Journal of New Media
DOI:10.32604/jnm.2021.024543
Article

Blockchain-Based Decentralized Reputation Management System for Internet of Everything in 6G-Enabled Cybertwin Architecture

Meimin Wang, Zhili Zhou* and Chun Ding

Nanjing University of Information Science & Technology, Nanjing, 210044, China
*Corresponding Author: Zhili Zhou. Email: zhou_zhili@163.com
Received: 21 October 2021; Accepted: 26 October 2021

Abstract: Internet of Everything (IoE) has emerged as a promising paradigm for the purpose of connecting and exchanging data among physical objects and humans over the Internet, and it can be widely applied in the fields of industry, transportation, commerce, and education. Recently, the emergence of 6G-enabled cybertwin network architecture provides the technical and theoretical foundation for the realization of IoE paradigm. However, the IoE has three open issues in the 6G-enabled cybertwin architecture, i.e., data authenticity, data storage and node reliability. To address these issues, we propose a blockchain-based decentralized reputation management system (BC-DRMS) for IoE in 6G-enabled Cybertwin architecture. In the proposed BC-DRMS, the traffic data collected from end nodes is stored on the blockchain and the decentralized file system, i.e., InterPlanetary File System (IPFS), to resist data tampering, and then the data is further processed by the edge clouds and core clouds to provide services to users. Also, a multi-level reputation evaluation scheme is designed to compute the reputation scores of IoE nodes to prevent malicious node attacks. The experiment results and analysis demonstrate that, compared to the traditional centralized reputation management systems (CRMS), the proposed BC-DRMS cannot only address the issues of data authenticity and storage, but also provides high reliability for IoE in 6G-enabled cybertwin architecture.

Keywords: 6G; blockchain; cybertwin network; reputation management system; Internet of Everything

1 Introduction

The Internet of Things (IoT) is a dynamic, global network infrastructure that connects millions of physical devices to the internet. As pointed out by the Internet Business Solutions Group (IBSG) of Cisco company [1], we are currently in the era of IoT. With the rapid development of intelligent hardware devices and communication technologies, the "things" add more capabilities including context awareness, increased processing power, and energy independence, and more people and new types of information are connected to the Internet. Consequently, we are rapidly entering the era of Internet of Everything (IoE). In contrast to IoT, IoE connects billions of humans, processes and things in a more valuable and significant network [2]. Moreover, IoE pays more attention to intelligent network connection and technology based on IoT infrastructure. Therefore, IoE has become the promising network paradigm, and it can offer wide application in many fields, such as industry [3,4], transportation [5,6], commerce [7], and education [8]. Although IoE can provide important values and benefits in real-word applications, it still faces huge challenges [5,9], including complex and dense network connections, frequent and abundant data exchanges, and massive data process and analysis. Limited by current communication technologies and network architecture, high latency and many other factors cannot meet the requirements of IoE.

Recently, many countries have declared that they are rolling out 5G [10–12], i.e., fifth-generation wireless technology for digital cellular network. Meanwhile, some researchers have begun to focus on the research of a new communication technology beyond 5G, i.e., 6G [13], which will lead to much faster communication with lower latency than 5G. However, due to the limitations of the current network architecture, we cannot realize the IoE by only using 6G. To update the network architecture for IoE, recently, Peng Cheng Lab [14–16] introduced a new network architecture called Cybertwin Network for 6G, i.e., 6G-enabled Cybertwin network [16], which is cloud centric network architecture consisting of three main roles: end nodes, edge clouds, and core clouds, as shown in Fig. 1. By representing humans and things in the virtual cyberspace, 6G-enabled Cybertwin has multiple capacities, including communications assistant, network behavior logger, and digital asset owner.

Due to the characteristics of 6G-enabled Cybertwin [16], it is possible to realize IoE in 6G-enabled Cybertwin network. However, there are three new challenges when using 6G-assistant Cybertwin Network for IoE. 1) Data Authenticity: the traffic data transmitted or exchanged in the networks would be intercepted or tampered by malicious attackers, which will affect the data authenticity for real-world applications. 2) Data Storage: Since massive traffic data is continuously produced every day in the networks, how to effectively store these data is a challenging problem. 3) Node Reliability: As there may be some faulty nodes and malicious nodes in the networks, it is also required to ensure reliability of nodes.

To deal with the above challenges, it is necessary to establish a blockchain based decentralized reputation management system (BC-DRMS) to ensure the authenticity and storage of the traffic data and the trustworthiness of nodes for IoE in 6G-enabled Cybertwin network architecture. In the proposed BC-DRMS, the traffic data collected from end nodes is stored on the blockchain [17] and the decentralized file system, i.e., Interplanetary File System (IPFS) [18], to resist data tampering operations. Then, the data is further processed by the edge clouds and core clouds to provide services to users. Also, based on the stored and processed data, a multi-level reputation evaluation scheme is designed to compute the reputation scores of IoE nodes to prevent malicious node attacks. The main contributions of the proposed BC-DRMS are summarized as follows.

1) We are the first to introduce the blockchain technique to design the reputation management system for IoE in 6G-enabled Cybertwin. Due to the decentralized and traceable characteristics of blockchain, it is hard to tamper traffic data stored on blockchain by malicious attackers. Thus, the authenticity of data is protected well in the proposed BC-DRMS.

2) A multi-level reputation evaluation scheme is designed to separately compute the reputation scores of nodes, edge clouds, and core clouds with the consideration of both subjective and objective aspects. Consequently, the impacts of faulty nodes and malicious nodes can be minimized, and thus the reliability of IoE nodes are further strengthened greatly.

3) The data storage strategy using IPFS. In the proposed BC-DRMS, the decentralized file system, i.e., IPFS, is employed to deal with the storage problem in big data scenario of IoE. The massive traffic data is effectively stored in the IPFS with a distributed manner, and then the hash addresses of the traffic data is automatically stored on the blockchain via smart contract. Compared to the traditional centralized file system and data transmission solution, the IPFS cannot only store massive traffic data but also enhance the stability of system in such manner.

The reminder of this paper is organized as follows. Section 2 introduces the related work, and Section 3 details the proposed BC-DRMS for IoE in 6G-enabled Cybertwin architecture. Section 4 analyzes the experiment results. Finally, conclusions are drawn in Section 5.

2 Related Work

To the best of our knowledge, there is few reputation management systems designed for IoE environment. We review the existing trust and reputation management systems for the other networks such as the traditional peer-to-peer (P2P) networks and IoT networks. To enhance the security of the system and the trustworthiness of nodes, a variety of trust and reputation management systems have been proposed.

These systems can be roughly divided into two categories [19]: centralized reputation management systems (CRMSs) and decentralized reputation management systems (DRMS).

2.1 Blockchain Technologies

Blockchain: In 2008, Satoshi Nakamoto first proposed the concept of Blockchain in [20]. Essentially, blockchain is a digital ledger distributed on a network without central authority and repository. Blockchain contains a set of chained blocks. The first block is called the genesis block. Each block after the genesis block contains a block header and block data. Where, the block header represents the hash value of previous block, while block data records the transaction data over a period of time. Each node in the network can access all the recorded information in the blockchain. In recent years, the blockchain systems such as Ethereum [17] and Hyperledger [21] have been widely adopted in a variety of practical applications such as transportation [22,23], education [24–26], e-commerce [27], and IoT [28,29].

IPFS: To address the problem of big data storage, the decentralized storage system is proposed [18], i.e., InterPlanetary File System (IPFS). The IPFS is content addressable, peer-to-peer, open source, a globally distributed file system that can be used for storing and sharing a large volume of files with high throughput [18]. Instead of relying on a central server, IPFS does not need any central server, and it distributes the data to different nodes of the system.

In IPFS, each file will be assigned a unique hash value and organized by Merkle DAG structure. Once one uploads a file to IPFS, he can obtain a unique address (a hash string) returned by IPFS. By using the file address, he can also access and download the file from IPFS.

Smart Contract: The term “smart contract” was first proposed by Szabo in 1994 [30], which is defined as “a computerized transaction protocol which conducts the terms of a contract” [30]. Subsequently, Szabo recommended to transform the terms of a contract to a string of code and embed it into an appropriate environment, so as to run the code automatically. Consequently, compared to the traditional contracts, the smart contract can enhance the transaction efficiency between the participants significantly and reduce the occurrence of malicious or accidental exceptions largely.

Generally, the smart contracts are predefined and deployed on the blockchain, and each node of the network can call the smart contracts by sending a transaction to it. By receiving the transaction data, the smart contracts conduct automatically on the blockchain [30–32]. It is notable that all nodes executing a same smart contract will obtain the same result from the execution, and the execution result is recorded on the blockchain.

2.2 Centralized Reputation Management System

In the traditional Client/Server (C/S) networks, the service providers including the governments, organizations and companies have established centralized reputation management systems (CRMS) to prevent the malicious behaviors of nodes in the system to provide better service for users. In web applications, service providers usually store data in a centralized server, as done by Amazon, Alibaba, Google, etc. The P2P networks do not use the traditional Client/Server (C/S) scheme, and each node connected to the P2P networks is equal. In P2P networks, some researchers have also proposed CRMSs for various real-world applications such as vehicle network [33,34], healthcare [35,36], finance [37,38], education [39–41], etc., based on the P2P networks.

However, in the C/S networks and P2P networks, all the traffic data and reputation data are controlled by the centralized server. If there are some malicious employees who can access the centralized server, these data can be easily tampered, which will lead to serious security issue. Therefore, although the CRMSs in C/S and P2P networks have improved service quality significantly, there are still fundamental security problems: the limited data authenticity and the low trustworthiness of nodes.

2.3 Decentralized Reputation Management System

As mentioned above, as all the traffic data and reputation data are controlled by the centralized server,

the existing CRMSs cannot be able to solve the problems of data authenticity and node trustworthiness. In recent years, some blockchain-based decentralized reputation management systems (BC-DRMSs) [42–46] have been proposed to compute and manage the traffic data and reputation scores.

In addition to the DRMS proposed for IoT/sensors, some trust and reputation models and systems were proposed and built for e-commerce [27], education [47], VANET [43], autonomous systems. These trust and reputation systems use blockchain and smart contract to prevent malicious attacks including tampering, unfair rating and collusion, and thus the stability and security of the system are enhanced significantly. In these BC-DRMSs, all the traffic data and reputation data are stored on the blockchain. However, with the continuous increase of these data and occurrence of other types of data such as images, voices, and videos, it is hard to store and process these data by merely using blockchain. Moreover, all of these BC-DRMSs are designed for other application environment rather than the IoE environment.

In the IoE era, as huge number of connected nodes are connected and communicated and massive traffic data is produced every day, it hard to directly apply the existing BC-DRMSs to address the security and trustworthiness issues of IoE. Recently, the occurrence of 6G-enabled cybertwin architecture supports the realization of IoE. Thus, in this paper, we focus on the design of BC-DRMS to address the issues of data authenticity, data storage and node reliability for the IoE in 6G-assistant Cybertwin Network.

3 6G-Enabled Cybertwin Network Architecture

In this section, we introduce the 6G-enabled Cybertwin Network architecture. In [14–16], the cloud-centric Internet architecture, i.e., 6G-enabled Cybertwin network architecture, was proposed by Peng Cheng Lab.

The 6G-enabled Cybertwin can represent humans, process and things in digital form, and serve as communication assistant, network behavior logger, and digital asset manager of humans, process and things for IoE. Different from end-to-end communication model, this architecture establishes the connection between the end nodes (e.g., sensors, smartphone, terminal devices, etc.) and clouds by 6G communication technologies to process data and provide the services for users.

To ensure the functionality, scalability and flexibility of the network architecture, in 6G-enabled Cybertwin, three infrastructure components are designed, i.e., the End Nodes, the Edge Clouds and the Core Clouds. Each component is detailed as follows:

The End Node-level: In the IoE environment, the nodes not only include objects but also humans and things, and the server providers can offer services to all of them. Accordingly, in end node-level of 6G-enabled Cybertwin, the nodes refer to objects, humans and things, as shown in Fig. 1. They are not only the consumers of network service through various access methods of the network, but also the source of data in the system. In these nodes, some of them are in charge of data collection and exchange, while some peripheral nodes are mainly responsible for transmitting data to the Edge Clouds using 6G communication technologies for further preprocessing.

Edge Cloud-level: The Edge Clouds reside between the Core Clouds and the End Nodes. They provide less services than the Core Clouds for the users, but they response more rapidly to the end nodes' request than the Core clouds. Therefore, Edge Clouds can help the Core Clouds in providing high-quality services for users.

Core Cloud-level: The Core Clouds are fully connected to establish a core network by high-speed 6G communication technology. These core clouds provide infrastructure services including computing, caching, and communication resource to the end nodes.

However, in 6G-enabled Cybertwin, and the data communicated between levels would suffer the tampering operations, and the End Nodes, Edge Clouds, and Core Clouds would contain some fragile and unreliable nodes. Moreover, how to store and manage the massive data is also a challenging task. Therefore, it is challenging to ensure the data authenticity, reliability, and data storage for the IoE in the 6G-enabled Cybertwin Network. To deal with the above challenges, in next section, we propose the BC-DRMS for IoE in 6G-enabled Cybertwin network architecture.

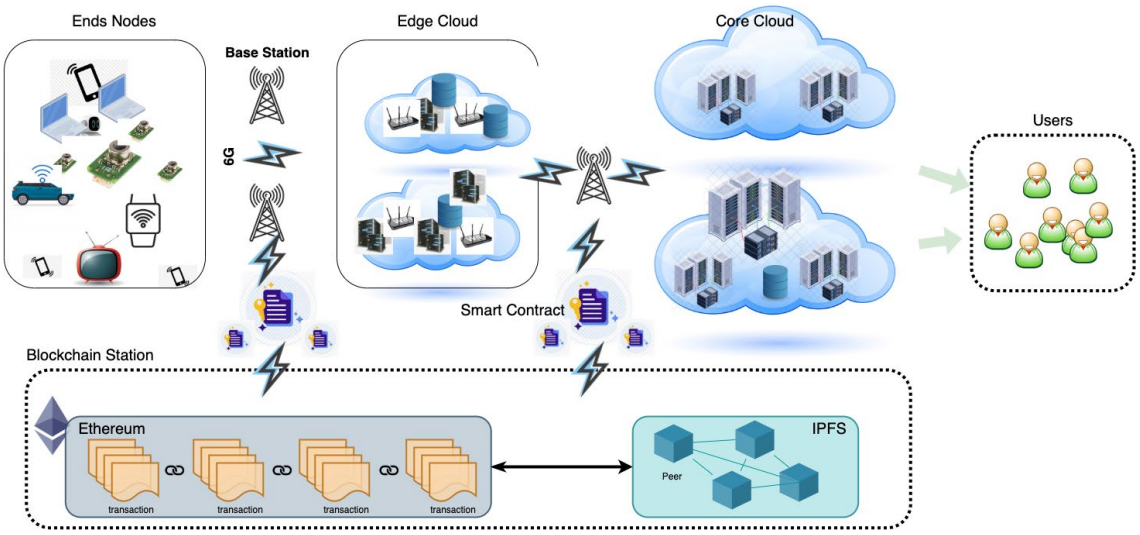

Figure 1: The framework of the proposed BC-DRMS for IoE in 6G-enabled Cybertwin Network. From left to right, there are the End Nodes, the Edge Clouds and Core Clouds, and the blockchain is shown at the bottom. Reputation information and other data exchange and transmission among different levels through 6G communication technology

4 The Proposed BC-DRMS For IoE in 6G-Enabled Cybertwin Network

In this section, we elaborate the proposed BC-DRMS for the IoE in 6G-enabled Cybertwin Network architecture. In Section 3, we first describe the framework of the proposed blockchain-based decentralized reputation management system (BC-DRMS) in 6G-enabled Cybertwin Network. Subsequently, in Section 4.2, the proposed multi-level reputation evaluation scheme is described. Finally, in Section 4.3, we introduce the data storage strategy using the IPFS to store the data in IoE.

4.1 The Framework of BC-DRMS

The framework of BC-DRMS for IoE in 6G-enabled Cybertwin Network is illustrated in Fig. 1. In our proposed BC-DRMS, the Ethereum blockchain, Smart Contract, and IPFS are employed to process and store the data in different levels of the 6G-enabled Cybertwin Network. The main steps of data generation and storage process are described as follows:

Step (1): The raw data collection by End Nodes. A large number of End Nodes deployed in the real environment collect real-world raw data by sensors or data collection devices, such as weather data sensors and traffic-data collection devices.

Step (2): The reputation score computation. In this process, the behaviors of End Nodes are stored by the Ethereum blockchain through designed smart contract, and the reputation scores of End Nodes are computed objectively and updated by the proposed multi-level reputation evaluation scheme.

Step (3): The data storage. The data collected by End Nodes and the reputation scores are uploaded on the IPFS by communication protocol (TCP/IP protocol), and then the hash addresses representing the data are returned to Ethereum blockchain by calling the function of designed smart contract.

Step (4): The data transmission from End Nodes to Edge Clouds. The peripheral End Nodes send the collected raw data to the Edge Clouds through 6G transmission technology for further preprocessing.

Step (5): The use of data by Edge Clouds according to the reputation scores. The peripheral Edge Clouds preprocess the acquired data. First, they obtain the corresponding reputation scores from Ethereum through the device ID information in the request. Then, they determine whether to use the data provided by the device for preprocessing and caching through the reputation of the corresponding device.

Step (6): The data transmission from Edge Cloud to Core Clouds. The Edge Clouds store the data in IPFS, and then the hash address of the data is returned to the Ethereum blockchain by calling the function of the smart contract deployed on Ethereum blockchain. Afterward, Core Clouds receive the event notification of data storage to provide the corresponding services according to the users' request.

Step (7): Service providing by Core Clouds. After receiving the data, Core Clouds provide the service to the Edge Clouds or the End Nodes as well as human users.

Step (8): The reputation scores of services given by users. After the users receives services provided by Core Clouds, the quality of services is subjectively evaluated to compute the reputation scores. Where, the reputation evaluation of the services is performed in a decentralized environment. These evaluation scores are stored in the Ethereum blockchain and IPFS through the smart contract.

By the above evaluation process in all levels of 6G-enabled Cybertwin Network, the node reliability can be effectively enhanced. Moreover, almost all data produced in the 6G-enabled Cybertwin Network are stored in IPFS by the smart contract function and the corresponding address is returned to the Ethereum blockchain. Due to the decentralized characteristics of blockchain and IPFS, the issues of data authenticity and data storage can be addressed well.

4.2 Reputation Evaluation Scheme

In this subsection, we design the multi-level reputation evaluation scheme. After Edge Clouds receive the device data in the End Node-level, End nodes will obtain the reputation score of a node ID, denoted as R_{ID}, from Ethereum blockchain. Where, the range of R_{ID} is $[-1,1]$. The reputation score $\mathrm{R_{ID}}$ is computed as follows:

$$R_{ID} = \alpha R_{ID}^{S} + \beta \sum_{S \in \mathcal{S}} R_{S \to ID}^{O} + \gamma \sum_{E \in \mathcal{E}} R_{E \to ID} \quad (1)$$

where $R_{ID}^{S} \in [-1,1]$ and $R_{ID}^{O} \in [-1,1]$ are the subjective scores evaluated by users and the objective scores evaluated by the other Core Clouds in the same level, respectively. Moreover, $R_{E \to ID}$ represents the reputatio n evaluation from the Edge Clouds $E \in \mathcal{E}$ in the cross level. In addition, α, β and γ represent the factors to balance the final reputation computation result.

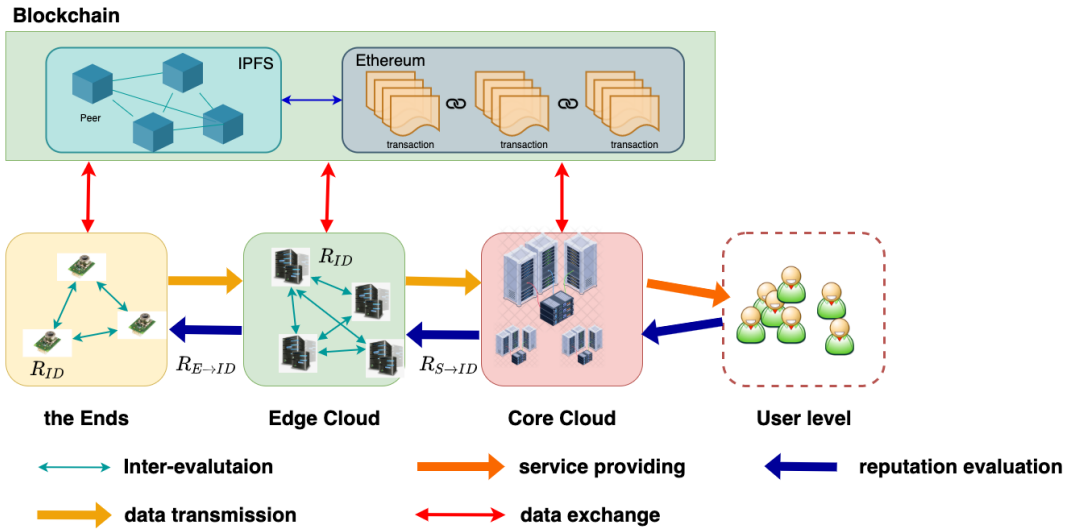

Figure 2: The reputation evaluation scheme in our proposed BC-DRMS for IoE in 6G-enabled Cybertwin Network

Subjective evaluation: In traditional IoT environment, the Core Clouds, i.e., service providers, directly register and manage the End Nodes and monitor their status in real-time. On the contrary, in the IoE environment, End Notes and services may not belong to the same holder or center. Thus, the Core Clouds

only need to receive the data through the interface specified by the physical device manufacturer without the management of these devices. As a result, some malicious nodes will take negative impacts on the service. In the proposed reputation evaluation scheme, the Core Clouds are allowed to subjectively evaluate the End Nodes with their ID information such as IP hash addresses.

Objective evaluation: In the IoE environment, End Nodes are fully-connected in a complex form. It is difficult for humans to manage and evaluate all nodes. Thus, we also design an objective reputation model for these nodes according to their historical behavior information such as data exchange and connection. Objective reputation score is calculated as follows:

$$R_{ID}^{O} = f(\boldsymbol{a_1}, \boldsymbol{a_2}, \cdots, \boldsymbol{a_n}) \tag{2}$$

where $\boldsymbol{a}_t$ represents a behavior vector at time t and function $f(\cdot)$ represents the computation rule deployed on the smart contract. In our simulation experiment, at a period of time t, we define the behavior of each node as the amount of data transmission denoted as B_{ID}^{t} and the times of data exchanges denoted C_{ID}^{t} with other nodes.

The whole system is the structure of multiple levels, including End Node-level, Edge Cloud level, Core Cloud level, and users-level from the left-right. Thus, not only evaluating the nodes by each other at same-level, we also consider cross-level reputation evaluation. The reputation scores are evaluated from the upper-levels to the lower-levels.

In the Edge Cloud-level, the edge nodes filter the abnormal data before preprocessing the data from the End Nodes according to the reputation scores stored on the Ethereum blockchain. Meanwhile, the edge nodes update the reputation scores of these End Nodes. To determine whether the data transmitted by End notes is abnormal, we adopt the clustering algorithm (e.g., K-means) to evaluate the abnormality to compute the reputation scores. Denote the distance between data point x and clustering center point c by

$$d = sim(\boldsymbol{x}, \boldsymbol{c}) \tag{3}$$

where c represents the clustering center. The function $sim: \mathbb{R}^D \times \mathbb{R}^D \to [0, +\infty)$ represents the distance metric such as Euclidean distance between the data. Afterwards, the reputation is computed from the cross-level by

$$R_{E \to ID} = \sigma(d) \tag{4}$$

where $\sigma(\cdot)$ is a function that computes the reputation score by using the distance between this data point x and the clustering center point c as input. As shown in Fig. 3, when the data is far from the clustering center, the reputation score is equal to a very small value; Otherwise, the node will gain high reputation score, that is

$$\lim_{d \to \infty} \sigma(d) = -1 \tag{5}$$

and

$$\sigma(0) = r \tag{6}$$

where, the reputation r is the maximum value when the data point $\boldsymbol{x}$ is at the center of data collected by devices.

In the Core Cloud-level, not only evaluating the reputation scores of Core Clouds by the Edge Clouds, the Core Clouds need to be evaluated by users subjectively in the above manner. It is notable that, according to different services, the Core Clouds can design different smart contracts to obtain the user's evaluation scores.

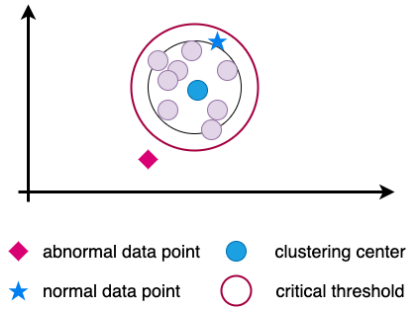

Figure 3: The data clustering in feature space. The star point represents that the data

Overall, the reputation evaluation scheme combines the subjective and objective evaluation in the same-level and cross-level to sufficiently evaluate the reputation scores of nodes and clouds in the 6G-enabled Cybertwin Network.

4.3 Data Storage Strategy

In the IoE environment, the system will generate massive traffic data in a short period of time. Thus, it is required to address the issue of data storage with the suitable and scalable storage technology. In addition, the reputation data also needs to be stored in the security database. In this paper, we adopt IPFS to store the traffic data and reputation data produced by nodes, clouds, and users in the 6G-enabled Cybertwin Network.

In the proposed BC-DRMS, we employ a decentralized storage system, i.e., IPFS, instead of centralized mechanism. The data generated in the system will be first stored in IPFS by 6G transmission technology and transmission protocol request. After the storage is completed, IPFS will return a hash address string of the data. Meanwhile, the smart contract deployed on Ethereum blockchain is called to store the hash address of the data in the blockchain. If the nodes need to access the data, they can obtain it from IPFS through the hash address stored on the blockchain.

The steps of storing the traffic data and reputation data to IPFS is given as follows:

Step (1) Smart contract design: In Core Cloud-level, a smart contract is designed and deployed on the Ethereum blockchain. The smart contract consists of two key functions: reputation evaluation function and data storage function. Some properties in smart contract are also included such as the node IDs, timesteps for data producing and reputation evaluating, hash address of raw data in IPFS.

Step (2) Data storage: Generally, raw data is divided into several data blocks and a distributed hash table (DHT) is established. Afterward, these DHTs representing data are organized through the Merkle DAG data structure. Finally, the index stored at the root node of the tree is used as the file's addressing hash value.

Step (3) Uploading address on Ethereum blockchain: After IPFS returns the hash address of raw data, the address with node information will be uploaded on the Ethereum blockchain by invoking the function defined in the smart contract.

Step (4) Status update: When the status in the smart contract is updated, the event is triggered and listened by the Core Clouds to provide the services for users.

In current network architecture, there is an issue of bad real-time in blockchain. In 6G-enabled Cybertwin Network, a cloud network operating system that can work in a distributed manner via establishing a real-time market driven trading platform for multi-agents according to [16]. Thus, the data storage strategy using IPFS in 6G-enabled Cybertwin Network can address the issue of bad real-time. Moreover, we adopt IPFS to store the traffic data and reputation data. Due to the decentralized storage in the data storage strategy, the issue of the single point of failure (SPOF) can be avoided effectively. These are beneficial for the stability of system.

5 Performance Evaluation and System Analysis

In this section, we demonstrate the security, reliability, and stability of the proposed BC-DRMS by a series of simulation experiments. In the simulation environment, we establish a simulation network topology as shown in Fig. 4 by Software Defined Networking (SDN) and Network Function Virtualization (NFV). In addition, the Ethereum blockchain and IPFS system are established offline by go-ethereum (Geth) [17] and IPFS toolkits.

In addition to simulation experiments, we further discuss and analyze the security, reliability, and stability of our proposed BC-DRMS for IoE in 6G-enabled Cybertwin Network architecture.

5.1 Authenticity

To verify the security of the data in BC-DRMS, we conduct the experiments from the End Nodes and the Edge Clouds. We designed, developed and deployed an indoor-air quality assessment service for humans. In this service, first, some sensor nodes collect air quality data (such as carbon dioxide, oxygen, and air humidity) in real-time. Subsequently, these data will be aggregated to the Edge Clouds for preprocessing. Finally, the data will be transmitted to Core Clouds for evaluation and prediction based on the air quality model, and the results will be fed back to the users' mobile terminal devices. We control the generation of malicious nodes at different levels and in different proportions to provide interference data to test the direct impact on the standard results, which represent the accuracy of air quality in range of [0,1].

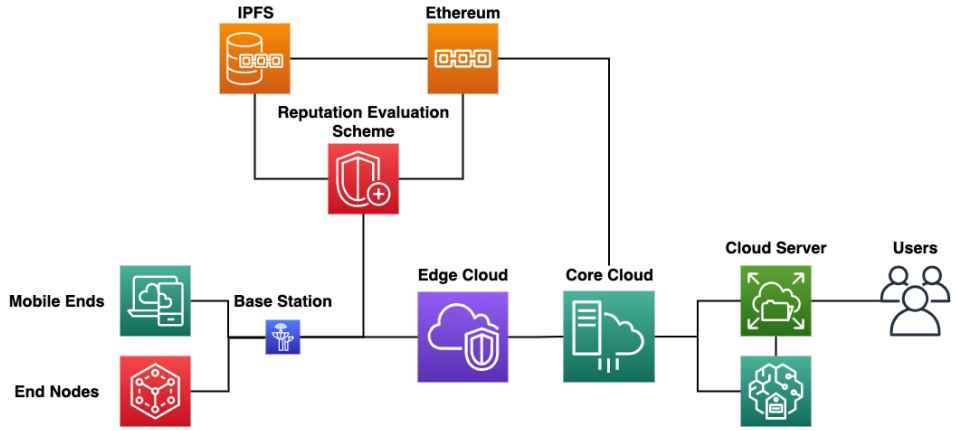

Figure 4: The topology structure of our simulation experiments

Generally, as shown in Table 1, malicious nodes cannot take a particularly large impact on the accuracy of air quality assessment when there are nearly 5K~1M sensors collecting air quality data. Moreover, in any case, no node can tamper the data stored on the blockchain in the IoE environment. As the sophisticated deep learning-based technology [48] is used to train the air quality model in Core Cloud-level, the data provided by a large number of malicious nodes will not follow the assumption of independent identified distribution (i.i.d). Therefore, with the increase of malicious nodes, the accuracy of air quality prediction will decrease.

In the End node-level, the nodes such sensors can only collect data from the real-world and exchange data with other device nodes. However, in Edge Cloud-level, malicious cloud nodes can process data purposefully to disrupt the operation of the system. Therefore, the existence of malicious nodes in Edge Cloud-level can threaten the system more than those in the End Node-level.

Table 1: The effect of different malicious attacking rates (MAR) on the accuracy of air quality assessment

Malicious nodes in different levels	MAR (%)	Accuracy (%)
The End node-level	5	92.53
	20	93.14
	40	90.34
	65	90.07
The Edge Cloud-level	5	91.74
	20	89.53
	40	84.67
	65	79.35

Finally, in any case, malicious nodes cannot tamper the data collected and processed by normal nodes, due to the decentralized characteristics of Ethereum blockchain and IPFS technologies used in proposed BC-DRMS.

5.2 Reliability

In the proposed BC-DRMS, in addition to data security, node reliability is another challenge for IoE in 6G-enabled Cybertwin Network. As the multi-level reputation evaluation scheme is designed and used to comprehensively compute the reputation scores of different nodes, it is hard for malicious nodes to gain high reputation scores by SPOF attack and collusion for the following reason.

For the SPOF attack, due to the multi-level reputation scheme, the Edge Clouds give a reputation penalty for the nodes that maliciously provide the data, and thus it is hard for the malicious nodes to disrupt the system. In addition to objective evaluation, the Core Clouds' subjective evaluation of malicious devices or nodes can also prevent malicious damage.

Another way to disrupt the system is collusion, i.e., multiple malicious nodes transmit and process data to each other to achieve high reputation scores to gain the trust of the system and users. However, the multi-level and subjective-objective combination evaluation scheme and decentralized storage mechanism make the reputation of malicious node groups converge gradually. As shown in Fig. 5, without subjective evaluation, the number of malicious nodes will significantly affect the accuracy of air quality assessment. As the trustworthy nodes in the Edge Cloud-level evaluate the data provided by malicious nodes according to the clustering algorithm, the reputation scores of the malicious nodes will gradually converge, as shown in Fig. 6. In addition, as the number of malicious nodes increases, the effects of their attacks on the system do not increase significantly. Thus, the negative effects of malicious nodes on the system are limited.

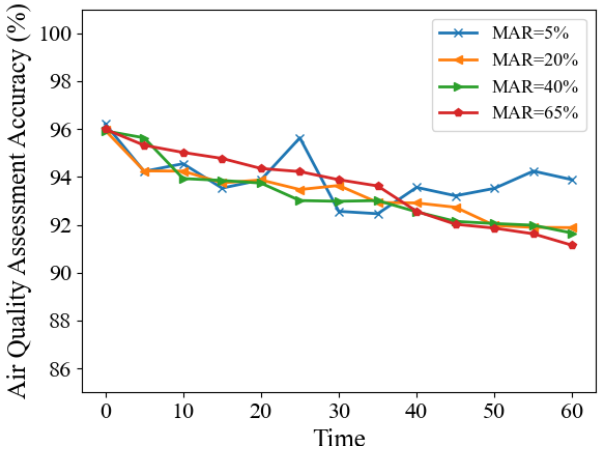

Figure 5: The effects of malicious node group in different levels on the accuracy of air quality assessment

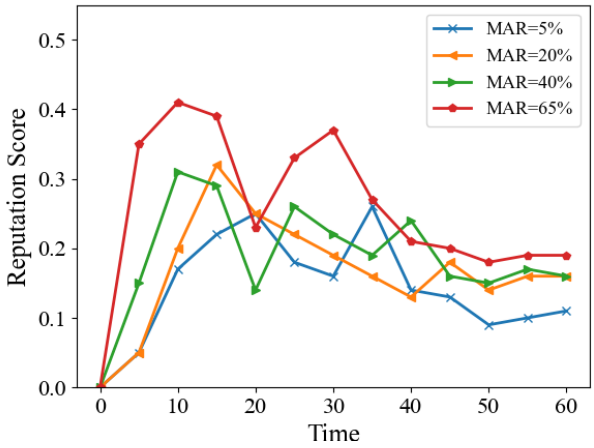

Figure 6: The effects of malicious node group in different levels on average reputation

5.3 Stability

In the IoE environment, the storage of massive data including traffic data and reputation data is another challenge.

The proposed data storage strategy is designed for IoE on 6G-enabled Cybertwin Network. Cybertwin Network's cloud operating system enables better real-time performance in a decentralized environment than the traditional end-to-end network architecture. Thus, the proposed data storage strategy can avoid the bad real-time problem.

In the proposed data storage strategy, the decentralized file system, i.e., IPFS, is used to store the data. Compared with hypertext transfer protocol, i.e., HTTP, IPFS has superiority in solving the issue of SPOF. Moreover, the storage strategy based on the hash address of file content will only store the same piece of data once in the network to minimize the data redundancy.

In our experiments, we simulate nearly 5K devices and continuously generate abundant data for air quality assessment. When there are a large number of storage nodes in IPFS, the access of the data stored on IPFS will get very low latency compared to data request from a centralized server via TCP/IP.

6 Conclusion

In this paper, we focus on addressing the issues of data authenticity, data storage and node reliability for IoE in 6G-enabled Cybertwin Network architecture. To this end, we have presented a blockchain-based decentralized reputation management system (BC-DRMS) for the IoE environment in 6G-enabled Cybertwin Network.

In BC-DRMS, the data in the entire system will be stored on the Ethereum blockchain and IPFS. Due to their decentralized characteristics, it is hard to tamper the data stored on them, which ensures the data authenticity. Moreover, the multi-level, subjective-objective combination reputation evaluation scheme is proposed to improve the node reliability of BC-DRMS. In addition, to store a large amount of data in the IoE environment, we adopt IPFS to store these data and upload the hash addresses to Ethereum blockchain through a smart contract. Consequently, IPFS storage strategy effectively improves the stability of the system and avoids the problem of the SPOF.

Acknowledgement: Thanks to the supervisor for writing guidance and other colleagues in the laboratory for their help.

Funding Statement: This work was supported in part by the National Natural Science Foundation of China under Grants 61972205, U1836208, U1836110, in part by the National Key R&D Program of China under Grant 2018YFB1003205, in part by MOST under Contract 108-2221-E-259-009-MY2 throSugh Pervasive

Artificial Intelligence Research (PAIR) Labs (Taiwan), in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund, and in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund (China).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton and J. Henry, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press, 2017.

[2] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," *Internet Technologies and Applications*, pp. 219–224, 2015.

[3] S. Hiriyannaiah, S. G. Matt, K. G. Srinivasa and L. M. Patnaik, "A multi-layered framework for Internet of Everything (IoE) via wireless communication and distributed computing in Industry 4.0," *Recent Patents on Engineering*, vol. 14, no. 4, pp. 521–529, 2020.

[4] M. Sanchez, E. Exposito and J. Aguilar, "Industry 4.0: Survey from a system integration perspective," *International Journal of Computer Integrated Manufacturing*, vol. 33, no. 10–11, pp. 1017–1041, 2020.

[5] Y. Liu, H. N. Dai, Q. Wang, M. K. Shukla and M. Imran, "Unmanned aerial vehicle for Internet of Everything: Opportunities and challenges," *Computer Communications*, vol. 155, pp. 66–83, 2020.

[6] J. P. Queralta, T. N. Gia, H. Tenhunen and T. Westerlund, "Collaborative mapping with ioe-based heterogeneous vehicles for enhanced situational awareness," in *IEEE Sensors Applications Sym.*, pp. 1–6, 2019.

[7] S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of Everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[8] H. D. Mohammadian and F. Rezaie, "The role of IoE-Education in the 5th wave theory readiness & its effect on SME 4.0 HR competencies," in *IEEE Global Engineering Education Conf.*, pp. 1604–1613, 2020.

[9] A. Raj and S. Prakash, "Internet of Everything: A survey based on architecture, issues and challenges," in *5th IEEE Uttar Pradesh Section Int. Conf. on Electrical, Electronics and Computer Engineering*, pp. 1–6, 2018.

[10] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch *et al.,* "Scenarios for 5G mobile and wireless communications: The vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[11] N. Hassan, K. L. A. Yau and C. Wu, "Edge computing in 5G: A review," *IEEE Access*, vol. 7, pp. 127276–127289, 2019.

[12] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu *et al.,* "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[13] W. Saad, M. Bennis and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2019.

[14] M. Dong and L. Fu, "Cybertwin-based network architecture," 2019. [Online]. Available: http://apb.regions.comsoc.org/files/2019/06/AP-Newsletter-No-55-May-2019Final.pdf.

[15] Q. Yu, J. Ren, Y. Fu, Y. Li and W. Zhang, "Cybertwin: An origin of next generation network architecture," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 111–117, 2019.

[16] Q. Yu, J. Ren, H. Zhou and W. Zhang, "A cybertwin based network architecture for 6G," in *2nd 6G Wireless Summit*, pp. 1–5, 2020.

[17] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[18] J. Benet, "Ipfs-content addressed, versioned, P2P file system," arXiv:1407.3561, 2014.

[19] E. Bellini, Y. Iraqi and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020.

[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.

[21] C. Cachin, "Architecture of the hyperledger blockchain fabric," 2016. [Online]. Available: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[22] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Computer Networks*, vol. 145, pp. 219–231, 2018.

[23] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," arXiv:1708.09721, 2017.

[24] G. Chen, B. Xu, M. Lu and N. S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, pp. 1–10, 2018.

[25] A. Alammary, S. Alhazmi, M. Almasri and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, pp. 2400, 2019.

[26] G. Srivastava, S. Dhar, A. D. Dwivedi and J. Crichigno, "Blockchain education," in *IEEE Canadian Conf. of Electrical and Computer Engineering*, pp. 1–5, 2019.

[27] Z. Zhou, M. Wang, C. N. Yang, Z. Fu, S. Xin *et al.,* "Blockchain-based decentralized reputation system in E-commerce environment," *Future Generation Computer Systems*, 2021.

[28] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

[29] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," in *19th Int. Conf. on Advanced Communication Technology*, pp. 464–467, 2017.

[30] B. K. Mohanta, S. S. Panda and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *9th Int. Conf. on Computing, Communication and Networking Technologies,* pp. 1–4, 2018.

[31] Y. Huang, Y. Bian, R. Li, J. L. Zhao and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019.

[32] B. Bünz, S. Agrawal, M. Zamani and D. Boneh, "Zether: Towards privacy in a smart contract world" in *Int. Conf. on Financial Cryptography and Data Security*, pp. 423–443, 2020.

[33] L. Yang, T. Mo and H. Li, "Research on V2V communication based on peer to peer network" in *Int. Conf. on Intelligent Autonomous Systems*, pp. 105–110, 2018.

[34] L. Yang and H. Li, "Vehicle-to-vehicle communication based on a peer-to-peer network with graph theory and consensus algorithm," *IET Intelligent Transport Systems*, vol. 13, no. 2, pp. 280–285, 2019.

[35] S. Fox, "After Dr Google: Peer-to-peer health care," *Pediatrics*, vol. 131, no. Supplement 4, pp. S224–S225, 2013.

[36] E. Sillence, C. Hardy and P. Briggs, "Why don't we trust health websites that help us help each other? An analysis of online peer-to-peer healthcare," in *ACM WebSci*, pp. 396–404, 2013.

[37] S. C. Moenninghoff and A. Wieandt, "The future of peer-to-peer finance," *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung*, vol. 65, no. 5, pp. 466–487, 2013.

[38] L. Einav, C. Farronato and J. Levin, "Peer-to-peer markets," *Annual Review of Economics*, vol. 8, pp. 615–635, 2016.

[39] S. J. Yang, "Context aware ubiquitous learning environments for peer-to-peer collaborative learning," *Journal of Educational Technology & Society*, vol. 9, no. 1, pp. 188–201, 2006.

[40] J. M. Juedes, "Outcomes of peer education on student learning in higher education," *Journal of Student Affairs*, vol. 20, pp. 77, 2010.

[41] J. A. Latino and C. M. Unite, "Providing academic support through peer education," *New Directions for Higher Education*, vol. 157, pp. 31–43, 2012.

[42] D. Liu, A. Alahmadi, J. Ni, X. Lin and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019.

[43] Z. Lu, Q. Wang, G. Qu and Z. Liu, "Bars: A blockchain-based anonymous reputation system for trust management in vanets" in *17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int. Conf. on Big Data Science and Engineering*, pp. 98–103, 2018.

[44] Z. Yang, K. Zheng, K. Yang and V. C. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *IEEE 28th Annual Int. Sym. on Personal, Indoor, and Mobile Radio Communications*, pp. 1–5, 2017.

[45] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *10th Int. Conf. for Internet Technology and Secured Transactions*, pp. 131–138, 2015.

[46] R. Dennis and G. Owenson, "Rep on the roll: A peer to peer reputation system based on a rolling blockchain," *International Journal for Digital Society*, vol. 7, no. 1, pp. 1123–1134, 2016.

[47] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conf. on Technology Enhanced Learning*, pp. 490–496, 2016.

[48] X. Li, L. Peng, Y. Hu, J. Shao and T. Chi, "Deep learning architecture for air quality predictions," *Environmental Science and Pollution Research*, vol. 23, no. 22, pp. 22408–22417, 2016.