Decentralized approach for data security of Medical IoT Devices

Mario Casillo[1], Francesco Colace[1], Brij B. Gupta[2], Francesco Marongiu[1] and Domenico Santaniello[1]

[1]*DIIn University of Salerno, Salerno, Italy*
[2]*National Institute of Technology Kurukshetra, India*

Abstract

In recent years, smart medical devices have become part of people's daily lives. The massive diffusion of these devices is due to the increasing availability and accessibility to hardware resources with limited features but sufficient to perform a particular task (i.e., monitoring of heartbeat, blood oxygenation, etc.). Recently it has been possible to allow these devices to connect with the outside world, and through the internet, they have become part of what is now generally defined as the Internet of Things (IoT) paradigm. Due to the limited computing power of these devices, very often security protocols are neglected or sometimes impossible to implement. In many cases this is not a problem, but in the medical field this issue is immediately crucial.

The purpose of this paper is to investigate the use of decentralized systems for the collection and certification of data from medical IoT (MIoT) devices. In particular, a software hardware architecture capable of connecting MIoT devices with a decentralized system based on Blockchain and Smart Contract has been described. The results obtained are promising, demonstrating the efficiency and effectiveness of the proposed solution.

Keywords

Blockchain, Internet of Things, Medical IoT, Data Security, Big Data, Decentralized Systems

1. Introduction

In recent years, it has been possible to connect more and more devices with a variety of hardware and software characteristics to the network. Thanks to the advancement of electronics and the reduction of production costs, the development of smaller and smaller hardware products specialized to perform specific tasks has been witnessed. There has been a gradual move away from the concept of *general purpose* to *single* or *special purpose* Connected over a network, these devices have permitted the development of what is now called the Internet of Things (IoT) paradigm [1], a network of millions of *special purpose* devices capable of collecting data and sending it directly over the network to larger, more complex systems. One of the many areas that have been revolutionized by IoT is certainly the medical field [2] [20-22]. Indeed, it has been possible to create devices with small dimensions and able to monitor in real time parameters related to the health of patients, opening the possibility of diagnosis and prevention of many diseases [3].

One of the main problems of these devices is certainly the transmission of the collected data to advanced storage and analysis [4]. The data collected represent one of the major sources of knowledge because it is possible to extrapolate correlations and useful information that would otherwise be hidden [5]. Ensuring the security and reliability of this data is therefore crucial, as dirty or manipulated data could lead to the creation of incorrect and therefore useless knowledge bases. This is particularly evident in the medical field, where these data are used to propose diagnoses or monitor the health status of individuals [6]. Blockchain, and decentralized systems in general, can help address these issues [7]. The architecture proposed in this work aims to develop a

International Conference on Smart Systems and Advanced Computing (Syscom-2021), December 25–26, 2021
EMAIL: mcasillo@unisa.it (A. 1); fcolace@unisa.it (A. 2); gupta.brij@gmail.com (A. 3); fmarongiu@unisa.it (A. 4); dsantaniello@unisa.it (4. 5)
ORCID: 0000-0003-2798-5834 (A. 2); 0000-0003-4929-4698 (A. 3); 0000-0001-5563-0411 (A. 4); 0000-0002-5783-1847 (A. 5)

software/hardware ecosystem in which MIoT devices communicate directly with a certified Blockchain-based storage.

This solution is possible since data saved on Blockchain technology is immutable over time and cannot be altered either voluntarily or accidentally [8], furthermore, by using the cryptographic properties inherent to the technology, data can be uniquely associated with the user who owns a MIoT device through digital signature mechanisms.

2. Related Works

Apart from healthcare [17-19], IoT devices have a variety of applications in industries and agriculture [10]; however, because of their low computational capability, these IoT devices are susceptible to a variety of cyber threats. However, it presented a variety of different detecting systems for cyber threats [11]. Many applications of Blockchain in the IoT field have been proposed in the literature; however, the focus of the research does not see IoT devices as an active part of the Blockchain, but as sensors that are queried by other systems that are then connected with the decentralized structure.

Chakraborty et al. [12] proposed a system has been proposed that uses a dual blockchain to store data from IoT devices. The first one directly managed by the user, while the second one is used to exchange information between patients, doctors, and the healthcare system. In practical this cannot be developed because the private user blockchain cannot guarantee any security because not decentralized.

Liu et al. [13], proposed an advanced blockchain architecture for the system governing e-health care systems. The work focused on the development of interoperable and an adaptable networking solution for the effective and proper sharing of the health care data within multiple stakeholders. The blockchain architecture follows the methodology of primary audits by the stakeholders such as the insurance companies, hospitals, and doctors about the authenticity and credibility of a record that is been shared over the platform.

3. Proposed Approach

The proposed methodology is based on three main modules: IoT Devices, Routing Devices, and a Blockchain system.

Figure 1 Proposed Framework

IoT devices are responsible for collecting data from the outside world and encoding it in a standard format. In addition, these devices possess a public and private key pair of the same space as those used in the Blockchain.

Routing Devices are exclusively responsible for forwarding data from IoT devices to the Blockchain.

The Blockchain is used as a decentralized certified storage, able to receive, via Smart Contracts [14], data from IoT sensors and automatically associate them with the users to whom they belong.

3.1. Device Registration

Before devices are enabled to send data, they must be registered on the Blockchain so that they can be uniquely associated with a user.

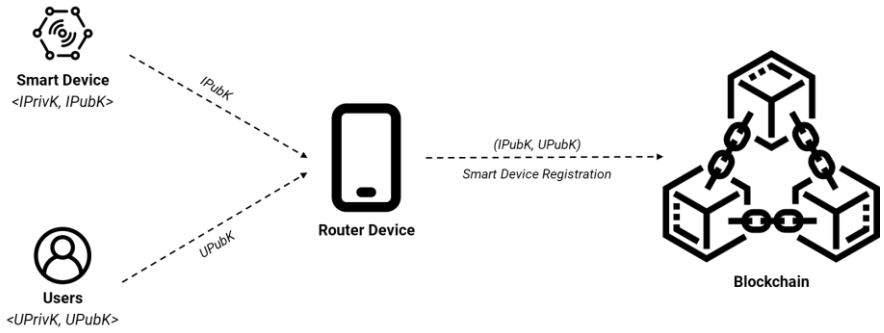

Figure 2 Device Registration Workflow

Users and devices both possess unique Public/Private key pairs belonging to the same domain from the Blockchain. The user who intends to use the smart device associates the latter's public key with his own via a Smart Contract. Further associations by other public keys will be rejected unless the device is removed by the user who originally registered it.

This mechanism means that devices can be located anywhere without ever losing data ownership information.

3.2. Data Transmission

IoT devices buffer data based on the type of time frame needed and specific to the use case, then the data is encoded according to a common structure and digitally signed using the private key contained within the <*IPrivK*> device.

The tuple that contains the device's public key, data and its signature *(IPubK, Data, Sig)*, is transmitted to a routing device that is responsible for forwarding the data to the Blockchain.

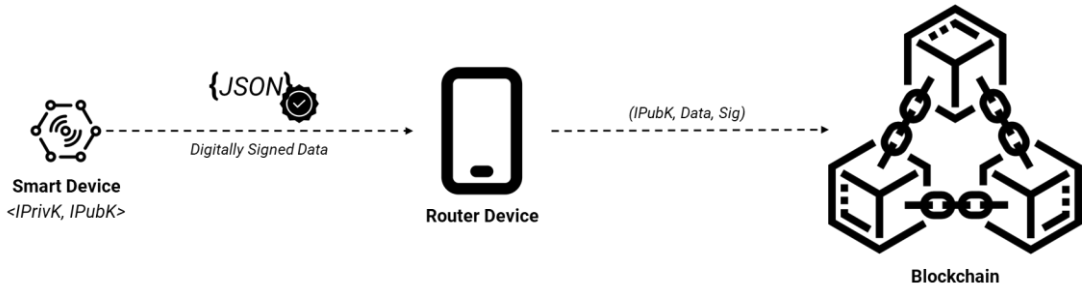

Figure 3 Data Transmission Workflow

Routing devices do not have to be trusted. When information reaches the Blockchain, it will be up to the Smart Contract to verify: The public key <*IPubK*> of the device is associated with a user; the digital signature is compatible with the <*IPubK*> key and that the data has not been corrupted or manipulated during transport. If the verifications are successful, then the data is saved within the Blockchain and then made accessible by the user.

3.3. Smart Contract

The memory of the Smart Contract has been organized to make the information entry and verification operations efficient. Two main structures have been used:

- A Hash table to store information and data history for a single IoT device.
- A Hash table that allows to quickly have the list of all the devices associated to a user.

```
        struct IoTDevice {
            bool registred;
            address owner;
            bytes32[] data;
        }

        //List of all registred devices in the smart contract, those devices
will be allowed to store content.
        mapping (address => IoTDevice) private registered_devices;

        //Lookup map to find all associated devices to a specific user.
        mapping (address => address[]) private devices_association;
```

Smart Contract functions are primarily concerned with managing data storage and access: associating devices uniquely to users; checking digital signatures on data from sensors; saving data within the described data structure.

4. Results

The system has been implemented experimentally on Test Ethereum network using the Solidity language; The results show a good compromise in the execution of operations from the point of view of GAS: *Device Registration* had an average GAS cost of 44000; Digital Sign Verification of 25000; while Verification and insertion 69000. Specifically, the transactions do not have an acceptable cost in terms of GAS in relation to a base transaction (21000 GAS).

Table 1
Average GAS results

Operation	Average GAS consummation
Device Registration	44192
Digital Sign Verification	25568
Verification and Data Insertion	69822

An interesting aspect of the Smart Contract concerns the verification of the correctness of the signature affixed to the data. For this purpose, was used the function **`ecrecover`** native to EVM, which allows to efficiently extract the public key from the data signature.

5. Conclusions

In conclusion, the system turns out to be robust and efficient for storing data in a certified manner, thus going to solve one of the main problems of IoT devices. Understanding exactly where the data comes from and being sure that it has not been manipulated during transport and after storage is an important property in the world of Industry 4.0. The result assumes even more relevance when it comes to the medical world and therefore IoT devices applied to health [15]. The experimental results are promising, and it is certainly possible to expand the research in multiple directions. The focus has been on data certification, but it could be interesting to add an additional layer of encryption to create a selective data access system [16]. Or explore the use of innovative Blockchain technologies to improve Smart Contract efficiency and execution.

6. References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[2] M. Hassanalieragh *et al.*, "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," in *2015 IEEE International Conference on Services Computing*, Jun. 2015, pp. 285–292. doi: 10.1109/SCC.2015.47.

[3] G. Yang *et al.*, "A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2180–2191, Nov. 2014, doi: 10.1109/TII.2014.2307795.

[4] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.

[5] A. L. Beam and I. S. Kohane, "Big Data and Machine Learning in Health Care," *JAMA*, vol. 319, no. 13, p. 1317, Apr. 2018, doi: 10.1001/jama.2017.18391.

[6] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, Jan. 2018, doi: 10.1016/j.future.2017.02.014.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[8] M. Kassab and G. Destefanis, "Blockchain and Contact Tracing Applications for COVID-19: The Opportunity and The Challenges," in *2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Mar. 2021, pp. 723–730. doi: 10.1109/SANER50967.2021.00092.

[9] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sep. 2016, pp. 1–3. doi: 10.1109/HealthCom.2016.7749510.

[10] AlZu'bi, S., Hawashin, B., Mujahed, M., Jararweh, Y., & Gupta, B. B. (2019). An efficient employment of internet of multimedia things in smart and future agriculture. Multimedia Tools and Applications, 78(20), 29581-29605

[11] Tripathi, S., Gupta, B., Almomani, A., Mishra, A., & Veluru, S. (2013). Hadoop based defense solution to handle distributed denial of service (ddos) attacks. Journal of Information Security. Vol. 4 No. 3 (2013) , Article ID: 34629

[12] S. Chakraborty, S. Aich, and H.-C. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, Feb. 2019, pp. 260–264. doi: 10.23919/ICACT.2019.8701983.

[13] W. Liu, S. S. Zhu, T. Mundie, and U. Krieger, "Advanced block-chain architecture for e-health systems," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Oct. 2017, pp. 1–6. doi: 10.1109/HealthCom.2017.8210847.

[14] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[15] M. H. Kassab, V. V. G. Neto, G. Destefanis, and T. Malas, "Could Blockchain Help With COVID-19 Crisis?," *IT Professional*, vol. 23, no. 4, pp. 44–50, Jul. 2021, doi: 10.1109/MITP.2021.3072585.

[16] M. Casillo, A. Castiglione, F. Colace, M. de Santo, F. Marongiu, and D. Santaniello, "COVID-19 data sharing and organization through blockchain and decentralized models," in *CEUR Workshop Proceedings*, 2021, vol. 2991, pp. 128–140.

[17] Al-Ayyoub, M., AlZu'bi, S., Jararweh, Y., Shehab, M. A., & Gupta, B. B. (2018). Accelerating 3D medical volume segmentation using GPUs. Multimedia Tools and Applications, 77(4), 4939-4958

[18] Al-Ayyoub, M., AlZu'bi, S., Jararweh, Y., Shehab, M. A., & Gupta, B. B. (2018). Accelerating 3D medical volume segmentation using GPUs. Multimedia Tools and Applications, 77(4), 4939-4958.

[19] AlZu'bi, S., Shehab, M., Al-Ayyoub, M., Jararweh, Y., & Gupta, B. (2020). Parallel implementation for 3d medical volume fuzzy segmentation. Pattern Recognition Letters, 130, 312-318.

[20] Sandeep Kumar (2021) Artificial Intelligence and Machine learning for Smart and Secure Healthcare System, Insights2Techinfo, pp.1
[21] A. Dahiya, K. Psannis (2021), Internet-of-Medical-Things (IoMT): An Unexplored Dimension in Healthcare, Insights2Techinfo, pp.1
[22] Mamta (2021) Quick Medical Data Access Using Edge Computing, Insights2Techinfo, pp.1