

Blockchain Based Remote Patient Monitoring System

Bashayer Al-Ahmadi and Sanaa Sharaf

Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Jacob.sayid@hotmail.com

Abstract. Remote Patient Monitoring system is an approach of a health care system that enables the patient-user of performing a remote periodical check-up. Unfortunately, these types of systems usually don't provide the advantages of securely sharing the patient health information among different health providers. Many types of research aimed to solve this issue by applying the blockchain technique to the existing patient health information records at hospitals. However; none was found regarding the remote patient monitoring system's generated data. Therefore, this proposal aims to integrate the advantages of blockchain and the Remote Patient Monitoring (RPM) system by building a secure blockchain based RPM system.

Keywords: Remote Patient Monitoring, RPM, Blockchain, PHI, Healthcare.

1. Introduction

Remote Patient Monitoring (RPM) system is a technological advancement that enables a remote patient monitoring by the supervising doctor through the data provided by a remote device ^[1]. Then, the health information in this device is feed into a remote destination usually a cloud to be later viewed by the supervisor doctor. The stream of information that is feed into the cloud contains also the patient's private information.

By 2014 the Saudi Ministry of Health ^[2] declared that there are 1.1 million Saudi males and 356 thousand Saudi females suffer from diabetes. At the same time, there are 1.16 million Saudi male and 705 thousand females suffer from high blood pressure. These types of illness required continuous monitoring at a supervised doctor. There are two major problems with this approach: 1. the patients

wait too long in waiting room for a simple periodical check-up 2. It is not suited for the rural area due to the lack of medical service provided there. Therefore; the RPM system considers the optimal solution to monitor these diseases on distant. It saves time for both the doctor and the patient as it serves the rural area too. That's why the Saudi government adopted this approach - firstly through King Fahd Medical City - to serve these purposes.

Adverse drug reactions (ADRs) ^[3] is a situation when a harmful reaction results from medication conflicts. This is usually happening when a patient takes many prescriptions form different doctors. To avoid this issue, the concept of medical records patient-centric approach has emerged. The patients can share their previous medical records with their current doctors. This approach is implemented through blockchain.

The blockchain is a decentralized, peer to peer data processing service that enables building an open and distributed online database. These databases are consisting of data structure called blocks. Each block has a timestamp of its production, the previous block's hash value and a reference to the patient's healthcare data and the healthcare provider information. The hash value of the previous block makes the chain as it makes the blockchain immutable to modification. The major benefits of applying the blockchain in the RPM will be as follow: the patient's medical history is going to be complete, consistent, timely, accurate, and easily distributed. Also, the patient will have control over his\her data. Moreover, any change on the blockchain is visible to any members of the patient network, and all data insertions are immutable. Which makes any unauthorized modifications is an easy detected one. One of the major strong points of using such a technique is that it doesn't need a trusted third party and it doesn't have a single point of failure. The primary blockchain was designed for and implemented in Bitcoin. Currently, there are different blockchain infrastructures such as Ethereum, where the blockchain generation can every participant, and the Hyperledger Fabric, where the blockchain generation is restricted to the approved participant only. Ethereum has something called the smart contract which is a block of code that is automatically run based on a predefined conditional trigger^[4-7].

Many research^[8-10] studied the benefit of applying blockchain in authenticating, authorizing and viewing the patient health information (PHI). These researches were designed to securely share the PHI among different parties including the patient him\herself. On the other hand, no research was found that address the integration of the Remote Patient Monitoring (RPM) systems

generated data with the blockchain sharing capabilities. Applying the blockchain technology to the RPM system will help to enhance the diagnosis and reducing the adverse drug reactions (ADRs) because of its immutable log between the hospitals participating in the blockchain network. It allows sharing the patient health information (PHI) stored in these hospitals to the RPM system.

The important of this research is to fill the gap found between the need to review the patient health information (PHI) and the existing remote patient monitoring solutions. The gap found between the need to review the PHI and the existing remote patient monitoring solutions motivates this research. It aims to incorporate the advantages of Blockchain with the RPM system to answer the following questions: can the proposed system integrate the existing RPM solutions with the Blockchain based systems to enable sharing of the PHI? Can it also adapt the need to a quick consultation through higher response time?

In the paper, Section 2 discusses literature review while Section 3 discusses research design and methodology. Section 4 mentioned the implementation and Section 5 contains the result and discussions. Finally Section 6 conclusion and future work.

2. Literature Review

We review the literature review in three categories: first the traditional RPM systems, then the blockchain based medical data sharing system and finally, the hybrid system.

A. The Traditional RPM Systems

Kriangsiri Malasri and Lan Wang proposed the Sensor Network for Assessment of Patients (SNAP)^[11] which aimed to solve the wireless health monitoring security issues through using public-key architecture. Unfortunately, the provided schema doesn't

support sharing the medical records. MEDiSN^[12] is also an RPM system used to monitor patients in hospitals and during disaster events. It consists of multiple custom-built physiological notes that send the patients data into the backbone server. Moosavi *et al.*^[13] built a secure schema for the mobility enabled healthcare IoT. It consisted of 3 layers: the device layer, fog layer, and Cloud layer. Moosavi focused on the security of the proposed RPM solution by using certificate DTLS (Datagram Transport Layer Security) handshake for the authentication and authorization process. Unfortunately, the proposed system doesn't address the higher response time required by the RPM solution nor the need to review the EHR. On the other hand, Yeh^[14] proposed an RPM solution that is built on a predefined architecture called Body Sensor Network-Care (BSN-Care)^[15]. The author added an authentication layer on that architecture through a hash-based public/private key. However; All the RPM solutions mentioned earlier are a central server-based architecture which means they have a single point of failure, unlike the blockchain. These types of systems focus on sending the patient's data into a remote destination to be viewed by the doctor later rather than focusing on viewing the patient's previous medical records. Therefore, all the papers listed in this category doesn't support the feature of sharing previous medical Records.

D. The Blockchain Based Medical Data Sharing System

Kria Both A. Zhang and X. Lin^[8] and K. Fan *et al.*^[9], aimed to provide a system that helps in the patient diagnosis process through reviewing the previous medical records issued for this patient. To handle this issue, A. Zhang and X. Lin^[8] propose a novel schema called blockchain-based secure and privacy-preserving personal health information sharing

(BSPP) scheme. To achieve their goal, they used two types of blockchain structure. The first one is a private blockchain in which it is responsible for storing the patient records. The second one is a consortium blockchain which is responsible for storing an index used to search for the patient records stored in the private blockchain. In their schema, they solved both data confidentiality and integrity by enabling public key encryption. Unfortunately, this schema handles the data stored in the hospital's database and it doesn't handle the data generated from the RPM systems. Hence, it is limited in terms of handling quick consultations in cases of emergencies. The same things go for K. Fan *et al.*^[9], where the system provided does not handle the RPM data generated. They presented MedBlock: Which is a blockchain-based information management system to handle the patient medical records. In their system, they used access control and encryption strategy to ensure data integrity and confidentiality. Using the Breadcrumbs mechanism in their system affected data retrieval in a fast manner. The greater number of users' increases the fastest Breadcrumbs mechanism guide the user to the required corresponding blocks. This new technique helps in speeding up the data retrieval, but it suffers from the additional amount of data. Again, their research does not support the RPM generated data since it assumes that the data is already stored in the hospital database.

On the other hand, G. Dagher *et al.*^[10] propose a novel approach called Ancile in order to overcome the weak security systems that allow hackers to steal the patients' information. Their systems securely transfer the data among different parties as it puts the full control of the patient's records to the patient him\herself. It allows him\her to decide who can view their data. This was done by implementing a permissioned blockchain in

which only certain entities can participate in e.g. the health providers.

The system is composed of 3 entities:

1. The Database Manager: responsible for searching through the patients' records as well as hashing both the result record and the query asked for that record to ensure data integrity.

2. The Cipher Manager: responsible for the cryptography part in the system which guarantees data confidentiality through public key encryption.

3. Ethereum-Go Client: responsible for permitting nodes to access the private blockchain.

The system used six types of smart contracts to achieve the paper goal. The system also supports the role-based access, but it doesn't support the emergency situation nor the RPM generated data.

C. The Hybrid System

One of the blockchain based security solutions designed for the RPM data is K. Griggs *et al.* [16]. In the system provided, they took advantage of the smart contract on a consortium-managed blockchain to automate the notification for the patient. However; on the provided system they emphasize that it shouldn't be used for emergency situations since it aggregates the data and sends it to a large time interval. The previous system provides each of the following: data integrity, confidentiality, availability, and role-based access. However, it didn't provide the feature of medical records sharing. Table 1 below illustrates the differences between the reviewed systems in the literature review. The * symbol symbolized the proposed system by this research.

Table 1. Comparisons between the reviewed systems and the proposed system.

Paper	Share Medical Records	Blockchain Based	Rpm System	Fast Response
[11]	X	X	✓	X
[12]	X	X	✓	X
[13]	X	X	✓	X
[14]	X	X	✓	X
[8]	✓	✓	X	X
[9]	✓	✓	X	X
[10]	✓	✓	X	X
[16]	X	✓	✓	X
*	✓	✓	✓	✓

3. Research Design & Methodology

The currently proposed RPM systems focus simply on sending the data through the patient to the supervisor doctor. They don't pay attention to the different health conditions the patients may suffer from nor the historical health situations or events. They don't also consider the possibility of prescriptions conflicts. Therefore, the proposed model will solve this issue by adapting Blockchain techniques with the traditional RPM systems. It assumes the following: first, the system will adapt already existent data set. Second, all the patient health information (PHI) follow the same format and schema. Finally, the data is encrypted, and the channel is secured.

The proposed model will be able to connect different health providers' databases including the one that contains the supervisor doctors. It will also connect the RPM systems to these databases. The patient's smart device will contain a smart software responsible for saving, gathering and analyzing the patient's reading data e.g. blood pressure. Then, the patient will send a request to a certain doctor in a certain hospital to be examined. If the doctor needs to view the patient's reading data, the patient will send his/her saved reading data to the doctor. After that, the doctor will generate a block for that patient containing its reading data and saved on the blockchain. In order to view the patient medical history, the

doctor easily can search through the blockchain. The system manager is responsible for authenticating both the users and the doctors. Figure 1 describes the procedure of the proposed model.

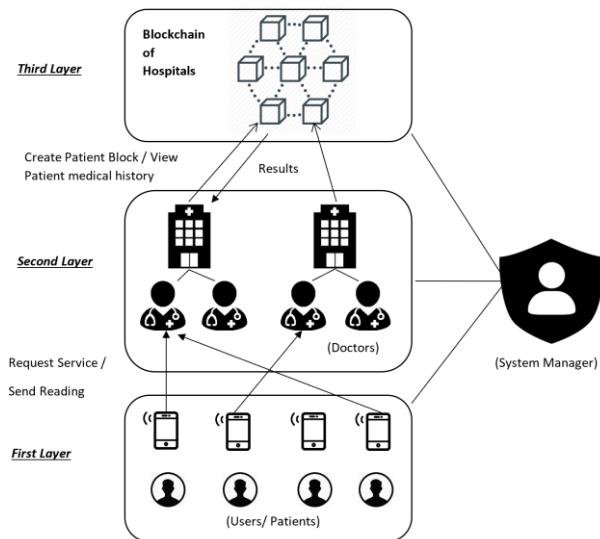


Fig. 1. The Proposed Model Procedure.

4. Implementation

The proposed system is composed of two parts the backend blockchain which is implemented by multichain platform. The other part is the user interface which is implemented using firebase development platform. The user interface collects the patient health information and store it at the platform real database in JSON format. Then, the doctor can examine and view the patient's information through platform called multichain web. The later one is a PHP web interface for multichain blockchains.

5. Results and Discussions

The authentication process is present within the smart device application for both the doctors and the patients to restrict their access and privileges to the application data. For example, the patient can enter his data while the doctor can only view these data. The mobile device application could add the

patient's both health and personal information. The doctor on the other hand, could view the patient's health information. Figure 2 illustrates the mobile application patient's layout. Through this layout the patient got to choose whether he/she wants to add the blood pressure or the diabetes reading to the system. Figure 3 shows the blood pressure layout in which the patient can actually add his/her own readings.

The private blockchain that was designed to connect the different health providers could connect different nodes to share a single or multiple stream in which all these provider's patient's health data are stored. The stream stores the data in text or JSON format. It also can upload different files types e.g. images. Figure 4 illustrates the stream and the data stored within.



Fig. 2. The Mobile Application Patient's layout.



Fig. 3. The Mobile Application Blood Pressure Layout.

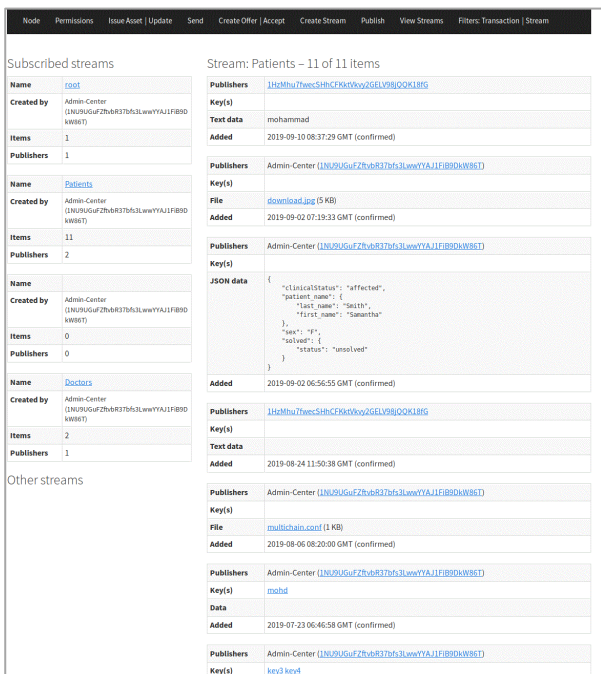


Fig. 4. The Stream of Patients' Data.

Both the mobile application and the blockchain is complete and ready to use yet to be integrated with each other. Upon its completion the system will be able to serve its purpose by viewing the patient's previous health records and adding more health records through the mobile application.

6. Conclusion and Future Work

This paper proposed an integrated system between the RPM and the Blockchain. It can view the patient's previous health information and enable the patients to contact their doctors in a fast manner. Upon its completion, it will help in decreasing the number of periodical checkups at the hospital. A better diagnosis and less adverse drug reactions will also result from the proposed system. As a future work, we aim to proceed with the implementation of the proposed system.

References

- [1] Wang, L., Yang, G., Huang, J., Zhang, J., Yu, L., Nie, Z. and Cumming, D. (2010) "A Wireless Biomedical Signal Interface System-on-Chip for Body Sensor Networks", *IEEE Transactions on Biomedical Circuits and Systems*, 4(2): 112-117.
- [2] Moh.gov.sa (2018). "وزير الصحة -ف. الصحة" أخبار الوزارة (يعلم نتائج المسح الوطني للمعلومات الصحية بالمملكة) [Online]. Available: <https://www.moh.gov.sa/Ministry/MediaCenter/News/Pages/News-2014-03-09-001.aspx>. [Accessed: 06- Oct- 2018].
- [3] Edwards, I. and Aronson, J. (2000) "Adverse drug reactions: definitions, diagnosis, and management", *The Lancet*, 356 (9237):1255-1259.
- [4] Esposito, C., De Santis, A., Tortora, G., Chang, H. and Choo, K. (2018) "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing*, 5(1): 31-37.
- [5] Kaur, H., Alam, M. Jameel, R., Mourya, A. and Chang, V. (2018) "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment", *Journal of Medical Systems*, 42(8).
- [6] Cachin, C. (2016) "Architecture of the Hyperledger Blockchain Fabric" https://www.zurich.ibm.com/dcc/papers/cachin_dccl.pdf.

- [7] **Hölbl, M., Kompara, M., Kamišalić, A. and Nemeč Zlatolas, L.** (2018) "A Systematic Review of the Use of Blockchain in Healthcare", *Symmetry*, **10**(10): 470.
- [8] **Zhang, A. and Lin, X.** (2018) "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain", *Journal of Medical Systems*, **42**(8).
- [9] **Dagher, G., Mohler, J., Milojkovic, M. and Marella, P.** (2018) "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", *Sustainable Cities and Society*, **39**: 283-297.
- [10] **Fan, K., Wang, S., Ren, Y., Li, H. and Yang, Y.** (2018) "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain", *Journal of Medical Systems*, **42**(8).
- [11] **Malasri, K. and Wang, L.** (2006) "SNAP: an architecture for secure medical sensor networks", *2006 2nd IEEE Workshop on Wireless Mesh Networks*.
- [12] **Ko, J., Dutton, R., Lim, J., Chen, Y., Musvaloiu-E, R., Terzis, A., Masson, G., Gao, T., Destler, W. and Selavo, L.** (2010) "MEDiSN", *ACM Transactions on Embedded Computing Systems*, **10**(1): 1-29.
- [13] **Moosavi, S., Gia, T., Nigussie, E., Rahmani, A., Virtanen, S., Tenhunen, H. and Isoaho, J.** (2016) "End-to-end security scheme for mobility enabled healthcare Internet of Things", *Future Generation Computer Systems*, **64**:108-124.
- [14] **Yeh, K.** (2016) "A Secure IoT-Based Healthcare System with Body Sensor Networks", *IEEE Access*, **4**: 10288-10299.
- [15] **Gope, P. and Hwang, T.** (2016) "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network", *IEEE Sensors Journal*, **16**(5): 1368-1376.
- [16] **Griggs, K., Ossipova, O., Kohlios, C., Baccarini, A., Howson, E. and Hayajneh, T.** (2018) "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", *Journal of Medical Systems*, **42**(7).

نظام مراقبة المرضى عن بعد باستخدام تقنية الكتل المتسلسلة (Blockchain)

بشاير عبدالله خليل الأحمدى و سناء شرف

كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، جدة، المملكة العربية السعودية

balahmadi0023@stu.kau.edu.sa

المستخلص. يعتبر نظام مراقبة المرضى عن بعد أحد اشكال الرعاية الصحية والذي يتيح مراقبة المريض عن بعد بإشراف طبيبه الخاص. للأسف، فإن هذا النوع من الأنظمة لا يوفر خاصية تبادل الملفات الطبية بين مزودي الخدمة الطبية المختلفين وبسريرة. توجهت العديد من الأبحاث إلى حل هذه المشكلة بصفة عامة للملفات الطبية الموجودة في المستشفيات من خلال تطبيق تقنية الكتل المتسلسلة (Blockchain) إلا أنه للأسف لحين كتابة هذا المقترح لم تُوجد أي أبحاث تُعنى بخاصية تبادل الملفات الطبية في أنظمة مراقبة المرضى عن بعد. وبناءً على النتيجة السابقة فإن هذا البحث يهتم ببناء نظام متابعة للمرضى عن بعد باستخدام تقنية الكتل المتسلسلة (Blockchain) بطريقة امنة.

الكلمات المفتاحية: نظام مراقبة المرضى عن بعد، الكتل المتسلسلة، الملف الطبي، الرعاية الصحية، تبادل الملفات الطبية.