-IoT devices and edge server \( i \) |
| \( x^{(k)} \) | The ratio of data offloading to the edge server |
| \( M \) | The number of CPU cycles needed to process one bit of computing task |
| \( f_{m} \) | The CPU cycle frequency of local H-IoT device |
| \( \mu \) | The effective capacitance coefficient |
| \( T_{i}^{(k)} \) | The transmission duration during to offload computing task to edge server \( i \) |
| \( P \) | The transmission power to offload computing task to edge server \( i \) |
| \( b^{(k)} \) | The battery level |
| \( \rho^{(k)} \) | The amount of energy harvested during time slot \( k \) |
| \( E_{i}^{(k)} \) | The energy consumption of the local H-IoT devices |
| \( E_{i}^{(k)} \) | The energy consumption of offloading task to edge server \( i \) |
| \( E^{(k)} \) | The total energy consumption during time slot \( k \) |
| \( \Omega \) | The transactional throughput of permissioned blockchain system |
| \( S_{b} \) | The block size of permissioned blockchain system |
| \( T_{b} \) | The block interval of permissioned blockchain system |
| \( \chi \) | The average transactional size |

1) Energy consumption of local computing

Following related studies [36], [38], we assume that the central processing unit (CPU) is responsible for local computing. Hence, the CPU cycle frequency can be adopted to measure the performance. Given that \( M \) is the required number of CPU cycles for one input bit, the total CPU cycles for local computing is \((1 - \overline{x^{(k)}})C^{(k)} M\). Based on [36], [38], dynamic voltage and frequency scaling techniques can be applied, and the H-IoT devices can control the energy consumption by adjusting the CPU frequency \( f_{m} \) for each cycle \( m \) (where \( m \in \{1, 2, ..., (1 - \overline{x^{(k)}})C^{(k)} M\} \)). The local computing energy consumption \( E_{i}^{(k)} \) can hence be modelled as follows:

\[
E_{i}^{(k)} = \sum_{m=1}^{(1-\overline{x^{(k)}})C^{(k)} M} \mu f_{m}^{2}
\]

where \( \mu \) is the effective capacitance coefficient, which depends on the chip architecture of H-IoT devices [51].

2) Energy consumption of MEC

According to [36], [38], the H-IoT devices can offload \( x^{(k)} C^{(k)} \) bits of tasks to mobile edge devices \( i \) at time slot \( k \) with the uplink radio transmission rate \( B_{i}^{(k)} \). Given that \( T_{i}^{(k)} \) is the transmission duration of the H-IoT device to offload tasks to the edge server, the transmission duration can be modelled as follows.

\[
T_{i}^{(k)} = \frac{x^{(k)} C^{(k)}}{B_{i}^{(k)}}
\]

Following [36], [38], given the transmit power \( P \) to offload the tasks to mobile edge device \( i \) at time slot \( k \) during \( T_{i}^{(k)} \), the H-IoT device energy consumption for offload computing \( E_{i}^{(k)} \) can be modelled as follows:

\[
E_{i}^{(k)} = \frac{x^{(k)} C^{(k)} P}{B_{i}^{(k)}}
\]
where \( b^{(k)}(t) \) is the battery level, \( C^{(k)}(t) \) denotes the computing task, \( \rho^{(k)}(t) \) represents the energy harvesting volume, and \( \chi(t) \) denotes the transactional size. Similar to related research [52], in the state transition model, the state transition from the current state \( s(t) \) to a new state \( s(t + 1) \) can be modeled as follows:

\[
s(t + 1) = f(s(t), a(t), r(t))
\]

where \( r(t) \) is the randomness, \( s(t), s(t + 1) \in S(t), a(t) \in A(t) \), which shows that the state transition is controlled not only by the current action \( a(t) \) but also by random conditions, such as the energy harvesting conditions and the wireless communication conditions.

3) System action space
The DRL agent can dynamically choose actions to maximize the system reward. These actions at each epoch \( t \), including the offloading decision \( a_o(t) \), block size \( a_{bs}(t) \), and block interval \( a_{bi}(t) \), can be modelled as follows:

\[
A(t) = [a_o(t), a_{bs}(t), a_{bi}(t)]
\]

The offloading decision, which decides whether to process the computing task by local devices or to offload the computing task to edge server devices, can be defined as follows:

\[
a_o(t) = [a_{o1}(t), a_{o2}(t), ..., a_{oN}(t)]
\]

Following related studies [17], [47], the block size and block interval decision, which are important for optimizing the throughput of the proposed permissioned blockchain system, can be defined as follows:

\[
a_{bs}(t) \in [0.2, 0.4, ..., M_{bs}]
\]

\[
a_{bi}(t) \in [0.5, 1, ..., M_{bi}]
\]

where \( M_{bs} \) and \( M_{bi} \) represent the maximum block size and maximum block interval, respectively.

4) Reward function
The objective of this research is to jointly optimize the security and energy efficiency of the proposed H-IoT system to respond to the COVID-19 pandemic. This can be represented as a joint optimization problem to maximize the transactional throughput of the permissioned blockchain system and minimize the energy consumption of the H-IoT system. This implies that it is necessary to jointly optimize the offloading decision, block size, and block interval. The reward function can hence be represented as equation (14).

\[
\max \left\{ \sum_{t=1}^{T} (w_1 \Omega - (1 - w_1)w_2 E^{(k)}) \right\}
\]

\[
C1 : \rho^{(k)}(t) \leq \max(b^{(k)})
\]

\[
C2 : b^{(k)}(t) > 0
\]

where \( C1 \) represents the amount of energy harvested from available resources, which cannot exceed the maximum battery level, and \( C2 \) denotes that the H-IoT system will drop the computing task when the battery level is insufficient.

The reward function can be illustrated as follows:

\[
r_t = \begin{cases} O^{(k)}, & \text{if } C1, C2 \text{ are satisfied} \\ 0, & \text{otherwise} \end{cases}
\]

Where \( O^{(k)} = w_1 \Omega - (1 - w_1)w_2 E^{(k)} \).

IV. DRL METHODS FOR H-IoT SYSTEM
The details of the DRL algorithm are presented in this section. It also includes the comparison of two mainstream DRL algorithms and the pseudocode of the proposed DRL algorithm. Growing DRL algorithms are often employed in IoT areas to address the MDP problem [44]. However, considering the special features of the H-IoT system, only DRL algorithms that can fit discrete action spaces are discussed in this research. Therefore, the deep Q-network (DQN) algorithm [53] and A3C [54] are used in this research. In addition, we compare the performance of the DQN and A3C with that of the random algorithm, which means the agents will randomly choose available actions without considering the complex scenarios [36]. The comparison results are shown in Figure 2. In Figure 2, the blue solid line represents the average reward of the A3C algorithm, while the orange dashed line and green dashed line denote the performance of the DQN algorithm and random algorithm, respectively. Both the DQN and A3C algorithms achieve better performance than the random algorithm. This demonstrates the validity of these two algorithms. Although the DQN algorithm can obtain a large average reward quickly, their results fluctuate as the episode number increases, and it is difficult for the DQN algorithm to obtain a stable and good performance. The A3C algorithm is much more robust and can achieve...
stable and good performance with an increasing number of episodes.

In addition, according to the simulation results in [54], the A3C algorithm is more robust than other DRL algorithms. Therefore, we chose the A3C algorithm to address our joint optimization problem. In addition to its robust performance, the A3C algorithm can take advantage of the benefits of both the value-based and policy-based methods. In addition, it fits both the discrete and continuous action spaces.

According to [54], [55], the A3C algorithm adopts a single deep neural network to approximate both the policy and the value function. It maintains a policy function \( \pi(a_t|s_t; \theta) \), which can be approximated by a softmax layer and an estimate of the value function \( V(s_t; \theta_v) \), which can be output by a linear layer. Because the agents share the network parameters in A3C, the policy and value functions need to update the weights and parameters after every \( t_{max} \) step action, or when they reach a terminal state. Following related studies [17], [30], [55], there are two cost functions in the A3C algorithm associated with the two deep neural network outputs; for the policy function, the cost function can be defined as follows:

\[
    f_\pi(\theta) = \log \pi(a_t|s_t; \theta)(R_t - V(s_t; \theta_v)) + \beta H(\pi(s_t; \theta))
\]  

(16)

where \( \theta \) and \( \theta_v \) are the parameters, while \( H(\pi(s_t; \theta)) \) is an entropy term, and the parameter \( \beta \) controls the strength of the entropy regularization term. In function 16, \( R_t \) denotes the estimated discounted reward in the time interval from \( t \) to \( t + k \), which can be defined as follows:

\[
    R_t = \sum_{i=0}^{k-1} \gamma^i r_{t+i} + \gamma^k V(s_{t+k}; \theta_v)
\]  

(17)

where \( k \) is upper bounded by \( t_{max} \), \( r_{t+i} \) denotes the immediate reward, and \( \gamma \) indicates the discount factor, with \( \gamma \in (0, 1] \).

In addition, the cost function for the estimated value function can be modelled as follows:

\[
    f_v(\theta_v) = (R_t - V(s_t; \theta_v))^2
\]  

(18)

In terms of [54], [55], the gradient of policy function \( f_\pi(\theta) \) with respect to parameter \( \theta \) can be defined as follows:

\[
    \nabla_\theta f_\pi(\theta) = \nabla_\theta \log \pi(a_t|s_t; \theta)(R_t - V(s_t; \theta_v)) + \beta \nabla_\theta H(\pi(s_t; \theta))
\]  

(19)

The gradient of the value function \( f_v(\theta_v) \) with respect to parameter \( \theta_v \), can be represented as follows:

\[
    \nabla_{\theta_v} f_v(\theta_v) = 2(R_t - V(s_t; \theta_v))\nabla_{\theta_v} V(s_t; \theta_v)
\]  

(20)

Following related studies [17], [30], [54], [55], the standard non-centered RMSProp algorithm is used to optimize both the policy functions and the value functions, which can be illustrated as follows.

\[
    g = ag + (1 - a)\Delta \theta^2
\]  

\[ (21) \]

\[
    \theta \leftarrow \theta - \eta \frac{\Delta \theta}{\sqrt{g + \epsilon}}
\]  

(22)

where \( a \) indicates the momentum, \( \Delta \theta \) represents the accumulated gradient of the cost functions, \( \eta \) denotes the learning rate, and \( \epsilon \) is a small positive parameter.

In terms of related studies [17], [30], [54], the pseudocode of the A3C algorithm is described in Algorithm 1 as follows.

**Algorithm 1** A3C based joint optimization algorithm for H-IoT

1: Initial global parameters \( \theta, \theta_v \), and global step counter \( T = 0 \)
2: Initial related parameters \( T_{max}, t_{max}, \) discount factor \( \gamma \), learning rate \( \eta \), number of agents \( W \), and \( \epsilon \)
3: Initialize local parameters \( \theta', \theta_v' \), and local step counter \( t = 1 \)
4: for each episode do
5:     for \( w = 1 \) to \( W \) do
6:         Reset global gradient \( d\theta = 0 \) and \( d\theta_v = 0 \)
7:     \quad Synchronize local parameters \( \theta' = \theta \) and \( \theta_v' = \theta_v \)
8:     \quad Set \( t_{start} = t \) and get state \( S(t) \)
9:     \quad repeat
10:        \quad Perform \( a_t \) according to policy \( \pi(a_t|s_t; \theta') \)
11:        \quad Receive reward \( r_t \) and new state \( s_{t+1} \)
12:        \quad \quad t = t + 1
13:        \quad until terminal \( s_t \) or \( t - t_{start} = t_{max} \)
14:        \quad if terminal \( s_t \) then
15:            \quad \quad \( R = 0 \)
16:        \quad else
17:            \quad \quad \( R = V(s_t, \theta_v') \)
18:        \quad end if
19:        \quad for \( i = t - 1 \) to \( t_{start} \) do
20:            \quad \quad \( R = r_t + \gamma R \)
21:        \quad end for
22:        \quad Asynchronous update weight parameter \( \theta \) and \( \theta_v \)
23:     \quad end for
24: \quad end for
25: \end for
26: \end for

V. SIMULATION RESULTS

In this section, extensive simulations are conducted to evaluate the proposed H-IoT system. The simulation parameters and numerical results are as follows:

The simulation was conducted using PyTorch on a Python-based PyCharm platform. In detail, the CPU of the computer
is an Intel Core i9-10900k with 64 GB memory, while the GPU is an Nvidia GeForce RTX 3090 with 24 GB memory. The software is PyTorch 1.7.1 with Python 3.8 on Windows 10. An H-IoT system composed of an MEC system with some MEC server devices, a permissioned blockchain system, and several H-IoT devices is presented. Extensive simulations were conducted to evaluate the performance of the proposed H-IoT system. The details of the main simulation are presented in Table 3.

To evaluate the performance of the proposed method, we compared the results with the following three schemes:

- **Proposed scheme with fixed block size:** The scheme uses the same method as the proposed scheme, except that the block size is fixed for a permissioned blockchain system;
- **Proposed scheme with fixed block interval:** The scheme adopts a fixed block generating interval for the permissioned blockchain system, and the other parameters are the same as those of the proposed scheme;
- **Proposed Scheme with Only Offloading:** The scheme does not process computing tasks by local devices; all the computing tasks are offloaded to the MEC server devices.

Because the learning rate is crucial for the DRL algorithm, we evaluated the performance of the proposed A3C algorithm under different learning rates, and the results are shown in Figure 3.

As illustrated in Figure 3, the green dashed line is higher than the orange dashed line in most episodes, while the blue solid line performs better in the majority of the time. This demonstrates that the learning rate of 1e-4 has the best average reward in most episodes. Therefore, we chose this rate to conduct further simulation.

The comprehensive comparison of the four different schemes is demonstrated in Figure 4 as follows.

### TABLE 3. The main simulation parameters

| Parameters   | Definitions                        | Values                  |
|--------------|-----------------------------------|-------------------------|
| $M_{bs}$     | Maximum block size                | 8M [17, 30, 47]         |
| $M_{bi}$     | Maximum block interval            | 10s [30, 47]            |
| $\chi$       | Average transaction size          | 200KB [17]              |
| $P$          | Transmission power                | 2W [16, 51]             |
| $p_{h(k)}$   | Energy harvesting                 | 0.001J [16]             |
| $max_{k}h(k)$| Maximum battery level             | 3.2mJ [16]              |
| $\mu$        | Effective capacitance coefficient | $10^{-28}$ [16, 51]     |
| $f_{m}$      | CPU cycle frequency               | 1.5GHz [16, 51]         |
In addition, we explored the performance of the proposed scheme under different conditions, and the results are presented in Figures 5, 6, and 7.

First, the effects of computing tasks are presented in Figure 5.

In Figure 5, all four types of lines decrease with an increase in the computing task. This is mainly because the growing computing task will increase the energy consumption. In addition, the proposed scheme (the blue solid line) also obtains the largest average reward at most times. This shows the performance of the proposed scheme when dealing with different computing tasks.

Second, the effects of average transaction sizes are illustrated in Figure 6.

As shown in Figure 6, the average rewards of the four proposed schemes all decrease with increasing average transaction size, while the proposed scheme (the blue solid line) achieves the highest value most times. The increase in the average transaction size will reduce the throughput of the proposed permissioned blockchain system, which can reduce the average reward.

Third, the effects of the maximum block size are presented in Figure 7.

In Figure 7, the performance of the four proposed schemes increases with an increase in the maximum block size, whereas the proposed scheme (the blue solid line) has the highest value in the majority of the time. The fixed block size of the proposed scheme with a fixed block size (green dashed line) changed with the maximum block size. The proposed scheme (blue solid line) also performs best most times. The performance of the four proposed schemes increases with an increase in the maximum block size. This is because the number of transactions in a block increases with the increase in the maximum block size, which can improve the throughput of the proposed permissioned blockchain system.

VI. DISCUSSION

The COVID-19 pandemic has not only caused severe consequences globally but has also impacted on the healthcare industry, especially in terms of pandemic prevention and control. Although an increasing number of H-IoT applications have already been applied to respond to the pandemic, most of them do not address both security and energy efficiency issues. In this research, the permissioned blockchain method and DRL method are adopted to guarantee the security and energy efficiency of the applications of H-IoT systems in the COVID-19 pandemic area.

Since it is difficult to conduct field experiments, this research adopts simulation methods to evaluate the performance of the proposed H-IoT system. Although the simulation results can demonstrate the effects of the proposed system, they cannot reflect complex real-world situations, especially for large-scale applications. Therefore, field experiments should not be neglected. In addition, there are still...
other challenges for H-IoT to be addressed, including latency and real-time operation issues.

VII. CONCLUSION

To improve the performance of the H-IoT system to mitigate the impact of COVID-19 globally, a security and energy-efficient H-IoT system for COVID-19 has been developed in this research. The proposed system not only ensures security by using a permissioned blockchain system but also reduces the energy consumption by offloading tasks to MEC server devices as well as by capturing energy using energy-harvesting devices. In addition, a DRL algorithm is employed to optimize both the throughput of the blockchain systems and the energy efficiency of the proposed H-IoT system. The extensive simulation results demonstrate that the proposed system can balance both the throughput of the permissioned blockchain system and the energy efficiency of the H-IoT system. This illustrates that the proposed methods can alleviate the H-IoT system’s security and energy efficiency issues, thereby improving the performance of H-IoT systems in mitigating the impact of COVID-19.

Future research will focus on two main directions. First, we will study how to apply the proposed H-IoT system to real-world healthcare applications to alleviate the security and energy efficiency concerns during COVID-19 pandemic control, this will imply that more factors need to be considered. Second, we plan to further study the combination of blockchain and DRL to address more complex applications in H-IoT areas, such as real-time H-IoT applications and big data-related H-IoT applications.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[2] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, “The future of healthcare internet of things: a survey of emerging technologies,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020.
[3] H. Habibzadeh, K. Dinesh, O. R. Shishavan, A. Boggio-Dandry, G. Sharma, and T. Soyata, “A survey of healthcare internet of things (hiot): A clinical perspective,” IEEE Internet of Things Journal, vol. 7, no. 1, pp. 53–71, 2019.
[4] M. Abdel-Basset, V. Chang, and N. A. Nabeeh, “An intelligent framework using disruptive technologies for covid-19 analysis,” Technological Forecasting and Social Change, vol. 163, p. 120431, 2021.
[5] G. Aceto, V. Persico, and A. Pescapé, “Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0,” Journal of Industrial Information Integration, vol. 18, p. 100129, 2020.
[6] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scaffham, “The internet of things: Impact and implications for health care delivery,” Journal of medical Internet research, vol. 22, no. 11, p. e20135, 2020.
[7] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, “Digital technology and covid-19,” Nature medicine, vol. 26, no. 4, pp. 459–461, 2020.
[8] Y. Dong and Y.-D. Yao, “Iot platform for covid-19 prevention and control: A survey,” IEEE Access, vol. 9, pp. 49929–49941, 2021.
[9] S. Elagang, S. F. Abdelwahab, E. Zanaty, M. H. Alkinnan, H. Alotaibi, and M. E. Zanaty, “Remote diagnostic and detection of coronavirus disease (covid-19) system based on intelligent healthcare and internet of things,” Results in Physics, vol. 22, p. 103910, 2021.
[10] H. K. Kim and C. W. Lee, “Relationships among healthcare digitalization, social capital, and supply chain performance in the healthcare manufacturing industry,” International Journal of Environmental Research and Public Health, vol. 18, no. 4, p. 1417, 2021.
[11] X. Xu, H. Zhao, H. Yao, and S. Wang, “A blockchain-enabled energy-efficient data collection system for unassisted iot,” IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2431–2443, 2020.
[12] M. S. Ali, M. Vecchio, M. Pinchera, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the internet of things: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2018.
[13] H.-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for internet of things: A survey,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, 2019.
[14] A. Fusco, G. Dicuonzo, V. Delli’Atti, and M. Tatullo, “Blockchain in healthcare: Insights on covid-19,” International Journal of Environmental Research and Public Health, vol. 17, no. 9, p. 7167, 2020.
[15] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, “Learning-based computation offloading for iot devices with energy harvesting,” IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1930–1948, 2019.
[16] J. Zhang, J. Du, Y. Shen, and J. Wang, “Dynamic computation offloading with energy harvesting devices: A hybrid decision-based deep reinforcement learning approach,” IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9303–9317, 2020.
[17] J. Feng, F. R. Yu, Q. Pei, X. Chu, J. Du, and L. Zhu, “Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6214–6228, 2019.
[18] L. M. Pang, M. Piran, D. Han, K. Min, H. Moon et al., “A survey on internet of things and cloud computing for healthcare,” Electronics, vol. 8, no. 7, p. 768, 2019.
[19] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, “A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and big in managing its impact,” ieee access, vol. 8, pp. 90 225–90 265, 2020.
[20] P. Chatterjee, A. Tesis, L. J. Cumberknop, and R. L. Armentano, “Internet of things and artificial intelligence in healthcare during covid-19 pandemic—a south american perspective,” Frontiers in Public Health, vol. 8, 2020.
[21] W. Li, Y. Chai, F. Khan, S. R. U. Jan, S. Verma, V. G. Menon, X. Li et al., “A comprehensive survey on machine learning-based big data analytics for iot-enabled smart healthcare system,” Mobile Networks and Applications, pp. 1–19, 2021.
[22] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, “A review on the role of machine learning in enabling iot based healthcare applications,” IEEE Access, vol. 9, pp. 38 859–38 890, 2021.
[23] N. Taimoor and S. Rehman, “Reliable and resilient ai and iot-based personalised healthcare services: A survey,” IEEE Access, vol. 10, pp. 535–563, 2021.
[24] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain, “Privacy-enhanced data fusion for covid-19 applications in intelligent internet of medical things,” IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15 683–15 693, 2020.
[25] T. Alatif, A. M. Tehame, S. Bajba, A. Barnawi, and S. Zia, “Machine and deep learning towards covid-19 diagnosis and treatment: survey, challenges, and future directions,” International Journal of Environmental Research and Public Health, vol. 18, no. 3, p. 1117, 2021.
[26] Y. Ming, X. Yu, and X. Shen, “Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare internet of things,” IEEE Access, vol. 8, pp. 153 561–153 576, 2020.
[27] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain technologies for the internet of things: Research issues and challenges,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2018.
[28] R. Huo, S. Zeng, W. Zhang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, “A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges,” IEEE Communications Surveys & Tutorials, 2022.
[29] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, “Deep reinforcement learning for blockchain in industrial iot: A survey,” Computer Networks, vol. 191, p. 108004, 2022.
[30] L. Liu, J. Feng, Q. Pei, C. Chen, Y. Ming, B. Shang, and M. Dong, “Blockchain-enabled secure data sharing scheme in mobile-edge comput-
[31] J. Yun, Y. Goh, and J.-M. Chung, “Dnn-based optimization framework for secure shared blockchain systems,” IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2342–2353, 2020.

[32] Y. Mao, J. Zhang, and K. B. Letaief, “Dynamic computation offloading for mobile-edge computing with energy harvesting devices,” IEEE Journal on Selected Areas in Communications, vol. 34, no. 12, pp. 3590–3605, 2016.

[33] Z. Wan, H. Li, H. He, and D. Prokhorov, “Model-free real-time ev charging scheduling based on deep reinforcement learning,” IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5246–5257, 2018.

[34] M. Babaeizadeh, I. Frosio, S. Tyree, J. Clemons, and J. Kautz, “Reinforcement learning through asynchronous advantage actor-critic on a gpu,” arXiv preprint arXiv:1611.06256, 2016.

[35] ZHICHAO LI received the B.S. degree from the China University of Geoscience, in 2003, the M.S. degree from the Renmin University of China, in 2005, and the Ph.D. degree from Tsinghua University, China, in 2013. He is currently an Associate Professor with the School of International and Public Affairs, Shanghai Jiao Tong University. His research interests include emergency management, social network analysis and network governance.

[36] LONG LIU received the Ph.D. degree from the University of Science and Technology of China, in 2015. He is currently a distinguished associate professor at the School of Political Science and Public Administration, East China University of Political Science and Law. His research interests including mobile computing, governance, public administration and public policy.