BIoMT: Blockchain for the Internet of Medical Things

Mohamed Seliem, Khalid Elgazzar
Center for Advanced Computer Studies
University of Louisiana at Lafayette, USA
{mohamed.seliem1, elgazzar}@louisiana.edu

***Abstract*— The Internet of Things promises to connect more than 50 billion devices in a multitude of application domains. However, user privacy and security remain a major challenge in IoMT. In this paper, we present a work in progress for a lightweight blockchain based scheme aiming to secure the Internet of Medical Things (IoMT). The proposed approach consists of four main components: a cloud server, network cluster, medical facility, and smart medical devices. Each medical facility contains a "bolster", a powerful computing device that operates as a gateway/server to support in-range smart medical devices. The bolster holds a private and secure block role. It is used to securely communicate with other blocks in the same blockchain. Experimental analysis shows that the proposed scheme presents a non-significant overhead; yet it brings major advantages to meet the standard security and privacy requirements in IoMT.**

Keywords—Blockchain, IoT, Privacy, Security, Medical IoT.

I. Introduction

The Internet of Medical Things (IoMT) is a growing domain of IoT applications, where medical devices are used to provide different healthcare services. According to Allied Market Research [1], the IoT healthcare market will reach $136.8 billion worldwide. IoMT devices are typically attached to the human body and collect various types of sensitive data. This data enables caregivers and healthcare providers make timely and data-driven decisions related to the individual's health status. However, this data is sensitive and private. Therefore, users need to ensure that their medical data is handled in a confidential, secure and private way.

Security and privacy are major challenges in IoMT. IoMT devices are recourse-constrained; and cannot afford the high resource requirements of complex and heavyweight traditional security algorithms. In addition, the centralization used in the state-of-the-art security frameworks, is not well suited for IoMT due to the large distributed scale of IoMT networks and single point of failure [2]. In this paper, we propose a novel blockchain technology scheme, which is mainly optimized for IoMT, to tackle the security challenge and preserve the privacy of IoMT users.

Blockchain is mainly introduced for secure digital money transactions [3]. It is a decentralized, distributed and public digital record book, which is used to store data across its peer-to-peer network and uses public key cryptography for block addressing. This assures the transparency of block level data to everyone involved. Therefore, blockchain eliminates the risks due to data centralization such as data manipulation. Therefore, it is a good choice to implement a secure and privacy-preserving IoMT. Importing the blockchain technology to IoMT environments is not straightforward and poses several challenges [4]. For example, the most popular blockchain technology, bitcoin, suffers from long latency for inscribing a transaction on the blockchain, high resource demand due complex cryptography, poor scalability, and high traffic overhead. However, the blockchain technology offers many advantages such as (1) transaction messaging with end-to end cryptographic signing capabilities such as military grade encryption; (2) decentralized communications to allow peer to- peer connections between devices; (3) acid-base functionality through reinventing the role of the IoMT devices as digital assets that provide metering capabilities or digital contracts that expire at a certain time.

Many research initiatives tried to solve this important and timely problem. Dorri et al. [5] propose a blockchain framework to secure communications and data exchange in IoT environments. Their proposed framework specifically targets smart home applications. Puthal et al. [6] discuss the benefits of blockchain decentralization to solve the security challenges in IoT scenarios. Despite the sensitivity of medical IoT applications, only a few existing studies suggest leveraging the blockchain technology to secure IoMT. Rabah et al. [7] provide a review for the challenges and opportunities in developing security solutions for healthcare IoT systems based on the blockchain technology. Unlike the above referenced work, our work presents a holistic framework to optimize the blockchain technology to secure Internet of medical devices.

II. System Architecture Overview and Implementation

Figure 1 illustrates the architecture of the proposed system and its different components. It encompasses multiple layers that interact and exchange data with each other.

A. System architecture

BIoMT follows a hierarchical structure with distributed privacy-preserving techniques, which makes it suitable for IoMT. It extends our previous work in [8], and mainly consists of four layers as follows:

(1) **Device layer,** which consists of the smart medical devices, body sensors, wearable devices, and user-interfacing devices (e.g. smartphones and tablets). Those devices collect health related data about users inside or outside the medical facility. In this layer, we implement a scheme that combines the Elliptic Curve Cryptography (ECC) [9] key establishment protocol and the identity-based credential (IBC) mechanism [10]. Thus, it provides decentralized privacy, which better fits the integrated blockchain security fundamentals for IoMT.

(2) **Facility layer,** that includes the bolster that manages IoMT devices. It runs algorithms such as: (1) Attribute Number Selection (ATS) that takes the list of attributes from a specific device and associate each attribute with a number that is only known for this device. (2) Security generator (SecGen) that takes the attribute number from the device credentials and generates a unique hash value. (3) Identity issue (ID) that takes the attribute number and its associated hash value to generate a unique identity for the smart medical device.

978-1-7281-3234-1/19/$31.00 ©2019 IEEE

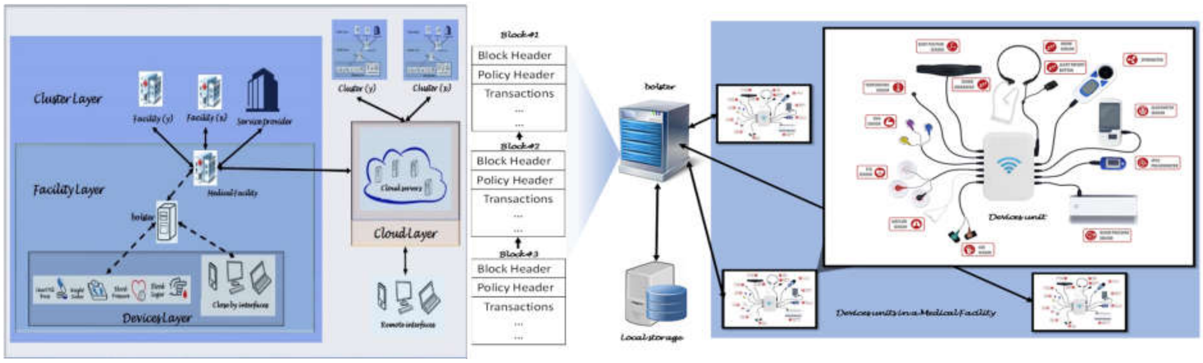


Figure 1: An overview of the blockchain IoMT system architecture.

The bolster itself consists of two entities: (a) Local blockchain, a centralized entity that allows the authorized owner the responsibility to add/remove devices through creating new transactions, delete transactions from the ledger, or control through the policy header. (b) Local storage for storing data locally as a backup drive. Close by authorized users can access local data in case of no connection to the global cloud storage.

(3) **Cloud layer,** which provides computational power and storage support to the cluster layer. This layer groups the data into identical blocks with unique block numbers. Users should authenticate before requesting data through providing the block number and block hash. Following the data processing, the shared key extracted from the IBC is used to encrypt the block number. The cloud servers also run anonymization algorithms [11] to strip the private/identity information to allow for identity-free data analytics.

(4) **Cluster layer,** that contains several medical facilities, service providers, and cloud servers. For each cluster, medical facilities elect a cluster head (CH), which communicates with other CHs forming a distributed network that corresponds to the blockchain technology. Each CH stores two types of public key lists: a list that contains the public keys of users and a list of the public keys used by different facilities. CHs uses these public keys to form a peer-to-peer network to decrease the network overhead and delay.

B. System use case components

The medical facility use case implements the proposed blockchain scheme in the medical domain with three main units, which are necessary for system functionalities:

1) Transactions, which represent the communication and data exchange, different types of transactions listed in table 1. ECC encrypts the transactions for secure communication. Then, they get stored in the local blockchain.

2) Local blockchain that stores the transaction blocks of the smart medical facility. Each block consists of two headers: block header and privacy header. The block header preserves the hash of the previous block to keep the block chain well established. The privacy header enforces the facility-defined privacy policies and authorize IoMT devices.

3) Medical facility bolster, which performs the following functionalities: (a) Processing the transactions sent and received by IoMT devices, (b) Implementing the key establishing scheme, (c) Generating origin transactions to add new devices, (d) Communicating with other cluster bolsters to elect the cluster head. (e) Maintaining the local blockchain through creating and appending blocks to the chain, (f) Managing local storage to provide additional and extra backup space for the ledger chain.

C. System functionailities

Framework initialization: The bolster initializes and runs the key establishment mechanism. Initially, each device submits its attributes to be mapped into numbers using ATS. Then, the SecGen uses the attribute number and other information to create the agreement and form the policy header. Then, each device obtains a unique identity (shared public key) based on the agreement and the attribute number. Finally, the encrypted shared key stored in an origin transaction is added to the block.

Communication setup: devices can communicate with each other, associated bolster in the same medical facility, or any outside entity. This process requires exchanging the shared key of both communicating entities. If the facility bolster permits the access, the devices can communicate directly as long as the shared key is valid. If access is denied, bolster marks the shared key as invalid.

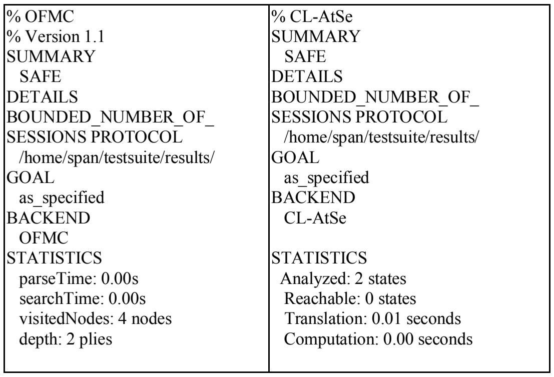
Storing data: data is stored locally in the local storage or on the cloud to be accessed by remote customers or service providers. In case of local storage, the device should authenticate with the bolster and sends a store transaction to permit the storage process and allow the bolster to maintain the transaction in the block. In case of cloud storage, the bolster checks for data anonymization. Therefore, an anonymization algorithm splits the personal information before data submission.

Device data access: medical residents, service providers, or users can request access for a certain device. A bolster can permit or deny the data access. In case of local storage, the designated bolster provides the data for the permitted requester. However, if the data is stored on the cloud with no local backup/cache, the requester will be redirected to the cloud to fetch the required data. Thus, it reduces the overhead on the medical facility network and maintains the data security.

Device monitoring: medical residents can request to monitor a certain or a group of devices. The process is initiated by sending a monitor transaction to the bolster that is responsible for this group of devices. The bolster defines a threshold for the periodic data update to control the network overhead and reduce the likelihood of certain security attacks (Flooding attack, denial of service).

Table 1: Transactions types.

Name	ID	Generator	Function
Origin	0	Admin user	Add new device
Remove	1	Admin user	Remove a device
Store	2	IoMT Device	Store data from device
Access	3	Service provider or authorized user	Access the stored data
Observe	4	Service provider or authorized user	Monitor a certain or group of devices



```
% OFMC
% Version 1.1
SUMMARY
  SAFE
DETAILS
BOUNDED_NUMBER_OF_
SESSIONS PROTOCOL
  /home/span/testsuite/results/
GOAL
  as_specified
BACKEND
  OFMC
STATISTICS
  parseTime: 0.00s
  searchTime: 0.00s
  visitedNodes: 4 nodes
  depth: 2 plies
```

```
% CL-AtSe
SUMMARY
  SAFE
DETAILS
BOUNDED_NUMBER_OF_
SESSIONS PROTOCOL
  /home/span/testsuite/results/
GOAL
  as_specified
BACKEND
  CL-AtSe

STATISTICS
  Analyzed: 2 states
  Reachable: 0 states
  Translation: 0.01 seconds
  Computation: 0.00 seconds
```

Figure 2: Outputs Results using OFMC and CL-AtSe backend in AVISPA.

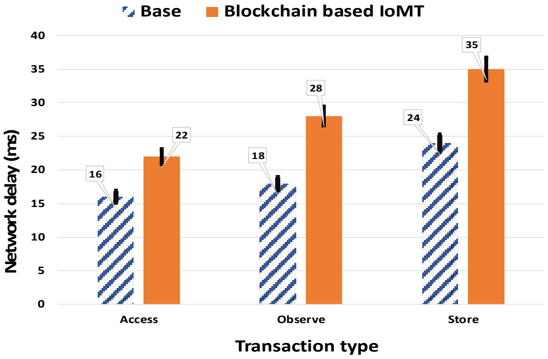


Figure 3: Network delay due to processing different type of transactions.

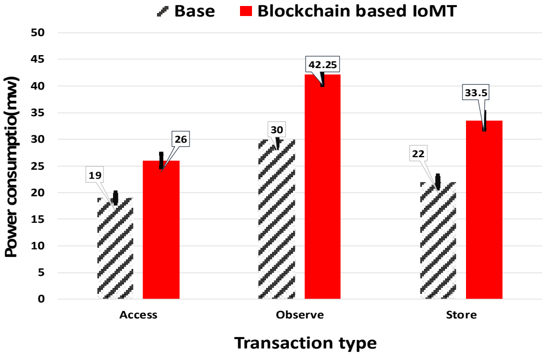


Figure 4: Power consumption due to processing different transactions by the network bolster.

Devices removal: reusable, devices used for different users, broken or out of service devices need to be removed before re-added or get fixed. The removal process is initiated by a device owner or an admin user through submitting a request to remove this device, by sending remove transaction to the bolster to remove all the notations for the data associated with this device from the ledger.

Multiple bolsters support: the size of medical facilities varies, which may require several bolsters to support large medical facility. In this case, a master bolster is essential to coordinate and support the data exchange between other bolsters. In this case, a shared blockchain will be required. The origin transactions of IoMT devices, associated with a certain bolster, will be chained to the origin transaction of this bolster. Then, stored in the master bolster as part of the shared blockchain. Further, the devices associated with a certain bolster can communicate with each other as mentioned above.

III. SYSTEM ANALYSIS

We analyze the security performance of the proposed scheme from two perspectives: functionality and prone to security attacks [12]. To evaluate the functionality, we setup a group of devices to simulate a workflow. Then, we use AVISPA [13] security tool to verify the security functionality. We also provide a brief theoretical discussion to show the resistivity of blockchain IoMT to security attacks. Further, we study the computational and communication cost to evaluate the system performance.

A. Security analysis

AVISPA is a well-recognized tool for security verification. We use the High-Level Protocol Specification Language (HLPSL) to implement the framework. The schema (i.e., configuration file) is deployed on different back ends: OFMC, On-the-Fly Model Checker [14] and CL-AtSe, Constraint Logic-based Attack Searcher [15].

The simulations results presented in Figure 2 shows that the proposed blockchain-based IoMT is safe against inventory, replay and man-in-the-middle attacks. In the following, we describe how the proposed system meets the fundamental security requirements including authentication, confidentiality, integrity, availability, and user control. Authentication: All data requests must be authenticated before gaining access to data. The proposed scheme accomplishes this requirement using a shared key management scheme in addition to both the privacy header and security agreement.

Confidentiality: Only permitted users can interpret the received messages. The application of the Elliptic Curve Cryptography assures such a requirement. Additionally, the decentralized approach that we adopt in our design ensures that no single entity can hold all the information about the user's data, which offers better privacy and protection and is well suited for the IoMT nature

Integrity: All system transactions are hashed and only data owners can hold the hashing value. This provides high security measures even if communication channels are compromised.

Availability: To save energy and communication overhead, the proposed scheme enables threshold setups, where IoMT devices can be set to communicate their measurements only when the threshold is reached, otherwise remain standby and keep monitoring. This increases the device lifetime and improves availability.

User control: Users must have full control over their collected data. The proposed scheme stores all transactions in the blockchain ledger. Therefore, users know what exactly is collected, who collects it and for what purpose.

Next, we theoretically analyze the effectiveness of our proposed framework against famous attacks. Starting with DDOS attack in which the attacker manages to infect several IoMT devices and exploit them to overwhelm a targeted network device until it fails. The proposed framework has a hierarchy nature with different layers of security, which makes it resilient to DDoS attacks. For example, to gain access to an IoMT device, an attacker must crack the bolster's security measurements. Additionally, the fact that transactions are stored in the local blockchain makes it impossible for an attacker to install a malware on the devices.

In linking attack, the attacker establishes a link between the data exchanged through the network transactions to infer personal data related to anonymous user. In our design, the bolster uses the attribute number and the hash value to create a unique ID for each IoMT device, which prevents such kind of attacks.

B. *Performance evaluation*

We evaluate the proposed framework with the proposed key establishment mechanism and blockchain technology. We compare the framework performance with the state-of-the-art network deployment techniques, with no cryptography deployed, in medical facility settings. Therefore, we can assess the performance metrics of interest, which are listed below:

(1) Network overhead: refers to the overhead added due to the extra packets exchanged between the devices. Such as the time delay due to the packet processing and network transmissions.

(2) Power consumption: refers to the power consumed due to operating the bolster, as it is supposed to be online all the time to support network functionality.

Figure 3 shows the end-to-end delay due to network overhead for three commonly used transactions Access, Observe, and Store. Due to additional encryption and hashing operations, our framework incurs extra processing time compared to the base method. However, the delay is 11 ms at the worst case, which is relatively small compared to the gained security and privacy preservation gains.

Figure 4 shows the energy consumption at the facility bolster for the same three transactions and compare the results with the base case. The power consumption naturally increases due to the additional computation overhead (e.g., cryptography and transactions handling). The observe transaction entails the highest power consumption (~12.25 mw increase from the base case, which is around 35%). We argue that with such a non-significant overhead, our framework provides high security and privacy preservation in blockchain-based IoMT systems.

IV. Conclusion

Blockchain is evolving as one of the most promising and creative technologies for security. It stands as a powerful candidate to overcome the privacy and security issues in IoT applications. In this paper, we present a blockchain-based framework for IoMT applications. We combine ECC with IBC to provide a key establishment mechanism for IoMT devices. We introduce the bolster, which hosts the local blockchain in each medical facility and communicates with other facility bolsters form the global blockchain using clusters. Our analysis demonstrates that our framework provides a lightweight, secure and private environment with no significant overhead on the end-to-end latency or energy consumption. To the best of our knowledge, this work is one of the earliest to adopt the blockchain technology in the medical IoT context. Our prototype implementation and performance evaluation provide promising results towards a highly secured and privacy preserving IoMT. The research presented in this paper is a one small leap towards a bright future in the healthcare domain.

References

[1] IoT health market is excpected to reach 13.68 billion by 2021 [Online]. Available: https://www.marketwatch.com/story/internet-of-things-iothealthcare-market-is-expected-to-reach-1368-billion-worldwide-by-2021-2016-04-12-8203318, Accessed June 2018.

[2] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, Volume 76, 2015, pp. 146-164.

[3] J. Brito; Castillo, Andrea (2013). Bitcoin: A Primer for Policymakers (PDF) (Report). Fairfax, VA: Mercatus Center, George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.

[4] A. Dorri, Salil S. Kanhere, and Raja Jurdak. "Blockchain in internet of things: challenges and solutions." arXiv preprint arXiv:1608.05187 (2016).

[5] A. Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, pp. 618-623. IEEE, 2017.

[6] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos,and C. Yang, 2018. The blockchain as a decentralized security framework. IEEE Consumer Electronics Magazine, pp.18-21.

[7] K. Rabah. "Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review." Mara Research Journal of Medicine

[8] M. Seliem and K. Elgazzar, "IoTeWay: A Secure Framework Architecture for 6LoWPAN Based IoT Applications," 2018 IEEE Global Conference on Internet of Things (GCIoT), Alexandria, Egypt, 2018, pp. 1-5.

[9] He, Debiao, and Sherali Zeadally. "An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography." IEEE internet of things journal, Issue no. 1 (2015): pp. 72-83.

[10] A. Lewko, and Brent Waters. "Decentralizing attribute-based encryption." In Annual international conference on the theory and applications of cryptographic techniques, pp. 568-588. Springer, Berlin, Heidelberg, 2011.

[11] M. Terrovitis, Nikos Mamoulis, and Panos Kalnis. "Privacy preserving anonymization of set-valued data." Proceedings of the VLDB Endowment, Issue no. 1 (2008): pp. 115-125.

[12] M.U. Farooq, Muhammad Waseem, Anjum Khairi, and Sadia Mazhar. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications, Issue no. 7 (2015).

[13] AVISPA. Automation Validation of Internet Security Protocols and Applications. [Online]. Available: http://www.avispa-project.org/ , Accessed: June 2018

[14] D. Basin, Sebastian Mödersheim, and Luca Vigano. "OFMC: A symbolic model checker for security protocols." International Journal of Information Security, Issue no. 3 (2005): pp.181-208.

[15] M. Turuani. "The CL-Atse protocol analyser." In International Conference on Rewriting Techniques and Applications, pp. 277-286. Springer, Berlin, Heidelberg, 2006.