Data Sharing and Privacy for Patient IoT Devices Using Blockchain

Conference Paper · October 2019

DOI: 10.1007/978-981-15-1301-5_27

4 authors:

Gautam Srivastava
Brandon University
135 PUBLICATIONS **689** CITATIONS
SEE PROFILE

Reza M. Parizi
Kennesaw State University, Atlanta, USA
111 PUBLICATIONS **648** CITATIONS
SEE PROFILE

Ali Dehghantanha
University of Guelph
195 PUBLICATIONS **2,466** CITATIONS
SEE PROFILE

Kim-Kwang Raymond Choo
University of Texas at San Antonio
824 PUBLICATIONS **12,271** CITATIONS
SEE PROFILE

Data Sharing and Privacy for Patient IoT Devices Using Blockchain

Gautam Srivastava[1,2](✉), Reza M. Parizi[3], Ali Dehghantanha[4],
and Kim-Kwang Raymond Choo[5]

[1] Department of Mathematics and Computer Science, Brandon University,
Brandon, MB R7A 6A9, Canada
srivastavag@brandonu.ca

[2] Research Center for Interneural Computing, China Medical University,
Taichung 40402, Taiwan, Republic of China

[3] College of Computing and Software Engineering, Kennesaw State University,
Kennesaw, GA 30144, USA
rparizi1@kennesaw.edu

[4] Cyber Science Lab, School of Computer Science, University of Guelph,
Guelph, ON N1G 2W1, Canada
adehghan@uoguelph.ca

[5] Department of Information Systems and Cyber Security,
University of Texas at San Antonio, San Antonio, TX 78249, USA
raymond.choo@fulbrightmail.org

Abstract. Once a fitness fad, wearable and other related Internet of Things (IoT) devices are fast becoming common place in many different smart city applications such as healthcare. However, IoT devices, particularly inexpensive devices, often trade security and privacy for usability. One solution to protect privacy in the healthcare domain which has begun to be explored is blockchain-based technology. However, there are a number of limitations underpinning the use of blockchain, which limits its adoption particularly in applications that require low energy and computational footprints. In this paper, we present a transactional protocol for remote patient monitoring using directed acyclic graphs. We use a newer blockchain protocol called GHOSTDAG in both a public blockchain and a private blockchain. Our novel proposed solution aims to resolve known security issues for healthcare, without affecting scalability (a feature of classic blockchain architecture).

Keywords: Blockchain · Internet of Things · Privacy · Medical device · Smart cities · Healthcare

1 Introduction

We have seen a significant increase in the use of wearable technology in various aspects of life, including in healthcare services. This is not surprising, since with the doctor to patient ratio getting very lopsided, fitting patients with wearable

G. Wang et al. (Eds.): iSCI 2019, CCIS 1122, pp. 1–15, 2019.
https://doi.org/10.1007/978-981-15-1301-5_27

technology for monitoring patient activity makes sense. The steep trajectory of Internet of Things (IoT) and access to Internet have contributed to the reality of remote patient monitoring (RPM). Specifically, RPM provides patients with an unconventional yet effective way to monitor their personal health, as shown in Fig. 1. Some known benefits are:

- Allow patients convenience of remote healthcare;
- Stay connected with healthcare providers;
- Reduction of costs (medical); and
- Improve healthcare quality

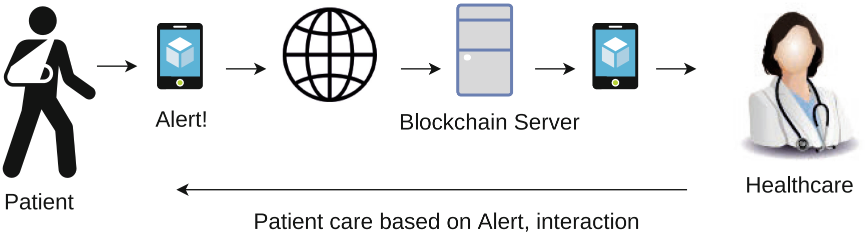

Fig. 1. Remote patient monitoring

RPM devices with respect to personal health are sensor driven electronic devices that are embedded into clothing or attached to a person's body. They are usually user-friendly and connected through a wireless connection, provide accurate feedback, and have some form of notification protocol. We can rely on these devices for accurate vital readings such as blood toxicity, blood pressure and body temperature. Healthcare IoT devices that fall into the RPM general title can be divided as presented in Fig. 2:

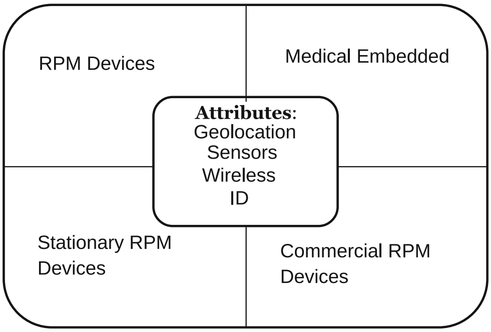

Fig. 2. Healthcare IoT devices

- Stationary RPM Devices - devices are stationary and usually large (e.g., chemotherapy dispensing stations)
- Medical Embedded Devices - are placed inside the body (e.g., pacemakers)
- RPM Devices - wireless devices to monitor some vitals (e.g., blood glucose monitor)
- Commercial RPM Devices - consumer products (e.g., Gear Fit, Apple Watch, etc.)

Internet of Things (IoT) prides itself on its interweaved devices, multi-output machines, sensors, unique identifiers (UIDs) for all involved and data transfer without human involvement as shown in Fig. 3. To accurately and securely share patient health data over multiple locations and/or stakeholders, RPM requires some level of IoT involvement. Health data is mostly private. The sharing of data will in most cases increase the chance of the data getting into adversarial hands. Furthermore, IoT has been plagued with security being an afterthought to ensure fast communication and prevent battery loss to often heavy security algorithms [13]. Lastly, current architectures of health data sharing use centralized architectures which also more often than not require centralized trust and security [7].

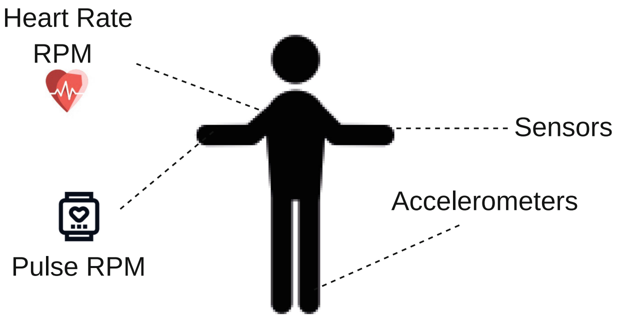

Fig. 3. Patient RPM

In an attempt to solve some of the issues mentioned earlier, we propose to the use of Blockchain technology. Blockchain technology has already shown that it can successfully provide data security and integrity as shown in [26],[24]. It is well known for its decentralized architecture (distributed ledger) and also to retain data records in the form of transactions. The immutability of blockchain makes it a logical choice in healthcare. However, there are still issues that plague blockchain technology. There have been ample attention given to its scalability, delays in transaction confirmation, and high power usage.

Since most positive characteristics of blockchain rely on blocks shared to all miners promptly, we can often see delays [1,4]. Delays in propagation are not well suited for healthcare.

In this paper, we introduce a novel and unique blockchain protocol for RPM. This new blockchain protocol makes use of the newly created GHOSTDAG protocol [20], which is well known for both security and throughput. The main noticeable difference in the GHOSTDAG protocol is its use of a directed acyclic graph (DAG), instead of classic long singular blockchains. This directed acyclic graph is known exclusively as blockDAG.

Paper Organization

The rest of this work is organized as follows. In Sect. 2 we present the related work to this research. We then give a brief overview of drawbacks of RPM in Sect. 3. Next, we present our proposed protocol in Sect. 4 and give all technical details is Sect. 5. Lastly, we conclude the paper with Future Work in Sect. 6 and concluding remarks in Sect. 7.

2 Related Work

Mettler was one of the first to look at the possible application of blockchain in healthcare in [15]. He went through an in-depth look at the possible applicable areas of blockchain within healthcare.

Our most recent motivation comes from the Canadian media article entitled "Cybersecurity of medical devices under scrutiny after FDA recalls insulin pumps". It was summarized how the U.S. Food and Drug Administration warned patients as well as healthcare agencies this week regarding a product called Medtronic MiniMed insulin pumps, citing cybersecurity vulnerabilities which could allow someone other than the patient to access the pump and change its settings [25]. With major vulnerabilities still like this present in healthcare, viable options need to be researched, explored, tested and deployed within the near future that not only meet the security needs of patients but also run in an efficient manner.

McGhin *et al.* surveyed a number of potential research opportunities connecting blockchain and healthcare. They noted that there are strong possibilities using blockchain in healthcare applications through smart contracts [9], detection of fraudulent activity, and verification of ID. However, they still had concerns using classic blockchain technology since it has its own issues that need to be addressed. These issues include many aspects of mining and specific key management issues.

Sullivan *et al.* dealt with e-Residency using blockchain. Specifically, and how it may take the place of losable objects like passports [23]. They explored the policy and governing related aspects of such a change.

Beninger *et al.* gave a thorough review of pharmacovigilance. They explored pharmacovigilance with respect to biomedical informatics. Their goal was to provide a discussion starting point for the future of pharmacovigilance as a major field [5].

Azaria *et al.* proposed MedRec. MedRec is a decentralized system handle Electronic medical records (EMRs). They propose the use of classic blockchain technology [2]. Their system gives patients a secure log and quick access to their medical history anywhere. MedRec can handle data sharing, authentication, and accountability. They also still had concerns using classic blockchain technology and suggested work on modifications to the classic blockchain protocol.

A recent health startup called BurstIQ has explored healthcare and blockchain in detail as shown in Fig. 4. BurstIQ's proprietary blockchain-based big data platform enables a known health provider to securely manage customers's data at scale and perform advanced analytics using the platform's machine learning and collaborative intelligence capabilities. Moreover, this marks the first-time healthcare data and records have been stored and managed on blockchain, making BurstIQ's proprietary blockchain platform the industry's leading Health Insurance Portability and Accountability Act HIPAA-compliant secure data platform [19].

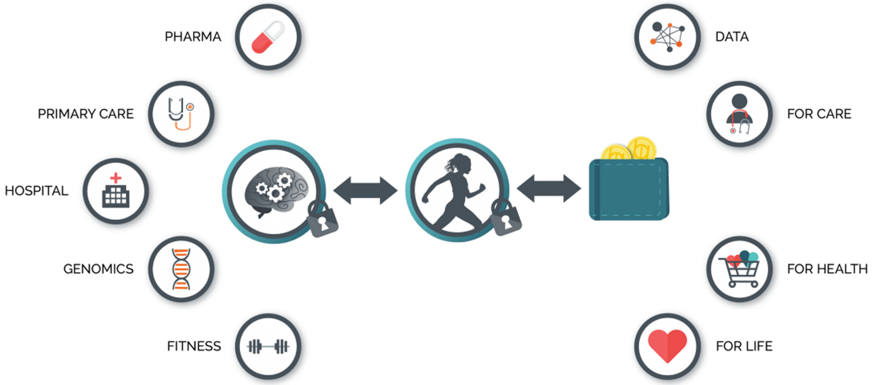

Fig. 4. BurstIQ startup [19]

Finally, in some previous work of ours, we have looked at other applications of blockchain technology as well [9,17,18,21,22,26].

3 Drawbacks and Security Issues

RPM systems are mainly concerned with the security of the health data and the efficiency of the transmission of the data. Healthcare data from RPM devices may become a commodity for adversaries. Therefore, being able to secure protected health information has remained a priority of healthcare providers [11,14]. It was indicated in [3] that a staggering 70% of United States healthcare providers surveyed indicated they had experienced some form of digital data breach in 2018/2019 calendar year. The immutability of information from blocks makes

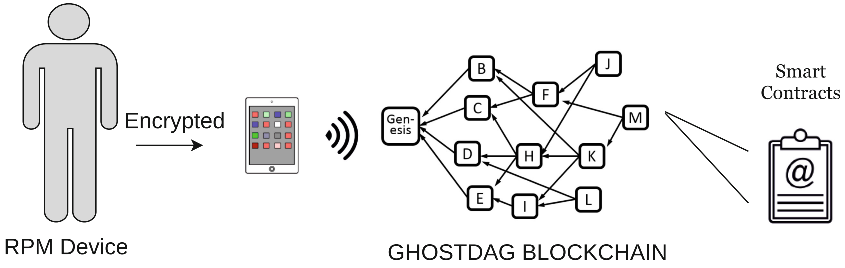

Fig. 5. Health-Data Flow

blockchain technology the best technology for healthcare coupled with its known security strengths makes blockchain worth exploring in this paper. That being said, using classic blockchain from [16] is not viable due to its delays to confirm transactions while also exhibiting high computational needs not suitable for constrained `RPM` devices. `RPM`s in the form of wearable devices are often both computationally and energy-consumption wise bounded.

4 Protocol Overview

The patient is affixed with an `RPM` device. The health-data is sent to their smart device for formatting and aggregation. The aggregated information is then sent on to the blockchain (private) to the respective smart contract. The health data undergoes a full analysis by the smart contract using threshold values. We give an overview of the process in Fig. 5. The desired threshold values as indicated in the smart contract will indicate whether the health-data is in a normal range or not, thus the analysis of health data can be done in real-time. We present a sample smart contract in Listing 41.

If the health reading is normal, no action is taken. However, if abnormal contract will execute the `Alert` function on the public blockchain. The contract will send an alert to the patient's device and authorized health institutions as advised in the contract itself (See Fig. 6). We propose the use of smart contracts like Oracle that can communicate quickly and directly to Oracle enabled smart devices [6].

Listing 41. Smart Contract for Patient

```
contract Health {
  // We can keep most information public in the contract

     address public patient;
     mapping (address => uint) public thresholdlow,
         thresholdhigh, value, reading;

 //We can create alerts if readings are abnormal
    event Alert(address fromwho, address towho, uint value);

    // This is the constructor run when contract is created.
    function Health() public {
        patient = msg.sender;
    }

    //This is the main abnormality checker
    function Send(address receiver, uint value) public {
        if ((reading[msg.sender] < thresholdhigh) || (
            reading[msg.sender]> thresholdlow)) return;

        emit Alert(msg.sender, receiver, value);
    }
}
```

We note here that no confidential medical information is stored due to HIPAA compliance reasons as mentioned in Sect. 2. The blockchain (public) stores an event when the Alert function executes. The health data gathered by an RPM device will be sent to proper EHR storage units. EHR storage units are most often run by local Medical Health institutions. Ideally as stated in [2], the EHR records could also be stored an a separate secure blockchain that could easily be integrated into our proposed model.

Lastly, treatment details from smart contracts and/or hospitals will be sent to EHR storage units while just the transactional event will be stored on the blockchain (public). The transactions are connected to the EHR system for authentication purposes. Authentication will help with alteration of patient data in the EHR storage units. Nodes on the blockchain will only be permitted to execute smart contracts, not alter them. This will limit visibility of patient data which will in turn assist to reduce data exposure.

5 Proposed Protocol

We break down our protocol into five distinct parts and summarize the protocol flow in Fig. 7

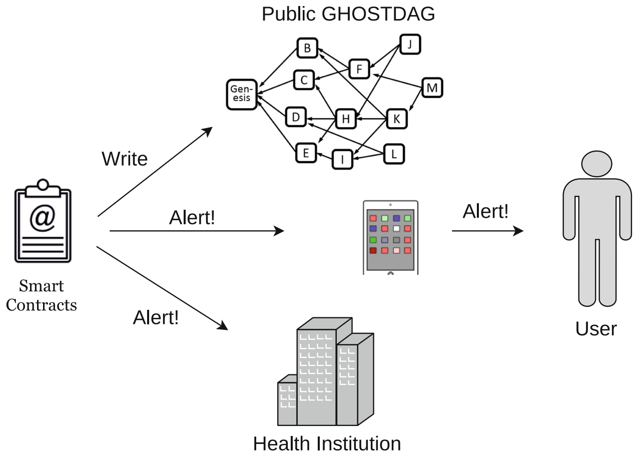

Fig. 6. Smart contracts: alerts for abnormality in readings

- Patient
- Healthcare Institution (Hospital)
- RPM on Patient
- GHOSTDAG blockchain
- Other Authorized Entities

The detail of the proposed protocol are as follows:

1. **Patient**
All health related data is collected directly from patients [8]. Some examples could be heart-beat, blood glucose levels, thyroid function, bio-markers or even walking distance. The patients own the data. They are independently responsible for data access being granted to any other parties. If the patient is in need of medical treatment, they can share their health data with the desired entity by granting them access. At the end of treatment, patient may choose to deny further access or set specific time periods for granting and revoking access.
2. **Healthcare Institution**
Healthcare institutions are appointed in some manner by Medical health bodies, other stakeholders, or directly by patients to perform some form of medical action (tests,treatment, etc.). Healthcare institutions can directly request patients to access their data and also medical treatment history if pertinent. Institutions may be able to setup alerts to be able to provide medical treatment once notified from a smart device controlled by the patient.
3. RPM **devices**
RPM devices are sensor driven devices used to collect the pertinent health data. RPM devices will be streaming data to smart devices like smartphones and raw medical data is transferred promptly. These state of the art devices

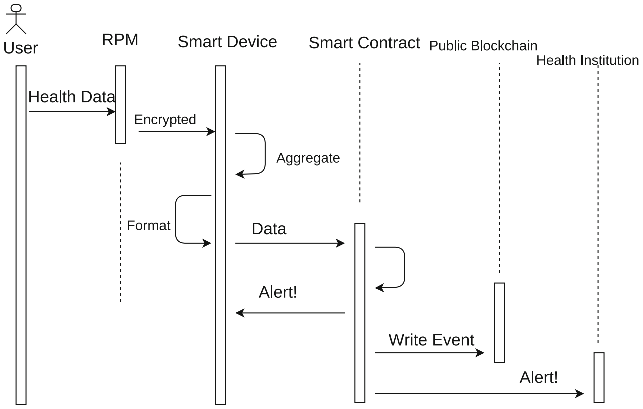

Fig. 7. System overview

will be able to measure many different types of vitals without ever being near a medical treatment facility.

4. `GHOSTDAG` **Blockchain**
   The use of two blockchains is needed, a private blockchain where smart contracts are used to monitor the patient's own healthdata. The smart contracts once setup can effectively issue alerts which can be written to the public blockchain. These transactions that are written to the public blockchain. The private and public blockchains are based on directed acyclic graphs which will be described in detail in Sect. 5.4.
5. **Authorizes Entities**
   A patient may request the sharing of their health data with a myriad of different types of stakeholders. Some examples include family members, insurance companies, medical units or perhaps even just to tender for health insurance.

5.1 Model Details

We use the following terminology for this section:

- Patient: P_i
- Raw Data: D
- `RPM` wearable device for Patient P: RPM_i
- Smart Device of Patient P: SD_i
- Encrypted Data: ED
- Private Blockchain: PRB
- Smart Contract for Patient P for condition C: SC_i^C
- Public Blockchain: PUB
- Symmetric Key: k_{sym}
- Asymmetric Key Pair: (rk_{priv}, rk_{pub})
- Symmetric Encryption function: $SE(data, k_{sym})$
- Asymmetric Encryption Function: $AE(data, rk_{priv})$

5.2 Technical Details

In this section, we will use an example for Patient P_i suffering from condition C to illustrate the use of the protocol. First, P_i will be equipped with RPM_i to monitor a given condition C. Raw sensor data D generated by patient P_i will be sensed through RPM_i and using a secure symmetrically encrypted path transmitted from RPM_i to SD_i using $SE(D, k_{sym})$ creating ED_1. There may be a processing step at SD_i to format ED for Private blockchain PRB to be used to compare with SC_i^C for a given condition C. Once SD_i sends the data to PRB, a smart contract SC_i^C for the specific condition C will compare reading with a normal range as specified in the contract. At this point, no further action is taken provided the readings are normal. However, if the readings are abnormal, an alert is generated by SC_i^C, sending alerts back to SD_i and authorized entities (Hospital, etc), while also sending a transaction write request to PUB using $AE(D, rk_{priv})$ generating ED_2. Authorized entities can access data ED_2 using there assigned public key rk_{pub}. In Sect. 5.3 we will outline the system requirements that will need to be maintained for security and privacy.

5.3 Requirements

In this section we give details and list some requirements the deployed system must possess. We give comments to requirements our system can achieve and for other we leave as future work.

1. **Strong Authentication**
   A major issue in healthcare is that most devices connect nowadays through a wireless connection. This opens up wireless data being accessed by adversarial users. Strong authentication of users should alleviate such problems, where users will have to prove who they are [10]. We propose using symmetric encryption in the private blockchain and asymmetric encryption in the public blockchain respectively. For accurate timestamps all devices must be logged into an IoT system. Only authorized entities can access health data as instructed by the patient from the public blockchain using their public key rk_{pub} as shared securely by patient to grant access.
2. **Scalability and Security**
   The GHOSTDAG blockchain is leaps ahead of the classic blockchain protocol in both security and speed of use. Its use here will ensure both scalability and security.
3. **Mutual Authentication:**
   In real-time, the user and RPM devices must authenticate one another. This way only trusted channels are used for communication. We propose a symmetric encryption scheme to ensure mutual authentication.
4. **Confidentiality**
   Any health related data can be considered highly sensitive and RPM devices connect only through a wireless connection. Therefore, health related data should stay private from common attacks like eavesdropping. Patient's data

needs to be transmitted only in encrypted form. As seen in Fig. 7 and details in Sect. 5.2, all transmitted data is shared in encrypted form.

5. **Session Key Establishment**
   There should always be a session key between a patient's device(s) and their respective RPM. This way, all communication can take place without fear of being compromised.
6. **Low Communication and Computational Cost**
   RPM devices are resource constrained devices, often created with low energy footprints and small CPUs. Moreover, healthcare application's on smart devices need some flexibility to run in the background not overly draining the device's resources. The protocol must be efficient both in computational, computational, and energy cost. The encryption function at the RPM device level needs to be light in nature. In [13] we propose such a scheme for encryption and decryption that are light in nature suitable for IoT. Moreover, use of a provable efficient blockchain protocol like GHOSTDAG, we ensure that the public and private blockchain will remain low impact [20].
7. **Fresh Data**
   Generally, patient data needs to be monitored at regularly. There must be some form of assurance that the data presented outside of the RPM device is recent. This protects against replay attacks.
8. **Secure Against Popular Attacks**
   Some level of defense should be provided against:
   - replay attacks
   - impersonation attack
   - stolen-verifier attack
   - password guessing attack
   - information-leakage attack

   Our use of symmetric encryption, asymmetric encryption, and secure blockchain protocol in combination provides relief against these types of attacks. We leave testing of this for Future Work as given in Sect. 6.
9. **User-Friendliness**
   Every aspect that involves the patient and other user's must be user-friendly.

5.4 GHOSTDAG Protocol

GHOSTDAG protocol, a variant of another protocol called PHANTOM [20], is a generalization of the original long singular blockchain protocol. The GHOSTDAG blockchain uses a directed acyclic graph (DAG) to structure the blocks. The blocks are placed in a k-cluster as given in Fig. 8. Figure 8 includes coloring of blocks. We see the block red in color as blocks outside the cluster. The blue blocks are inside the cluster. The largest n-cluster of blocks within a given DAG: A, B, C, D, F, G, I, J where $k = 3$ blue in color. Within a cluster, each block has ≤ 3 blue blocks in its anticone. For blocks E, H, and K, red in color have > 3 elements in their anticone respectively. Setting the value of k as 3, the upper limit is set to be 4 blocks that can be created per unit of time. GHOSTDAG finds

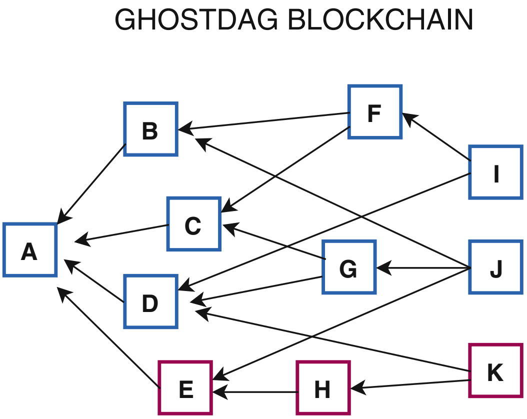

Fig. 8. k-cluster of GHOSTDAG (Color figure online)

a cluster using a greedy algorithm which differs from how PHANTOM does it. The optimization version of the maximum k-cluster problem is NP hard as shown in [12]. This sadly makes the PHANTOM protocol less practical for large blockDAGs. In contrast, finding a k-cluster for $k = 3$ is a feasible problem. This allows the GHOSTDAG protocol using a greedy algorithm more suitable for actual real world implementation.

6 Future Work

As a preliminary model, there is ample room for future work to the novel work presented here. A natural first step would be a simulation environment, to help gauge the performance of the protocol. Furthermore, an in-depth comparative analysis with some existing protocols would show the effectiveness of our scheme. That being said, the work in healthcare blockchain is still in its infancy with limited work presented thus far. To assist to demonstrate specific security goals, performance, limitations, computation complexity, and communication overhead in the IoT-based RPM environment, a simulation environment can help answer some of these questions as a natural next step. In a different direction, a mathematical overview of the schemes beyond what is presented here will also give some provable security guarantees of the protocol.

7 Conclusion

We utilized a GHOSTDAG blockchain that makes use of smart contracts to monitor the health data of patients. Smart contracts are used to trigger alerts when appropriate using patients health data and also record the details of events in blocks in either a private or public blockchain, based on the sensitivity of the actual data that needs to be stored. In a vital HIPAA-compliant manner for actual use, our model successfully delivers health-related notifications. Patient health information is not openly stored on the blockchain. It is well known that placing all health records on a blockchain is infeasible in size, which would require much more storage than IoT system nodes could provide. In place of this health data is transferred to EHR units. Slow computational speed and energy consumption are major issues in current blockchain implementations. Our model attempts to alleviate these issues and offers a secure, high-throughput, fast and reliable RPM system compared to any system that attempts to use a classic blockchain RPM system.

The proposed approach described in this paper is an initial work in progress that offers a blockchain-based model glimpsing into any IoT-based RPM system. The main next step for this project is a test-base able to implement the protocol to provide some experimental results to prove efficiency, scalability, security, and computational load.

References

1. Amiri, W.A., Baza, M., Banawan, K., Mahmoud, M.M.E.A., Alasmary, W., Akkaya, K.: Privacy-preserving smart parking system using blockchain and private information retrieval. CoRR abs/1904.09703 (2019). http://arxiv.org/abs/1904.09703
2. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, August 2016. https://doi.org/10.1109/OBD.2016.11
3. Bayern, M.: Why 70% of healthcare orgs have suffered data breaches (2019). https://www.techrepublic.com/article/why-70-of-healthcare-orgs-have-suffered-data-breaches/. Accessed 17 July 2019
4. Baza, M., Lasla, N., Mahmoud, M., Abdallah, M.M.: B-ride: ride sharing with privacy-preservation, trust and fair payment atop public blockchain. CoRR abs/1906.09968 (2019). http://arxiv.org/abs/1906.09968
5. Beninger, P., Ibara, M.A.: Pharmacovigilance and biomedical informatics: a model for future development. Clin. Ther. **38**(12), 2514–2525 (2016)
6. ConsenSys: A visit to the oracle (2016). https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f
7. Dwivedi, A.D., Malina, L., Dzurenda, P., Srivastava, G.: Optimized blockchain model for internet of things based healthcare applications. In: 42nd International Conference on Telecommunications and Signal Processing, TSP 2019, Budapest, Hungary, 1–3 July 2019, pp. 135–139 (2019). https://doi.org/10.1109/TSP.2019.8769060
8. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019). https://doi.org/10.3390/s19020326
9. Homayoun, S., Dehghantanha, A., Parizi, R.M., Choo, K.R.: A blockchain-based framework for detecting malicious mobile applications in app stores. In: 32nd IEEE Canadian Conference of Electrical and Computer Engineering (IEEE CCECE 2019) (2019)

10. Kumar, P., Lee, S.G., Lee, H.J.: E-sap: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors **12**(2), 1625–1647 (2012). https://doi.org/10.3390/s120201625. https://www.mdpi.com/1424-8220/12/2/1625
11. Liu, V., Musen, M.A., Chou, T.: Data breaches of protected health information in the united states. JAMA **313**(14), 1471–1473 (2015)
12. Mahajan, M., Nimbhorkar, P., Varadarajan, K.: The planar k-means problem is NP-hard. In: Das, S., Uehara, R. (eds.) WALCOM 2009. LNCS, vol. 5431, pp. 274–285. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00202-1_24
13. Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., Fujdiak, R.: A secure publish/-subscribe protocol for internet of things. IACR Cryptology ePrint Archive 2019, 740 (2019). https://eprint.iacr.org/2019/740
14. Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., Fujdiak, R.: A secure publish/subscribe protocol for internet of things. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, 26–29 August 2019, pp. 75:1–75:10 (2019). https://doi.org/10.1145/3339252.3340503
15. Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–3. IEEE (2016)
16. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
17. Parizi, R.M., Dehghantanha, A., Choo, K.R., Singh, A.: Empirical vulnerability analysis of automated smart contracts security testing on blockchains. In: Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, CASCON 2018, Markham, Ontario, Canada, 29–31 October 2018, pp. 103–113 (2018). https://dl.acm.org/citation.cfm?id=3291303
18. Parizi, R.M., Homayoun, S., Yazdinejad, A., Dehghantanha, A., Choo, K.R.: Integrating privacy enhancing techniques into blockchains using sidechains. In: 32nd IEEE Canadian Conference of Electrical and Computer Engineering (IEEE CCECE 2019) (2019)
19. Pennic, F.: Healthcare Blockchain Startup BurstIQ Secures $5M Investment (2018). https://hitconsultant.net/2018/02/23/healthcare-blockchain-startup-burstiq-secures-5m. Accessed 17 July 2019
20. Sompolinsky, Y., Zohar, A.: PHANTOM, GHOSTDAG: two scalable blockDAG protocols. IACR Cryptology ePrint Archive 2018, 104 (2018)
21. Srivastava, G., Dwivedi, A.D., Singh, R.: Crypto-democracy: a decentralized voting scheme using blockchain technology. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, ICETE 2018. SECRYPT, Porto, Portugal, 26–28 July 2018, vol. 2, pp. 674–679 (2018). https://doi.org/10.5220/0006881906740679
22. Srivastava, G., Dwivedi, A.D., Singh, R.: PHANTOM protocol as the new crypto-democracy. In: Computer Information Systems and Industrial Management - Proceedings of the 17th International Conference, CISIM 2018, Olomouc, Czech Republic, 27–29 September 2018, pp. 499–509 (2018). https://doi.org/10.1007/978-3-319-99954-8_41
23. Sullivan, C., Burger, E.: E-residency and blockchain. Comput. Law Secur. Rev. **33**(4), 470–481 (2017)
24. Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.K.R.: A systematic literature review of blockchain cyber security. Digit. Commun. Netw. (2019)

25. Vomiero, J.: Cybersecurity of medical devices under scrutiny after FDA recalls insulin pumps (2019). https://globalnews.ca/news/5446037/insulin-pump-medical-implant-cyber-attack-fda/. Accessed 17 July 2019
26. Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Choo, K.R.: Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. IEEE Trans. Netw. Sci. Eng. 1–14 (2019). https://doi.org/10.1109/TNSE.2019.2937481