INTI JOURNAL | eISSN:2600-7320
Vol.2022:21

Reducing Risks and Enhancing Security and Privacy in IoT-based Health Monitoring Application using Blockchain Technology

Chitra Batumalai[1], Assoc. Prof. Ir. Dr. Malathy Batumalay[1*], Chelsey Chang Yin Hang[1],

[1] Faculty of Data Science and Information Technology, INTI International University, Persiaran Perdana BBN, Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia.

[*]**Email:** malathy.batumalay@newinti.edu.my

Abstract

Due to the pandemic Covid-19, human's health has become one of the most important things to pay more attention to in our daily life. Pandemic Covid-19 could be controlled by social distancing. Therefore, if the condition is allowed, humans are encouraged to not have any physical touching between each other. The Internet of Things (IoT) based Health Monitoring Application is proposed for the medical staff to monitor their patients through their mobile devices. The proposed system allows patients to update their daily health condition to the system and medical staffs are able to monitor their patients through the system by their mobile devices. The proposed system is more feasible than most of the existing system because it is an application that can be accessed from their mobile devices rather than only browsing the website using the laptop or computers. Since patients can update their own health condition to the system, they are not required to go to the hospital for a medical check-up. They are required to go for a medical check-up only if or when doctors find abnormal symptoms in patients' recorded health. Besides, personal health conditions are considered as confidential information. Therefore, the author would analyze the security risks and the risks of the backend system of the proposed solution. Furthermore, the author would also enhance the security and privacy of the proposed system by implementing Blockchain Technology.

Keywords

IoT health monitoring system, Security and privacy, Blockchain technology

Introduction

Referring to the latest condition in the world, there are number of patients are increasing rapidly due to the pandemic of Covid-19. (Vrshneya, 2020) points out that in the battling with the pandemic Covid-19, digital tools such as telehealth is playing an important role in this situation. 'Telehealth is the use of digital information and communication technologies, such as computers and mobile devices, to access health care services remotely and manage your health care'(Mayo-Clinic-Staff, 2020). Telehealth is still growing and is a relatively new research. Many studies had shown the approach on developing telehealth using IoT resources.

Submission: 4 November 2021; **Acceptance:** 10 May 2022

Copyright: © 2022. All the authors listed in this paper. The distribution, reproduction, and any other usage of the content of this paper is permitted, with credit given to all the author(s) and copyright owner(s) in accordance to common academic practice. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license, as stated in the website: https://creativecommons.org/licenses/by/4.0/

There are incomparable advantages like improving the health of patients, quality and efficiency of the treatments with the use of technology-based healthcare method (Patel Nasrullah, n.d.). The benefits of using technology-based healthcare methods are real-time reporting and monitoring, end-to-end communication, tracking and alerts, etc. (*Benefits of Using IoT in Healthcare Industry*, 2019; Patel Nasrullah, n.d.).

As telehealth is still a relative new research that provides an end-to-end communication, hence, Blockchain Technology is used to enhance the security and privacy of the proposed system as this is the main problem of the telehealth technology. Blockchain is a system that stores information in a special way which makes the information hard or impossible to edit, hack, or cheat the system. A Blockchain is distributed across the network that does not require any third party to be involved. Therefore, only the authorized users are allowed to enter the network to get the information.

Methodology

Background study, conduct interview session, and conduct questionnaire session are the processes used by the author to collect the data. The author had read through many journals, article and did some background study to understand more about the IoT health monitoring system and study the risks and security problems raised by the IoT health monitoring system.

By conducting the interview session with the experienced medical staff, the author gets to know in-depth understanding about the procedures and processes of the healthcare system. Besides, the author gets to know the features and functions needed to be included in the system from the experienced medical staff to develop a more efficient and effectiveness system.

From the questionnaire session, the author gets to collect more information from the target users about the IoT health monitoring system, and to get to know whether the target users were alert with the existing risks, security, and privacy issues of the IoT health monitoring system. Also, the author was got to know whether the target users think that Blockchain Technology could enhanced the existing risks, security, and privacy issues.

By using the data gathered from all the research above, the author had successfully developed an IoT Health Monitoring System using Blockchain Technology to reduce the risks and enhance the security and privacy issues.

Results and Discussion

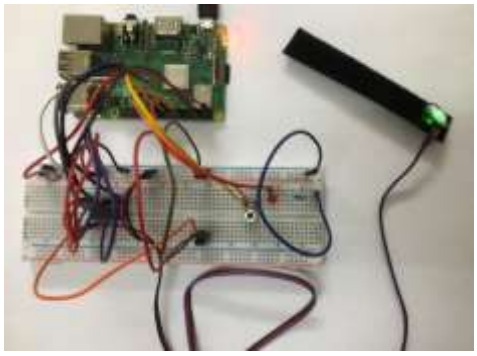

Figure 1. Setting Up the Sensors

In Figure 1, it is showing how the author had set up the sensors. The motherboard used is Raspberry Pi 3 B+. The reason of choosing this is because it supports wireless connection which allow the author to connect to the motherboard wirelessly. Besides, the author has included the 2 main sensors used to monitor the health condition which are Temperature sensor and Pulse Rate Sensor. Also, the author has included the Push Button Sensor which act as an emergency button, allowing the user to press the button if they were in bad condition.

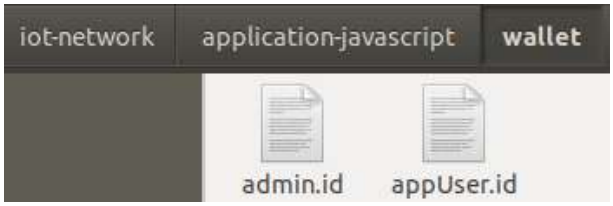

Figure 2. Wallet of Blockchain holding User ID

The Blockchain Technology selected in this proposed system was Hyperledger Fabric Blockchain. It is a private blockchain which using Certificate Authorities to generate the ID of the user. The main features of the proposed system used to enhance the security was only the admin of the system can register the authorized user into the blockchain network. Once the user was successfully register, the ID will be created in the wallet of the blockchain network as shown in Figure 2.



Figure 3. IoT Server running on Blockchain Network



Figure 4. Web Server running on Blockchain Network

With the use Blockchain Technology to enhance the privacy and security issues, the author had developed the IoT server and the Web server to be running on the Blockchain Technology, where only the registered user can access to it. With this, it was much reducing the attacking from outsiders such as attackers and hackers to hack the users' personal health data.

Referring to Figure 3, the IoT server is subscribing to the MQTT Broker. MQTT Broker is a lightweight transport protocol using a publish or subscribe message queuing model to carry out the message (*MQTT Documentation*, 2021). It was act as a connection between the IoT sensors and the IoT server to send and receive data.

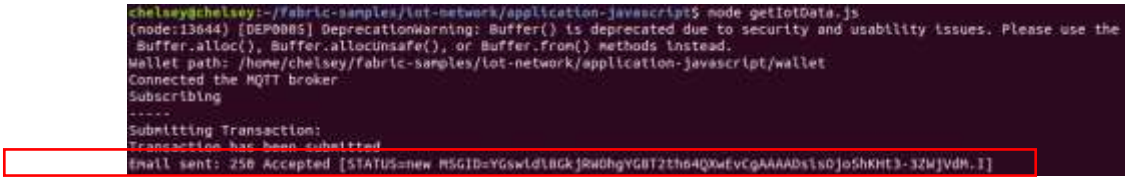

Figure 5. Email sent when button is pressed

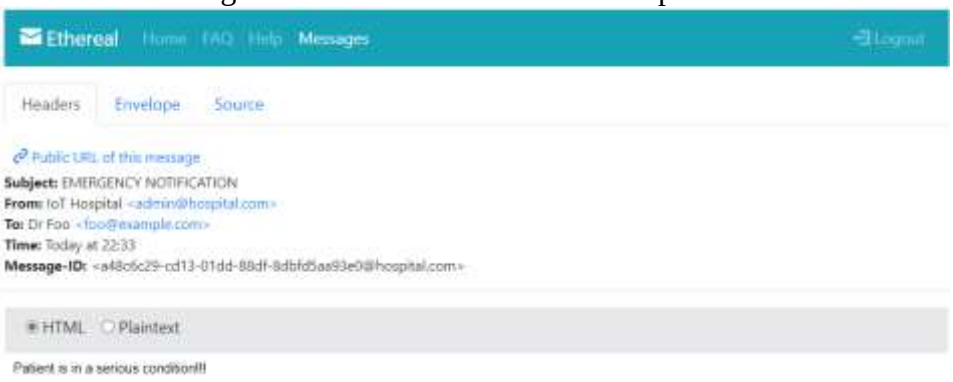

Figure 6. Example Mailbox sent when the button is pressed

From Figure 5 and 6, it was showing the example of sending email notification to the medical staff when the patient or user pressing the emergency button. This feature was to alert the medical staff that their patient was in a bad condition, hence, they can take action immediately.

Conclusion

The proposed system has been successfully develop and tested by the author. The IoT server and the Web server were successfully running on the Blockchain Network which to reduce the risks on being attack by the hackers or attackers to retrieve users' data during the data transmission. Besides, the membership service which using the Certificate Authority was playing an important role to allow user access to the Blockchain Network. Lastly, registered users were allowed to measure their health condition using the sensors and data was successfully transmit from the sensors to the Blockchain Network.

Acknowledgements

The author would like to express her special thanks of gratitude to the university who gave her the golden opportunity to do this wonderful project on the topic, "Reducing Risks and Enhancing Security and Privacy in IoT-based Health Monitoring App using Blockchain Technology", which also allowing the author to do a lot of research and came to know about so many new things. Besides, the author would also like to thanks to INTI International University, especially to all the lecturers of Faculty of Data Science and Information Technology on teaching and providing her the new knowledges throughout her whole Diploma and Degree study journey. It is very useful to complete the whole project.

References

Digiteum. (2019). *Benefits of using IoT in healthcare industry*. https://www.digiteum.com/iot-benefits-healthcare-industry

Cirstea, A., Enescu, F. M., Bizon, N., Stirbu, C., & Ionescu, V. M. (2019). Blockchain technology applied in health: The study of blockchain application in the health system (II). In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1–4). IEEE. https://doi.org/10.1109/ECAI.2018.8678952

Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: A security framework for the Internet of Things. *Security and Communication Networks, 9*(18), 3083–3094. https://doi.org/10.1002/sec.1259

Business Insider Intelligence. (2020). *The security and privacy issues that come with the Internet of Things*. https://www.businessinsider.com/iot-security-privacy

Mayo Clinic Staff. (2020). *Telehealth: Technology meets health care*. Mayo Clinic. https://www.mayoclinic.org/healthy-lifestyle/consumer-health/in-depth/telehealth/art-20044878

CloudMQTT. (2021). *MQTT documentation*. https://www.cloudmqtt.com/docs/index.html

Patel, N. (n.d.). *Internet of things in healthcare: Applications, benefits, and challenges*. Peerbits. Retrieved September 15, 2020, from https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html

Personal Data Protection Act (PDPA). (2010). *Laws of Malaysia Act 709 Personal Data Protection Act 2010*. http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf

Raspberry Pi Foundation. (2021). *Raspberry Pi 3 Model B+*. https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

Ren, Z., Liu, X., Ye, R., & Zhang, T. (2017). Security and privacy on Internet of Things. In *2017 IEEE 7th International Conference on Electronics Information and Emergency*

Communication (ICEIEC) (pp. 140–144). IEEE. https://doi.org/10.1109/ICEIEC.2017.8076530

Sadek, I., Rehman, S. U., & Codjo, J. (2019). Privacy and security of IoT-based healthcare systems: Concerns, solutions, and recommendations. In M. Mokhtari, B. Abdulrazak, & H. Aloulou (Eds.), *Inclusive Smart Cities and e-Health: ICOST 2019* (pp. 3–17). Springer. https://doi.org/10.1007/978-3-030-32785-9_1

Shirey, R. (2007). *RFC 4949: Internet security glossary, version 2*. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4949

Singh, N. (2020). *Permissioned vs permissionless blockchains*. 101 Blockchains. https://101blockchains.com/permissioned-vs-permissionless-blockchains/

Vrshneya, R. (2020). How technology is helping healthcare practitioners combat the COVID-19 pandemic. *The Journal of mHealth*. https://thejournalofmhealth.com/how-technology-is-helping-healthcare-practitioners-combat-the-covid-19-pandemic/

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, *136*, 10–29. https://doi.org/10.1016/j.comcom.2019.01.006