Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks

Weizhi Meng, *Senior Member, IEEE*, Wenjuan Li, *Student Member, IEEE*, and Liqiu Zhu

***Abstract*—Internet of Things (IoT) has gradually become one of the most important platforms across different disciplines, by enabling dedicated physical objects to communicate with other Internet-enabled things. With this trend, more devices in medical environments are capable of connecting with each other, named Internet of Medical Things (IoMT). It aims for improving efficiency and reducing communication delay, e.g., monitoring the status of patients and notifying abnormal events. However, due to the distributed nature, insider attacks are still one of the major threats to such IoT environment. How to improve the trust management in IoMT remains a challenge. Motivated by the popularity of blockchain technology, in this paper, our general goal is to investigate the performance of blockchain-based trust management. In particular, we focus on a particular type of IoMT, named medical smartphone networks (MSNs), because of the wide adoption of smartphones in the medical domain. Then, we apply blockchains for enhancing the effectiveness of Bayesian inference-based trust management to detect malicious nodes in MSNs. In the evaluation, we explore the performance of our approach in two different healthcare environments, and experimental results demonstrate that blockchain technology can help improve the detection efficiency of detecting malicious nodes with reasonable workload.**

***Index Terms*—Bayesian inference, blockchain technology, insider attack, Internet of Things (IoT), intrusion detection, medical smartphone network (MSN), trust management.**

I. Introduction

Internet of Things (IoT) is the connection of physical devices to the Internet via embedded equipment to sense, exchange, and interact with each other. It can make a big impact on people's daily lives, i.e., building a smart-home environment by connecting refrigerators and coffee makers. The IDC IoT decision-maker survey indicated that up to 65% respondents were deploying IoT solutions, or have a plan to implement based on the feedback from almost 5000 respondents across 25 countries [21]. According to the Deloitte report, a large number of companies will invest around 310 billion USD on IoT by 2020, across different disciplines such as manufacturing, energy, and transportation industries [9]. In addition to these, IoT has also been gradually adopted in the healthcare industry. The Internet of Medical Things (IoMT) is helping transform the healthcare industry in a more intelligent era, i.e., allowing real-time intervention, and machine-to-machine communication [1], [39]. It can monitor the patients' status, forward the data to healthcare providers, and notify important events.

With the convenience and capability of mobile devices, smartphones have become one common device in various healthcare organizations such as hospitals to help reduce communication cost and delay. Many studies reported that the rapid growth of mobile health market is due to the emergence of smartphone application [22], and smartphones are a good information-transfer station for personalized medical data acquisition [17]. For example, smartphone can play an important role in monitoring and sharing the electrocardiogram (ECG) data with an IoT environment to help the diagnosis of certain heart diseases [53]. As a result, these devices construct a special network, called medical smartphone network (MSN) [30]. It can be regarded as one special type of IoMT, where various Internet-enabled medical smartphones connect with each other and facilitate the operations of healthcare professionals.

In practice, the IoT ecosystem has a very complicated architecture, which results in an interdependent system. It allows different components to exchange information with each other, including real-time data collection, physical connection, data analysis, end-to-end application control, etc. [1]. The IoMT and MSN can provide many benefits to the healthcare industry, but they are also faced with the same technological vulnerabilities as the traditional networked techniques, i.e., subject to more stringent scrutiny [46]. A report from the Atlantic Council and Intel Security [19] identified that the number of reported information security breaches in the healthcare industry has increased 60% from 2013 to 2014, which is mostly two times than the number in other fields. This indicates that how to protect the patient's privacy and sensitive data still remains a big concern and challenge.

Manuscript received February 26, 2019; revised May 1, 2019; accepted June 3, 2019. Review of this manuscript was arranged by Department Editor K. K. R. Choo. *(Corresponding author: Wenjuan Li.)*

W. Meng is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Lyngby, Denmark (e-mail: weme@dtu.dk).

W. Li is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Lyngby, Denmark, and also with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: wenjuan.li@my.city.edu.hk).

L. Zhu is with the FinTech Startup, Macao 999078, China (e-mail: lqzhu@ct.mo).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2019.2921736

A. Motivation

As the healthcare data are mostly sensitive such as patients' record and diagnosis, many hackers consider healthcare information to be especially valuable for financial purposes. As an example, there was a serious data breach in Singapore, in which up to 1.5 million healthcare patients' personal data including their Prime Minister were comprised [41]. Therefore, the IoMT and MSN could have become a major target by cyberattackers. More specifically, due to the distributed nature, insider attacks are one of the major threats to IoMT and MSN. For instance, if an attacker successfully compromises a networked device, many other attacks or exploits could be committed via this device. Hence, the design of appropriate trust mechanisms in the IoMT and MSN is very necessary and important.

B. Contributions

Traditionally, healthcare organizations may deploy one central server to handle most tasks such as performing trust management. This can facilitate many operations, but the server itself may be vulnerable to overloaded traffic or events as a single point of failure. With the recent popularity and adoption of blockchain technology, it is found that it can provide a platform for mutually unknown parties to communicate without the need of a trusted third party [6], [32]. In this paper, we focus on insider attacks, and attempt to design a blockchain-based trust management scheme to help defend MSNs against insider attacks. Our contributions in this paper can be summarized as follows.

1) In this paper, we first introduce the background of MSN and then design a blockchain-based trust management scheme based on Bayesian inference to help enhance the accuracy of detecting malicious insider nodes. Our approach allows different MSN nodes to check the events in the blockchain and to build a verified chain of malicious events.
2) In the evaluation, we conducted two experiments to evaluate the performance of blockchain-based trust management in collaboration with two different healthcare organizations. Our experimental results demonstrate that our approach by integrating blockchains can help enhance the detection performance as compared with the original and other similar approaches, with reasonable workload.

It is worth emphasizing that we limit our discussion on how to defense against insider attacks in this paper, while the intrusion detection systems (IDSs) improvement is out of the scope. In addition, our proposed approach was tested in the healthcare industry, but it has a potential to be deployed in other domains. This paper attempts to complement the existing literature and stimulate more research in building trust management with blockchain technology.

The rest of this paper is organized as follows. In Section II, we introduce the background of MSNs and review relevant research studies on defeating insider attacks. Section III describes how to use Bayesian inference to evaluate trustworthiness of a node and our blockchain-based trust management scheme. Section IV presents our evaluation environments and settings, and analyzes the results. Section V discusses some limitations and open challenges in this field. Finally, Section VI concludes this paper.

II. Background and Related Work

In this section, we introduce the MSN architecture and related work on defeating insider attacks including various intrusion detection mechanisms and trust management schemes.

A. MSN Background

Currently, information and communications technology has been gradually adopted in the healthcare industry, making the communication easier between patients and healthcare professionals. Smartphone is one of the most important devices that has been implemented in various healthcare organizations, helping reduce cost, manage data access, and control outcomes. It also provides many easy-to-use applications for patients to record data and notify healthcare professionals about the status in a timely manner. For example, top pharmaceutical companies have developed 63% more applications in 2014 over 2013 [8]. In [17], Guo introduced a smartphone-powered electrochemical biosensing dongle, allowing healthcare professionals to access patients' biomedical record and provide precise and personalized treatment. Yang *et al.* [53] presented an IoMT that used smartphones to collect patients' ECG data in real time and send to the corresponding healthcare organizations for timely checking.

These Internet-enabled mobile phones thus construct an emerging network platform, called MSN [30], [31], which can be treated as one particular type of IoMT. Fig. 1 depicts the high-level architecture of MSNs. According to the connection scope, MSNs can be classified into local MSNs and wide MSNs. The former mainly refer to smartphones within a healthcare organization, while the latter further contain the smartphones outside the organization, i.e., the devices used by patients in their living places. For the wide MSNs, patients' devices can communicate with local MSNs via the Internet. Similar to a traditional network, each device in the MSN can be treated as a (network) node.

In particular, MSNs are expected to provide many benefits to both patients and healthcare providers (e.g., healthcare professionals) [1].

1) Handling emergency situations for patients in a timely manner.
2) Reducing financial cost and communication delay for patients.
3) Optimizing resource and infrastructure management for healthcare providers.
4) Reducing response time for healthcare providers in case of any unexpected situations.

However, due to the sensitive information exchanged within such MSNs, they may become a major target by cyber-criminals. For example, an attacker can pretend to be a patient and then try to compromise a mobile device in MSNs. Then, the intruder can launch other attacks via the infected device (or MSN node), e.g., spoofing attack, scanning, and spreading malware. As a result, it is very important to develop proper security mechanisms to

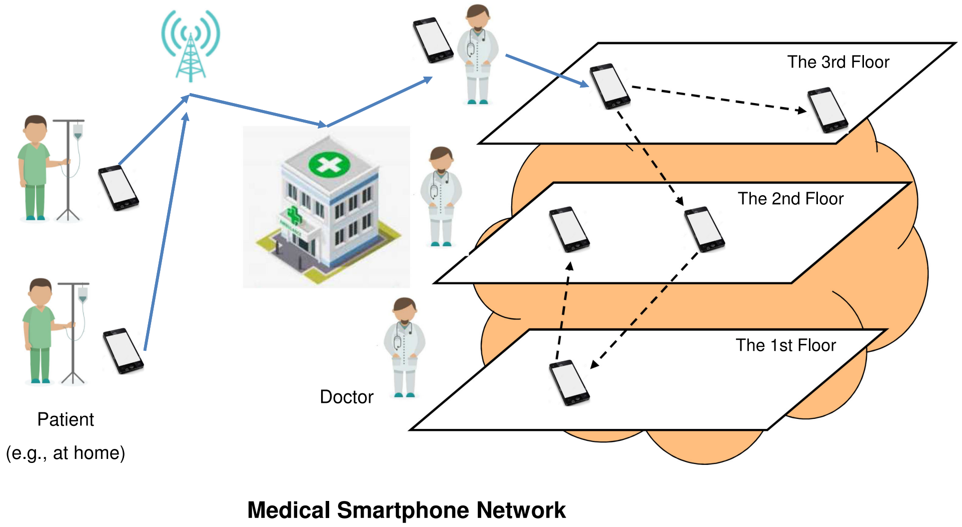

Fig. 1. High-level architecture of MSNs.

defend against insider attacks, i.e., identifying malicious nodes. On the basis of the observations in [30] and [34] (i.e., a survey with a total of 12 healthcare organizations), it was found that the mechanism is expected to be dynamic and centralized, enabling full-time monitoring and management.

B. *Related Work*

In practice, IDS is one most commonly deployed mechanism for protecting different kinds of networks, including healthcare networks. An IDS can be categorized as rule-based IDS and anomaly based IDS. In particular, a rule-based IDS detects potential attacks by comparing the existing events with its stored signatures [38]. An anomaly based IDS figures out a malicious event by discovering a deviation between the current profile and the predefined normal profile [14]. An alarm will be generated if any potential threats are found.

1) Collaborative Intrusion Detection and Trust Management: To improve the detection capability of a single IDS, collaborative intrusion detection has been widely deployed in many practical environments [47], [58]. Although it is known that insider attacks (internal attacks) are one big concern for collaborative systems. In this case, trust management is necessary for securing such kinds of networks against insider attacks. The term of *trust* borrowed from social science, which is used to help measure and predict the reputation of objects [15]. For instance, Probst and Kasera [37] proposed a type of distributed trust among sensor nodes to identify malfunctioning, malicious sensor nodes, and minimize their impact on applications. By analyzing the behavior of sensor nodes, their approach could compute statistical trust values and decide a confidence interval around the trust reputation.

Li *et al.* [23] identified that most distributed IDSs were heavily depended on either centralized fusion or distributed fusion, making the communication mechanisms unscalable. To mitigate this issue, they proposed a distributed detector with the emerging decentralized location and routing infrastructure. As they assumed that all peers are trusted, their approach was vulnerable to insider attacks, i.e., betrayal attacks where some nodes may suddenly become malicious. Then, Fung *et al.* [11] described a host-based IDS collaboration framework that allows each IDS node to send challenges and evaluate the trustworthiness of others based on its own experience. They also employed a forgetting factor, which could highlight the impact of the recently obtained experience. To further improve the detection performance, Li *et al.* [24] identified that not all IDSs have the same level of sensitivity in detecting any kinds of intrusions, and the detection accuracy should rely on their own signatures and deployed machine learning algorithms. They thus proposed a notion of *intrusion sensitivity* and investigated its performance in computing trust values of different IDS nodes. They then designed an intrusion sensitivity-based trust management model to enhance the robustness of CIDSs [25], and applied a machine learning-based approach to help allocate this value in an automatic way [26]. More relevant studies on trust-based IDS are available such as [12], [27], [29], [33], [35], and [43].

2) Trust Management in Wireless Sensor Networks (WSNs): Trust management with different theories has also been studied to protect WSNs against various internal attacks [7]. Guo *et al.* [18] showed how to compute reputation based on grey theory and fuzzy sets. Their approach considered the relation among neighbor nodes and added weights to the important ones. Bao *et al.* [2] presented a hierarchical trust management framework to enhance the performance of IDSs in clustered WSNs. Their approach integrated two trust levels to help identify insider attacks: namely, quality-of-service trust and social trust. Their results indicated that a lower false positive rate of 5% could be achieved as compared with traditional anomaly detection.

Wang *et al.* [48] introduced a trust management approach for ad hoc networks (WANET) by defining two trust concepts: evidence chain and trust fluctuation. Probst and Kasera [37] proposed an approach by using statistical trust and a confidence interval to describe the trustworthiness of a WSN node. Shaikh *et al.* [42] introduced a group-based trust management scheme that could work for two types of network topology: *intragroup topology* and *intergroup topology*. The former is a distributed scheme, whereas the latter is a centralized scheme. Chen *et al.* [5] focused on the use of watchdog and designed an event-based trust management scheme. Their approach could monitor the behavior across various events and compute the trust ratings for WSN nodes.

Zhang *et al.* [57] introduced a trust management approach that could build trust reputation in a dynamic way for WSNs. They particularly considered direct trust and indirect trust for a group of nodes, and used a varying function to help adaptively assign more weight to the most recently obtained trust values. Zahariadis *et al.* [56] designed an ambient trust sensor routing (ATSR) protocol to handle network dimensions by adopting a similar trust model with direct and indirect trust computations. Sun and Li [45] introduced a routing protocol by combining multiple attributes to evaluate the reputation of MSN nodes, e.g., energy, data, communication, and recommendation. Their method particularly depends on a sliding time window to help discover the attack frequency and malicious events. Some other related work/surveys on trust management in WSNs can be referred in [13], [16], and [55].

III. Our Proposed Approach

In this section, we introduce the background of blockchains and show how to design a blockchain-based trust management based on Bayesian inference.

A. Background on Blockchains

Due to the popularity of Bitcoin application, blockchain technology has attracted much attention from both academia and industry. The initial goal of blockchains is to make payments between entities without a trust relationship and build a temper-resistant blockchain. A typical blockchain contains a list of records (called *blocks*) that will be chronologically ordered by discrete time stamps [51]. One block is connected with the front block using a cryptographic hash, where the first one is called *genesis* block. Different blockchain implementations may result in distinct block contents. A block usually has a payload, a timestamp, and a special class of hash functions calculated by all the previous blocks. A blockchain is often managed or controlled by a distributed network, which can offer a transparent and traceable data storage, i.e., protecting data integrity. In particular, the linked data in any block cannot be modified maliciously without the approval from the majority of participants [32].

Generally, there are three types of blockchains: namely, permissionless or called public blockchain, and permissioned blockchains [51]. The former allows any entity to join the chain as either a writer or a reader during the consensus process. Some examples for such kind of blockchains include Bitcoin [36], Zerocash [4], and Ethereum [50]. On the other hand, the latter limits the number of entities that can participate in the chain. Although such kind of blockchains can still be distributed amongst different locations, a private permissioned blockchain is often controlled by a single entity or a centralized entity. A consortium blockchain allows the consensus decisions to be made by a predefined group, in which each participating entity needs to register before they can join the network. In practice, restrictions would be posed on the writer role for both private permissioned and public blockchains during the consensus process. Differently, private permissioned blockchains do not allow any participant to read, but public permissioned blockchains allow any participant to have a read access. Hyperledger [20] is an example of permissioned blockchains.

To establish a distributed consensus protocol for validating and updating blocks, there are some major approaches in a network [32], [51].

1) *Proof of Work (PoW).* For such kind of scheme, a block can be accepted by a network node if the participant can prove that a predefined amount of computational resources (known as “work”) have been spent. The Bitcoin network has already implemented a hash function of SHA-256 [36].
2) *Proof of Stake.* This method achieves consensus by requesting users to stake an amount of their tokens for having a chance of being selected to validate blocks of transactions and get rewarded. The more a user stakes, the better their chance of being selected.
3) *Proof of Elapsed Time.* This method is a bit similar to PoW by replacing the demand for a mining intensive process with a randomized timer system. The efficiency can be reached by running this fair lottery system.

B. Bayesian Inference

Bayesian inference is a way to help formally apply prior knowledge for calculating statistical probabilities [44]. It is very helpful especially when there is not enough information but a need to predict the occurrence probability of related events. The Bayes’ theorem has been studied in computing networks, which assumes that a packet to be malicious in a common network has a probability of $1/2$. This implies that malicious event could be found in different ways, either in a single packet or in a series of packets.

To derive the trust computation equation, assuming that a node sends a total of N packets, in which k of them are found to be *normal*. According to relevant studies [15], [44], it is reasonably assumed that the distribution of observing $n(N) = k$ is governed by a Binomial distribution. This distribution describes that a group of independent n observations with the same occurrence probability of p. Then, we have the following equation:

$$P(n(N) = k|p) = \binom{N}{k} p^k (1-p)^{N-k}. \tag{1}$$

The ultimate goal of applying Bayesian inference is to predict the probability of $P(V_{N+1} = 1|n(N) = k)$, judging whether the $(N+1)$th packet is normal or not. On the basis of the Bayesian theorem, we can have the following probability distribution:

$$P(V_{N+1} = 1|n(N) = k) = \frac{P(V_{N+1} = 1, n(N) = k)}{P(n(N) = k)} \tag{2}$$

where $P(n_i : \text{normal}) = p$ represents the probability of the ith packet, V_i indicates that the i th packet is normal, and $n(N)$ represents the number of normal packets. For the above equation, we can apply the marginal probability distribution, which indicates that the probability of one random variable without being affected by any other random variables. We then can have the following two equations:

$$P(n(N)=k)=\int_0^1 P(n(N)=k|p)f(p)\cdot dp \tag{3}$$

$$P(V_{N+1}=1,n(N)=k)=\int_0^1 P(n(N)=k|p)f(p)p\cdot dp. \tag{4}$$

As there is no prior information about p, it is reasonably assumed that p is determined by a uniform prior distribution of $f(p)=1, p\in[0,1]$. On the basis of the above equations, from (1) to (4), we can have the following target equation:

$$\begin{aligned} P(V_{N+1}=1|n(N)=k) &= \frac{\int_0^1 P(n(N)=k|p)f(p)p\cdot dp}{\int_0^1 P(n(N)=k|p)f(p)\cdot dp} \\ &= \frac{k+1}{N+2}. \end{aligned} \tag{5}$$

In terms of (5), MSN nodes' reputation can be evaluated by recording the number of normal packets k and the total number of packets N. Given a proper trust threshold, we can label MSN nodes to be either malicious or normal. It is worth noting that more robust trust computation for a node can be achieved by observing the network after a period of time, instead of judging by only several malicious packets. This is because some false positives may degrade the detection accuracy.

C. Blockchain-Based Trust Management

How to protect connected medical devices from being compromised has received much attention. A report from SANS institute [40] figures out that up to 94% of different healthcare organizations including their medical devices and infrastructure have ever been hacked by cyber-criminals. There is a great need to integrate medical devices with the protection of security mechanisms [49]. For example, if one device in MSNs is infected, then attackers can exploit other devices via the compromised one. Due to the distributed nature, insider attacks are a big challenge for IoMT and MSN.

As mentioned earlier, trust-based IDS is one essential and important security mechanism to help defeat insider attacks. Meng *et al.* [31] designed a trust-based IDS based on Euclidean distance and behavioral profiling. Then, they introduced how to use Bayesian inference to detect untruthful nodes in MSNs [30]. These approaches mainly adopt a central server to help manage the process of trust computation and make a decision. However, in practice, such central server may become a single point of failure as most IT personnel in the healthcare organizations are not security expert, and the deployed software may have a lag in updating and patching [49]. As a result, it is hard to ensure that the central server is trusted from the view of security.

With the popularity and application of blockchain technology, more research started investigating the integration of IDS and blockchains. This is because blockchain technology can enable unknown (or even untrusted) parties to exchange data with each other in a verifiable manner without the need of a trusted intermediary [28], [52]. Motivated by this observation, in this paper, our purpose is to design a blockchain-based trust management scheme for defending healthcare organizations against insider attacks.

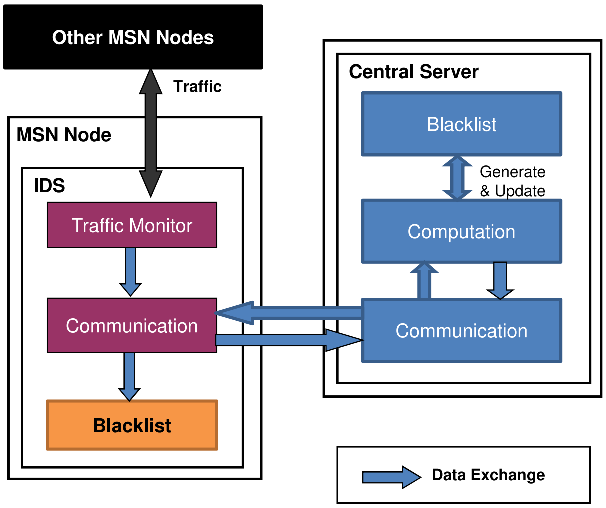

Fig. 2. Typical intrusion detection mechanism with interaction details between central server and MSN nodes (smartphones).

1) Application of IDS Into MSN: Fig. 2 describes the typical IDS mechanism with the detailed interaction between various MSN nodes and one central server [30]. More specifically, a lightweight version of IDS would be installed on the phones to help monitor network status, record traffic, and enforce security policies. It often has three components: traffic monitor, communication component, and a blacklist.

1) Traffic monitor: This component is used to help check traffic, record data, and send information to its communication component.
2) Communication component: This component is responsible for connecting and forwarding required data to the central server, which plays an important role during the whole interaction. It also helps update its blacklist based on the information from the server side.
3) Blacklist: This component contains a list of blocked MSN nodes (smartphones), which is decided by the trust values calculated by the server. On the basis of the feedback from healthcare managers, the list is expected to be dynamic in order to reduce the impact of false positives [30].

By contrast, the central server handles the process of trust computation and the detection of malicious nodes. It usually contains three major components: trust computation, communication component, and a blacklist.

1) Trust computation: This component mainly helps calculate trust values of MSN nodes based on the received data, identify malicious nodes, and decide the blacklist.
2) Communication component: This component is similar to the one on the phone side, which handles the connection between various nodes and the server. It helps gather the required data from nodes to facilitate the process of trust computation, and forward the updated blacklist to the corresponding MSN nodes.

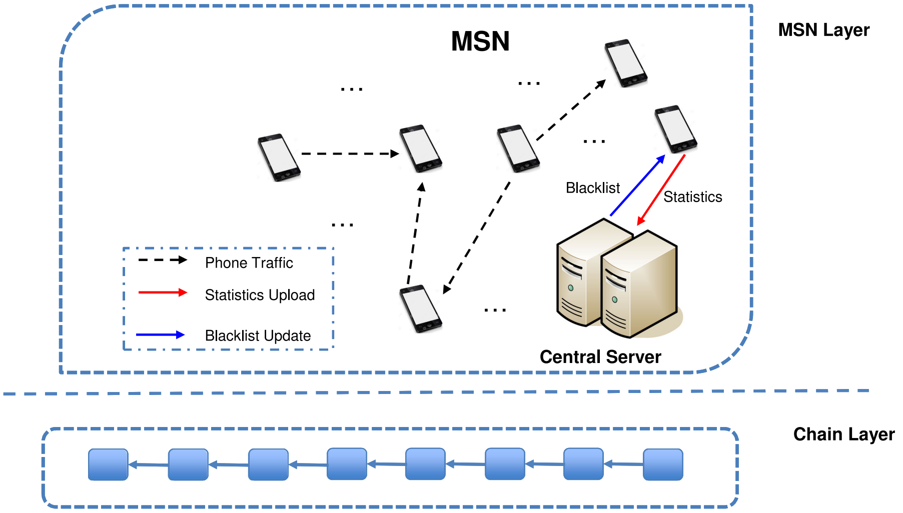

Fig. 3. Layered blockchain-based trust management framework for MSNs.

3) Blacklist: This list contains the most updated blacklisted nodes. In particular, some security policies can be deployed here to ensure the list to be dynamic and accurate.

2) Blockchain-Based Trust Management: The above architecture with one central server is demanded by the healthcare manager, but may become a single point of failure. As blockchains can enable different nodes to communicate in a distributed manner without the need of a central authority, we design a trust management scheme by integrating with blockchains. Fig. 3 shows the blockchain-based trust management scheme, which separates the MSN into two major layers: MSN layer and chain layer.

1) MSN layer: This layer allows the typical interaction between MSN nodes and the central server (as shown in Fig. 2). It can maintain the existing framework and reduce implementation cost in a healthcare organization. In fact, there are some other ways to implement the blockchain-based trust management, but may need to change the existing architecture.
2) Chain layer: This layer constructs a consortium blockchain that allows each node to upload features of unwanted or malicious packets. As each node can access the chain to check the features of malicious packets, they can quickly update their own blacklist and obtain more information by sending messages to the target node directly. In the original architecture, it is not easy to update the list in a fast way.

This blockchain-based trust management scheme can provide two benefits: 1) it can help quickly upload the blacklist across MSN nodes by checking the blockchains; and 2) it allows some more powerful nodes to communicate with potentially abnormal nodes and explore more information on their traffic status. According to (5), a malicious node could be detected quickly by decreasing the value of k.

3) Detection Threshold: Let t_{value} denote the trust value for a node, then it can be computed based on (5). To highlight the recent untruthful event, we apply a forgetting factor $\lambda \in [0,1]$ to gradually reduce the impact of historical data. Then, let t denote the time interval, the trustworthiness of MSN nodes can be measured according to the following equation:

$$t_{\text{value}} = \frac{\Sigma_1^i k_t \lambda^t + 1}{\Sigma_1^i N_t \lambda^t + 2}. \quad (6)$$

Similar to previous work [30], [34], one MSN node could be blocked for the sake of one malicious packet, whereas it may result in a high false positive, i.e., caused by accidents, or careless operations. Thus, we adopt a dynamic blacklist generation to degrade the influence of error rates. Given a threshold of $T \in [a, 1]$, we can make a decision accordingly: 1) the blocked node can be removed from the blacklist if its $t_{\text{value}} \in T$; and 2) otherwise, this node should stay in the blacklist.

IV. Evaluation

In the evaluation, similar to [30], we mainly investigate the performance of our proposed trust management through collaborating with two healthcare organizations (in South China). For the sake of privacy concerns and control, our approach was implemented in these two medical environments, named *ME1* and *ME2*, with the help of corresponding IT administrators and managers. More specifically, there are 18 and 23 phone nodes in *ME1* and *ME2*, respectively. A mobile Snort version was deployed, which is an open-source rule-based IDS. A central server with Intel Core 2, Quad CPU 2.66 GHz, handled the collection of statistical data and relevant information from each MSN node. It is worth noting that both organizations added a set of their own rules for controlling traffic (135 for *ME1* and 253 for *ME2*). The consortium blockchain was deployed in a mid-end computer with Intel Core i6, CPU 2.5 GHz with 50 GB storage.

A. Normal Condition

In this experiment, we explore the network traffic under the normal condition. Fig. 4 depicts the average trust values of MSN nodes for each healthcare environment. On the basis of the impact analysis of forgetting factor in [30], we set $\lambda = 0.8$ in this

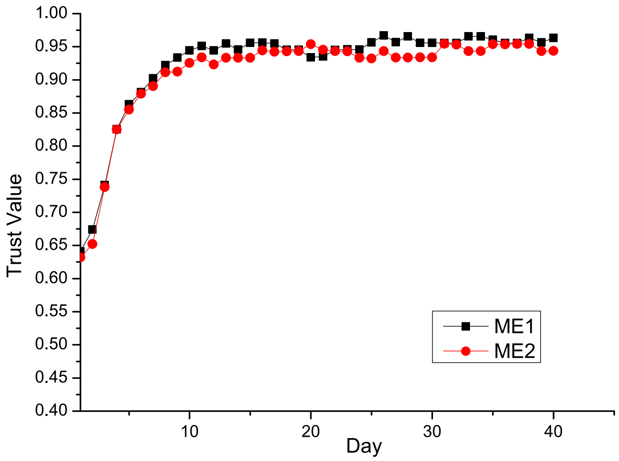

Fig. 4. Average trust values of MSN nodes under the normal condition.

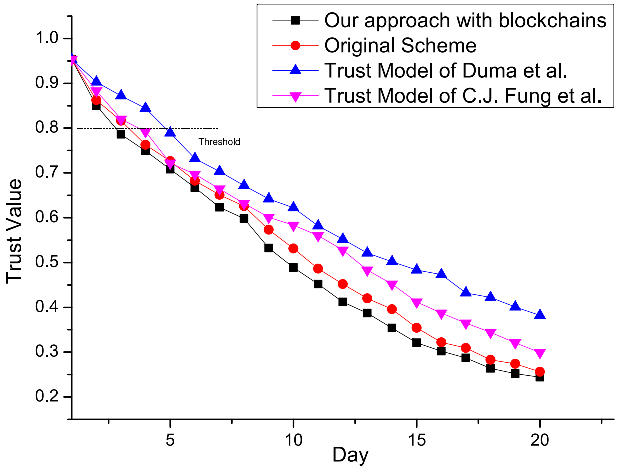

Fig. 5. Average trust values of malicious nodes in *ME1*.

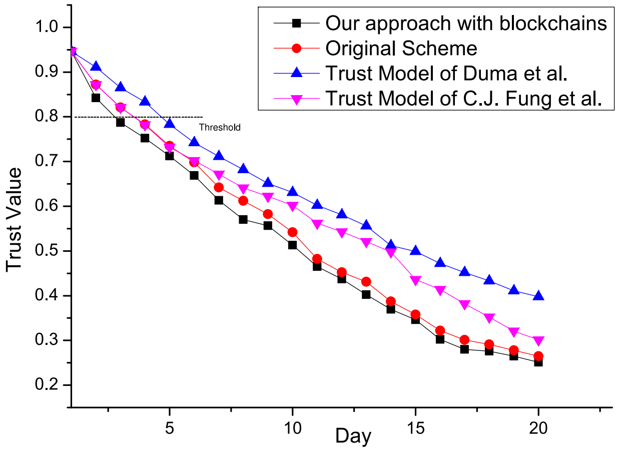

Fig. 6. Average trust values of MSN nodes in *ME2*.

paper. It is observed that after a time period, the trust values could become stable, i.e., very close to one, after the central server completed the collection of data. In practice, it is very difficult to achieve one according to (5) and (6), due to the communication delay and different security requirements. In addition, it is found that the average reputation in *ME1* was a bit higher than that in *ME2*. This is because *ME2* employed more self-rules to control traffic, resulting in a more security-sensitive environment.

B. Adversarial Condition

In this experiment, our purpose is to evaluate the performance of our blockchain-based trust management scheme under the adversarial condition. To launch internal attacks, we randomly selected three nodes and five nodes to send malicious packets to other nodes in *ME1* and *ME2*, respectively. In particular, the malicious traffic was sent by our developed program based on the wireless IDS testing tool, which has the capability of sending various forms of manipulated packets, e.g., airjack beacon packet (WVE-2005-0018).[1] We also set the forgetting factor as $\lambda = 0.8$.

1) Comparison and Results: In this paper, we consider two related trust management schemes in the evaluation: Duma *et al.* [10] and Fung *et al.* [11]. The former detected malicious insider nodes using a trust-aware engine and an intelligent trust management. The latter designed a challenge-based trust model to identify malicious nodes by evaluating the satisfaction level between the expected answers and the received feedback. In the experiment, both of them deployed in the same architecture with a central server.

The insider attack was launched when the network and the trust values become stable in both healthcare environments. To reduce the impact of unexpected factors, the experiment was run by six times. The average trust values of malicious nodes are shown in Figs. 5 and 6. The major observations are discussed as follows.

1) It is observed that after launching the attack, the trust values of malicious nodes started decreasing under all trust management schemes. The trust model of Fung *et al.* could decrease the reputation faster than the trust model of Duma *et al.*, for the sake of forgetting factor that highlights the recent node' behavior.
2) The original trust management scheme of Bayesian inference could reduce the reputation level faster than both Fung *et al.*'s and Duma *et al.*'s trust model. This is because the trust model of Bayesian inference computes the trust values based on the packet's status, which is more sensitive to the status of (malicious) traffic. In contrast, the trust model of Fung *et al.* may suffer from delay, as it has to receive the feedback from target nodes and then perform the evaluation.
3) By comparing our proposed blockchain-based trust model with the original scheme, it is found that our approach could further improve the detection speed, i.e., in both healthcare environments, our approach could decrease the trust value below the threshold of 0.8, one day faster than the original scheme. The main reason is that with the blockchain, our approach allows MSN nodes to update their blacklist more quickly than the original scheme, and

[1] [Online]. Available: https://code.google.com/p/wireless-intrusion-detection-system-testing-tool/.

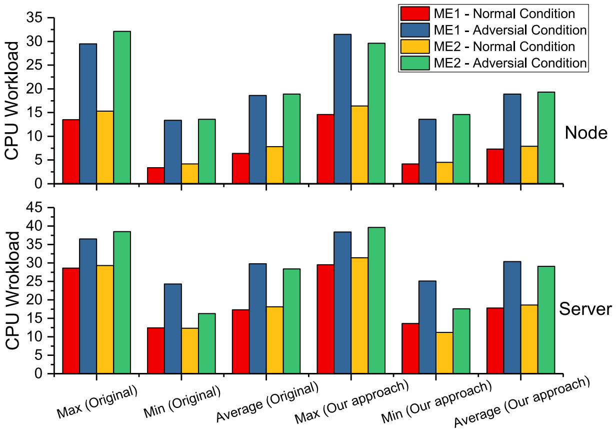

Fig. 7. CPU workload under different conditions for nodes and server in *ME1* and *ME2*.

nearby nodes can communicate with the suspicious nodes more often to obtain more traffic information.

Overall, our experimental results demonstrate that our proposed blockchain-based trust management scheme can achieve better detection performance as compared with the original scheme as well as two similar trust models. In addition, the trend of malicious nodes' reputation is similar in both healthcare environments, validating the scalability of our approach. The IT administrators from the participating organizations also confirmed our observations.

C. CPU Workload

It is reasonable that some workload would be added for both phone side and server side, due to the implementation of trust-based mechanisms. 1) The workload on the central server is mainly caused by interaction such as the collection of packet status, the communication between nodes and the server, and the update of blacklist. 2) The workload on the phone side is primarily caused by interaction such as the communication with MSN nodes, trust computation, blacklist generation and update, security policy enforcement, the retrieval of blockchains, and so on.

Fig. 7 depicts the CPU workload under different conditions for nodes and the server in two healthcare environments (*ME1* and *ME2*) in our experiments, including the maximum, minimum, and average CPU workload. We have the following main observations.

1) It is easily found that as compared with the normal condition, the CPU workload was much higher in the adversarial condition. For instance, the average CPU of the central server in *ME1* is 17.3% in the normal condition, while it could increase to 29.8% under attacks. This is because malicious traffic would cause more interaction between different MSN nodes and between nodes and the server.
2) It is identified that the workload in the server was much higher than that on the phone side, i.e., the CPU workload is 17.3% and 6.4% for the server and phone nodes in *ME1*, respectively. This is because the server has to undertake many tasks such as data collection, trust computation and evaluation, blacklist generation, and update.
3) It is observed that our approach could increase the CPU workload a little bit higher than that in the original scheme, i.e., the average CPU workload is 7.3% and 6.4% (node in *ME1* - normal condition), and 17.8% and 17.3% (server in *ME1* - normal condition) between our approach and the original scheme, respectively. The increased rate was found to be small, i.e., less than 3%.

The results on the original scheme is similar to [30]. It is worth noting that the reported CPU workload contains all interaction between nodes and the server (not just caused by our approach), i.e., including the basic workload required to maintain connection and communication with other nodes. As the workload difference is quite small between the original scheme and our approach, we consider that our approach is practical in a real-world application. The IT managers from the participating healthcare organizations also confirmed this observation.

V. Further Discussion

This paper is an early study to investigate how to apply blockchain technology for enhancing trust management in the healthcare industry. The current results demonstrate the positive impact by combining blockchains and trust management, while there are still many challenges in this field.

1) *Blockchain Limitations:* As an emerging technology, blockchains are still under development, which suffer from many inherent limitations. For example, blockchain implementation may require a high computation power for mining process [54]. As transactions have to be connected with known parties, there is a concern on data privacy. In addition, depending on the network scope, blockchains may also cause much delay for the sake of updating the corresponding blocks. There is a need to investigate these issues in our future work.
2) *Lack of IT Experts:* As more medical devices are inter or intraconnected, healthcare organizations need more IT experts in handling IT tasks and proving security protection. However, it is not easy for healthcare organizations to recruit IT experts in practice, making security still a big concern. This requires an effort from healthcare industry, while it is also an interesting topic for security researchers to develop more intelligent security mechanisms without much human interference.
3) *Legacy System and Late Update:* In most cases, healthcare organizations use the legacy OS and software, which could be three to five years old. These systems leave many vulnerabilities such as misconfiguration to cyber-attackers. In addition, healthcare systems have a late update and patch, making the whole medical environment vulnerable to updated attacks. To address this problem, one solution is to recruit IT experts. There is also a need for security researchers to develop appropriate security policies for the healthcare industry.
4) *Centralized Trust Management:* The use of central server is likely to be a major target by cyber-criminals. If attackers compromise the server, then the whole medical

environment could be paralyzed. A distributed architecture can help reduce such risk, whereas the centralized management is a distinct requirement by healthcare industry [30]. This is because most healthcare professionals are not familiar with IT operations. It is a challenge to develop more usable security software as well as investigate how to design appropriate distributed trust management for healthcare organizations.

5) *External Attacks:* In this paper, we mainly examine the performance of our approach against insider attacks. It is also an important topic to study the impact of external attacks such as DoS attacks on the proposed trust management scheme. DoS is a very powerful attack that can deliver excessive packets of messages to a network component such as the central server.

6) *Workload Increment:* Under our settings, the caused workload was considered to be reasonable for a practical implementation. In practice, the MSN scale is not very big, whereas our two environments only adopted 18 and 23 nodes. It is still an interesting topic to investigate whether the workload will be further increased with more nodes involved.

7) *IDS Performance:* In this paper, how to improve the performance of an IDS is out of scope. Our blockchain-based trust management scheme is built on the existing IDS capability. In practice, healthcare organizations may have different security policies and particular rules in judging an event. It is an interesting topic to improve and tune an IDS for the healthcare industry.

VI. Conclusion

In the era of IoT, more healthcare organizations started adopting IoMT with either inter or intraconnected medical devices to help reduce cost and facilitate the communication between patients and healthcare professionals. However, medical devices are a common target by cyber-attackers, where if one device is compromised, hackers can threaten other healthcare sections within the network. In particular, insider attacks are one major threat to IoMT. To mitigate this problem, in this paper, we focused on MSNs and designed a blockchain-based trust management scheme to identify malicious nodes more efficiently. Our approach can help quickly update the blacklist across nodes by checking the blockchains, and allow nodes to obtain more information on traffic status from the suspicious nodes. In the evaluation, we investigated the performance of our approach in two healthcare environments. The results demonstrated that our approach can identify malicious nodes faster than the original scheme and similar approaches (i.e., one day faster than the original scheme). In addition, the workload was found to be similar to the original scheme, making our approach acceptable and practical in real-world applications.

Our future work could include investigating how to improve the blockchain-based trust management by exploring the aspects of latency and computational power. In addition, it is an interesting topic to study how to design appropriate distributed trust management for healthcare organizations.

Acknowledgment

The authors would like to thank the participating IT administrators and managers for their great support and helpful suggestions regarding our mechanism design and implementation.

References

[1] Aranca, Internet of Medical Things (IoMT), 2016. [Online]. Available: https://www.aranca.com/assets/uploads/resources/special-reports/Internet-of-Medical-Things-IoMT_Aranca-Special-Report.pdf

[2] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Trust-based intrusion detection in wireless sensor networks,” in *Proc. IEEE Int. Conf. Commun.*, 2011, pp. 1–6.

[3] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[4] E. Ben-Sasson *et al.*, “Zerocash: Decentralized anonymous payments from bitcoin,” in *Proc. IEEE Symp. Security Privacy*, 2014, pp. 459–474.

[5] H. Chen, H. Wu, J. Hu, and C. Gao, “Event-based trust framework model in wireless sensor networks,” in *Proc. Int. Conf. Netw., Archit., Storage*, 2008, pp. 359–364.

[6] L. Chen, W. K., Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” *Future Generation Comput. Syst.*, vol. 95, pp. 420–429, 2019.

[7] J.-H. Cho, A. Swami, and I.-R. Chen, “A survey on trust management for mobile ad hoc networks,” *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, Fourth Quarter 2011.

[8] Deloitte, “How digital technology is tranforming health and social care,” 2015. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf

[9] Deloitte, IoT innovation report, 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf

[10] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, “A trust-aware, p2p-based overlay for intrusion detection,” in *Proc. DEXA Workshop*, 2006, pp. 692–697.

[11] C. J. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba, “Trust management for host-based collaborative intrusion detection,” in *Proc. Int. Workshop Distrib. Syst., Oper. Manage.*, 2008, pp. 109–122.

[12] C. J. Fung and Q. Zhu, “FACID: A trust-based collaborative decision framework for intrusion detection networks,” *Ad Hoc Netw.*, vol. 53, pp. 17–31, 2016.

[13] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, “Trust-based secure clustering in WSN-based intelligent transportation systems,” *Comput. Netw.*, vol. 146, pp. 151–158, 2018.

[14] A. K. Ghosh, J. Wanken, and F. Charron, “Detecting anomalous and unknown intrusions against programs,” in *Proc. 14th Annu. Comput. Security Appl. Conf.*, 1998, pp. 259–267.

[15] J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, “A trust-based approach against IP-Spoofing attacks,” in *Proc. 9th Annu. Int. Conf. Privacy, Security Trust*, 2011, pp. 63–70.

[16] X. Gu, J. Wang, J. Qiu, and Z. Jiang, “Self-Recommendation mechanism in trust calculation among nodes in WSN,” *Wireless Personal Commun.*, vol. 97, no. 3, pp. 3705–3723, 2017.

[17] J. Guo, “Smartphone-Powered electrochemical biosensing dongle for emerging medical IoTs application,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2592–2597, Jun. 2018.

[18] J. Guo, A. Marshall, and B. Zhou, “A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks,” in *Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun.*, 2011, pp. 142–149.

[19] J. Healey, N. Pollard, and B. Woods, The Healthcare Internet of Things: Rewards and Risks, Mar. 2015. [Online]. Available: https://www.atlanticcouncil.org/images/publications/ACUS_Intel_MedicalDevices.pdf.

[20] The Linux Foundation, “Hyperledger blockchain for business,” 2017. [Online]. Available: https://www.hyperledger.org

[21] IDC, IDC’s 2018 Global IoT Decision Maker Survey, 2018. [Online]. Available: https://theinternetofthings.report/view-events.aspx?EventID=2664

[22] J.-H. Lee, “Future of the smartphone for patients and healthcare providers,” *Healthcare Informat. Res.*, vol. 22, no. 1, pp. 1–2, 2016.

[23] Z. Li, Y. Chen, and A. Beach, "Towards scalable and robust distributed intrusion alert fusion with good load balancing," in *Proc. SIGCOMM Workshop Large-Scale Attack Defense*, 2006, pp. 115–122.

[24] W. Li, Y. Meng, and L. F. Kwok, "Enhancing trust evaluation using intrusion sensitivity in collaborative intrusion detection networks: Feasibility and challenges," in *Proc. 9th Int. Conf. Comput. Intell. Security*, 2013, pp. 518–522.

[25] W. Li, W. Meng, and L. F. Kwok, "Design of intrusion sensitivity-based trust management model for collaborative intrusion detection networks," in *Proc. 8th IFIP WG 11.11 Int. Conf. Trust Manage.*, 2014, pp. 61–76.

[26] W. Li, W. Meng, L. F. Kwok, and H. H. S. Ip, "Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model," *J. Netw. Comput. Appl.*, vol. 77, pp. 135–145, 2017.

[27] W. Li, W. Meng, and L. F. Kwok, "Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks," *Future Internet*, vol. 10, no. 1, pp. 1–16, 2018.

[28] T. McGhin, K. R. R. Choo, C. Z. Liu, and H. Debiao, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.

[29] W. Meng, X. Luo, W. Li, and Y. Li, "Design and evaluation of advanced collusion attacks on collaborative intrusion detection networks in practice," in *Proc. Int. Conf. Trust, Security Privacy Comput. Commun.*, 2016, pp. 1061–1068.

[30] W. Meng, W. Li, Y. Xiang, and K.-K. R. Choo, "A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *J. Netw. Comput. Appl.*, vol. 78, pp. 162–169, 2017.

[31] W. Meng, W. Li, Y. Wang, and M. H. Au, "Detecting insider attacks in medical cyber-physical networks based on behavioral profiling," *Future Generation Comput. Syst*., Jun. 6, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.06.007

[32] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[33] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, 2018.

[34] W. Meng, K.-K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, "Towards bayesian-based trust management for insider attacks in healthcare software-defined networks," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 2, pp. 761–773, Jun. 2018.

[35] W. Meng, "Intrusion detection in the era of IoT: Building trust via traffic filtering and sampling," *IEEE Comput.*, vol. 51, no. 7, pp. 36–43, Jul. 2018.

[36] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," [Online]. Available: http://bitcoin.org/bitcoin.pdf, 2008.

[37] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," in *Proc. Int. Conf. Parallel Distrib. Syst.*, 2007, pp. 1–8.

[38] P. A. Porras and R. A. Kemmerer, "Penetration state transition analysis: A rule-based intrusion detection approach," in *Proc. Annu. Comput. Security Appl. Conf.*, 1992, pp. 220–229.

[39] M. M. Rathore, A. Ahmad, A. Paul, J. Wan, and D. Zhang, "Real-time medical emergency response system: exploiting IoT and big data for public health," *J. Med. Syst.*, vol. 40, no. 12, pp. 283:1–283:10, 2016.

[40] B. Filkins, SANS Institute. Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon, 2014. [Online]. Available: http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

[41] "Singapore suffers 'most serious' data breach, affecting 1.5M healthcare patients including Prime Minister," 2018. [Online]. Available: https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/

[42] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[43] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Comput. Security*, vol. 78, pp. 245–254, 2018.

[44] Y. L. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modelling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[45] B. Sun and D. Li, "A comprehensive trust-aware routing protocol with multi-attributes for WSNs," *IEEE Access*, vol. 6, pp. 4725–4741, 2018.

[46] Symantec. Networked Medical Devices: Security and Privacy Threats, Jun. 2015. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/white_papers/b-networked_medical_devices_WP_21177186.en-us.pdf

[47] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Comput. Surveys*, vol. 47, no. 4, 2015, Art. no. 55.

[48] F. Wang, C. Huang, J. Zhang, and C. Rong, "IDMTM: A novel intrusion detection mechanism based on trust model for ad-hoc networks," in *Proc. 22nd Int. Conf. Adv. Inf. Netw. Appl.*, 2008, pp. 978–984.

[49] P. A. H. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices: Evidence Res.*, vol. 8, pp. 305–316, 2015.

[50] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2016, EIP-150 Revision. Available: https://gavwood.com/paper.pdf

[51] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol.*, 2018, pp. 1–10. [Online]. Available: http://eprint.iacr.org/2017/375

[52] X. Xu *et al.*, "The blockchain as a software connector," in *Proc. 13th Working IEEE/IFIP Conf. Softw. Archit.*, 2016, pp. 1–10.

[53] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An IoT-cloud based wearable ECG monitoring system for smart healthcare," *J. Med. Syst.*, vol. 40, no. 12, pp. 286:1–286:11, 2016.

[54] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," *PLoS ONE*, vol. 11, no. 10, pp. 1–27, 2016.

[55] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[56] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 1–22, 2012.

[57] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, "A dynamic trust establishment and management framework for wireless sensor networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, 2010, pp. 484–491.

[58] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Comput. Security*, vol. 29, no. 1, pp. 124–140, 2010.

Weizhi Meng (SM'19) received the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, in 2013.

He is currently an Assistant Professor with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark. He was known as Yuxin Meng and prior to joining DTU, he was a Research Scientist with the Infocomm Security Department, Institute for Infocomm Research, Singapore. His primary research interests include cyber security and intelligent technology in security including intrusion detection, smartphone security, biometric authentication, human-computer interaction (HCI) security, cloud security, trust management, malware detection, blockchain in security, cyber-physical system security, and Internet of Things security.

Wenjuan Li (S'15) received the Ph.D. degree in computer science from the City University of Hong Kong (CityU), Hong Kong, in 2019.

She holds a visiting position with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby, Denmark. Before this, she was a Research Assistant with CityU and was previously a Lecturer with the Department of Computer Science, Zhaoqing Foreign Language College, Zhaoqing, China. Her research interests include network management and security, collaborative intrusion detection, spam detection, trust computing, web technology, and security in E-commerce technology.

Dr. Li was a Winner of Cyber Quiz and Computer Security Competition, Final Round of Kaspersky Lab "Cyber Security for the Next Generation" Conference in 2014.

Liqiu Zhu received the master's degree in computer science from Macau University, Macau, China, in 2015.

He is currently a Senior Research Engineer with the FinTech Startup, Macau, China. He has broad research interests including blockchain technology, artificial intelligent in security, smartphone security, Internet of Things, and cyber-physical system security.