Blockchain-based and IoT-based Health Monitoring App: Lowering Risks and Improving Security and Privacy

Chelsey C. Y. Hang, M. Batumalay, T D Subash, R. Thinakaran, B. Chitra
Faculty of Data Science and Information Technology, INTI International University, Malaysia, Nilai, Malaysia[1, 2, 4, 5]
Key Laboratory of Oceanographic, Big Data Mining and Application-School of Information Engineering,
Zhejiang Ocean University, Zhoushan, Zhejiang China[3]

***Abstract*—Blockchain technology is known for its decentralized and immutable nature, which makes it highly resistant to hacking and unauthorized access. This would ensure that patients' private health information remains secure and protected from potential breaches. Moreover, the use of blockchain can also enhance data integrity by creating a transparent and tamper-proof record of all health updates, further increasing trust in the systems. The COVID-19 epidemic has made human health one of the most crucial things we should focus on more in our day-to-day lives. Social separation could help contain the COVID-19 pandemic. Humans are therefore urged to avoid physical contact with one another if the condition is permitted. It is suggested that medical professionals use the Internet of Things (IoT)-based Health Monitoring Application to keep an eye on their patients via their mobile devices. With the help of the suggested system, patients can update the system with their daily health status, and medical professionals can use their mobile devices to monitor their patients for future health policy. Because the suggested system is an application that users can access from their mobile devices rather than just using a laptop or computer to browse the website, it is more practical than most of the current system. Patients do not need to visit the hospital for a check-up because they can update the system with their health information. If physicians discover unusual symptoms in a patient's medical record, are they obligated to seek medical attention? Furthermore, private health information is regarded as confidential. Consequently, this would examine the risks associated with the backend system of the suggested solution as well as security threats. Additionally, by utilizing blockchain technology, improvements in security and privacy can be achieved.**

***Keywords*—IoT health monitoring system; security and privacy; and blockchain technology; health policy**

I. Introduction

In reference to the most recent global ailment, the number of patients is fast rising because of the COVID-19 pandemic. According to study [1] telemedicine and other digital tools are becoming more and more important in the fight against the COVID-19 epidemic. According to the study [2], "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." Being a relatively new field of study, telehealth is still expanding. Numerous studies have demonstrated the strategy for leveraging IoT resources to develop telehealth. These studies have shown that integrating IoT devices into telehealth systems can improve patient monitoring, increase access to healthcare services, and enhance overall patient outcomes. Additionally, the use of IoT in telehealth has the potential to reduce healthcare costs and alleviate the burden on traditional healthcare systems. As technology continues to advance, further research and development in this field will likely lead to even more innovative applications of IoT in telehealth. Internet-of-Things (IoT) in healthcare is a system that consists of various sensors or devices to collect data and store it in the cloud online. IoT Healthcare Monitoring system allows many end-users like doctors and patients access to the system. IoT sensors or devices are generating real-time data which the doctors are using to analyze the patient's health condition and create outcomes. The communication between the sensors or devices with the cloud is connected through Internet-Connected Gateways like Wi-Fi or Bluetooth.

Using technology in healthcare has unmatched benefits, such as improving patient health and treatment quality and efficiency [3]. Real-time reporting and monitoring, end-to-end connectivity, tracking, alarms, and other features are advantages of employing technology-based healthcare techniques. Additionally, IoT in telehealth can also improve access to healthcare services, particularly for individuals in remote or underserved areas. This technology enables patients to receive virtual consultations and monitoring, reducing the need for travel and increasing convenience. Furthermore, the integration of IoT devices with electronic health records can enhance data collection and analysis, leading to more personalized and effective treatment plans.

Since the primary issue with telehealth technology is its security and privacy, blockchain technology is utilized to improve the proposed system's security and privacy, even if telehealth research is still relatively young and only offers end-to-end communication. Blockchain technology keeps data in a unique manner that makes it difficult or impossible to alter, hack, or manipulate the system. A blockchain is dispersed throughout the network without the need for outside involvement. As a result, the only people who are permitted to access the network and obtain information are authorized users. This ensures that patient data remains secure and confidential, reducing the risk of unauthorized access or data breaches. Additionally, blockchain technology provides a transparent and

auditable record of all transactions and interactions within the telehealth system, enhancing accountability and trust among users. With the continuous advancements in telehealth and blockchain technology, the future holds great potential for further strengthening the security and privacy of telehealth systems. Blockchain Technology into IoT system helps to enhance security and privacy. It is because 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.

II. Literature Review

"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. Telehealth is still growing and is relatively new research. Many studies have shown the approach of developing telehealth using IoT resources. Two main problems have been found throughout the research. Firstly, most of the current system is a system that needs to be browsed through a website using laptops or computers. This is inconvenient for the medical staff or doctors if they have outpatient cases. It is inconvenient for them to bring the laptops along during the outpatient cases. Therefore, a web application will be preferable to them, allowing them browsing through the website using their laptops, computers or even mobile devices [3].

Secondly, privacy, data security and data integrity are the challenges of IoT-based systems [4]. An IoT-based system connects the sensors or devices to the system with an internet connection and stores the data in the cloud. In an IoT system, data is moving around to be transmitted, stored, and processed. In between processing the data, a hacker can easily gain access to sensors or devices to change the data. Therefore, a system under a healthcare industry must have integrity and accuracy of the data to make sure the medical staff or doctors are getting the right information.

A permission and private blockchain can help in reducing risks on the front-end and back-end of a system. A permissioned blockchain is a blockchain that requires permission to join or access to the consensus. It supplies an additional level of security over the system. Permissioned blockchain is supplying membership service which allows creating differences in roles or views in the system (Singh, 2020). Membership service requires the users to register themselves to the blockchain and get a private key from the blockchain before they can access the network. This could enhance access control to the system. Besides, a private blockchain network is only allowing a certain company or single organization to take part. It only allows a small group controls to the network [5]. A given participant is only allowed to see the given instance of a smart contract within that network. A private network could enhance the privacy and security of the proposed system

III. Methodology

The waterfall model was applied to the system development process in this study. The waterfall model allows for a systematic and sequential approach to developing the telehealth system, ensuring that each phase is completed before moving on to the next. This methodology also facilitates thorough documentation and clear communication between stakeholders, which is crucial for the successful implementation of a secure and efficient telehealth system. Additionally, by following this model, any potential issues or risks can be identified early in the development process, allowing for timely mitigation strategies to be put in place.

A. Phase 1: Data Collection

As the proposed system is related to the healthcare industry, conducting an interview session with the experienced medical staff to get an in-depth understanding of the healthcare procedure and the features was included in the proposed system. Enhancing the system's efficiencies and making it more accurate or useful would be beneficial to the proposed system and the overall telehealth experience. Incorporating cutting-edge technologies like artificial intelligence and machine learning algorithms can help achieve this by analyzing patient data and offering individualized recommendations or diagnoses. Additionally, continuous feedback from both patients and healthcare providers should be sought to ensure that the system is meeting their needs and addressing any potential limitations or shortcomings in the future.

The methods employed to get the data were background research, questionnaires, and interviews. To gain a deeper understanding of the Internet of Things health monitoring system and analyze the hazards and security issues it raises, numerous publications, articles, and background research were deployed. Additionally, the questionnaires were distributed to healthcare professionals and telehealth system users to gather insights on their experiences and perceptions of security and privacy in telehealth. In addition, expert opinions are obtained, and the research findings are validated through interviews with subject-matter experts. These interviews provided valuable insights into the potential hazards and security vulnerabilities of the Internet of Things health monitoring system. Furthermore, the analysis of existing telehealth platforms helps to identify common security measures and best practices that can be applied to mitigate these risks.

The questions were divided into two sections to study on IoT-based Health Monitoring system and their relation with Privacy and Security. The outcome was to determine whether the experienced medical staff had heard about the IoT-based Health Monitoring system. On the other hand, the Privacy and Security related questions were to determine whether the experienced medical staff had other suggestions or opinions on enhancing the IoT-based Health Monitoring system.

Comprehensive knowledge of the protocols and workings of the healthcare system was acquired through interviews with experienced medical staff. The skilled medical team's recommendations for adding the appropriate new features and functions led to the creation of a system that was also more effective and efficient. The input provided valuable insights from experienced medical staff, which helped in gaining a comprehensive understanding of the protocols and workings of the healthcare system. By incorporating their suggestions, a more effective and efficient IoT-based health monitoring system was developed. However, it is essential to continuously seek

feedback from medical professionals to ensure ongoing improvement and development of the system.

Conversely, a series of questionnaires disseminated via Google Form sought additional data from the intended audience regarding the IoT health monitoring system in order to ascertain whether the intended audience was aware of the risks, security, and privacy concerns associated with the IoT health monitoring system. Additionally, details regarding the target customers' perceptions of how blockchain technology could worsen current security, privacy, and risk issues. The feedback received from medical professionals is crucial in order to address any potential flaws or shortcomings of the system and make necessary improvements. This iterative process ensures that the IoT health monitoring system remains up-to-date and effective in meeting the needs of both medical professionals and patients. Furthermore, gathering insights from the intended audience regarding their awareness of risks, security, and privacy concerns associated with the system helps in designing appropriate measures to mitigate these concerns and build trust among users. Understanding their perceptions of how blockchain technology could exacerbate. These concerns are also crucial in order to address them effectively. Additionally, regularly conducting vulnerability assessments and penetration testing can help identify any potential weaknesses in the system's security measures. By continuously improving and updating the system based on user feedback and emerging technologies, the IoT health monitoring system can ensure that it remains secure, reliable, and trusted by both medical professionals and patients alike.

The analysis shows that respondents agree that blockchain technology may improve an IoT system's security and privacy. The data gathered from all of the aforementioned research projects allowed for the successful development of an IoT health monitoring system using blockchain technology to reduce risks and enhance security and privacy issues. Additionally, the research findings highlighted the importance of user education and awareness about blockchain technology to ensure its effective implementation. This can be achieved through informative campaigns and training programmes to address any misconceptions or fears related to the technology. Ultimately, the successful integration of blockchain in IoT systems can lead to increased user trust and confidence in the overall security and privacy of such systems.

B. Phase 2: System Design

System design is an important step in defining how the system is going to be developed. It is the process of outlining the elements of the system, such as the architecture of the system, components, and system interfaces and data, based on the requirements. Fig. 1 shows the use case diagram of the IoT-Blockchain Network. The use case diagram of the IoT-Blockchain Network provides a visual representation of how different components and actors interact within the system. It helps in identifying the various use cases and scenarios that can be implemented to ensure the seamless integration of blockchain technology in IoT systems. Additionally, this diagram serves as a blueprint for developers and stakeholders to understand the overall functionality and potential benefits of incorporating blockchain into IoT systems.

The component diagram in Fig. 2 was very useful for a complex or huge system. It was used to demonstrate the static implementation view of a system. With a component diagram, it helps to break down the system into smaller components and show how they interact with each other. This allows developers to easily identify the different functionalities and connections within the system, making it easier to design and implement the integration of blockchain technology in IoT systems. Additionally, the use case diagram helps stakeholders understand the specific use cases and scenarios where blockchain can be applied in IoT systems, enabling them to make informed decisions about its implementation and potential benefits.

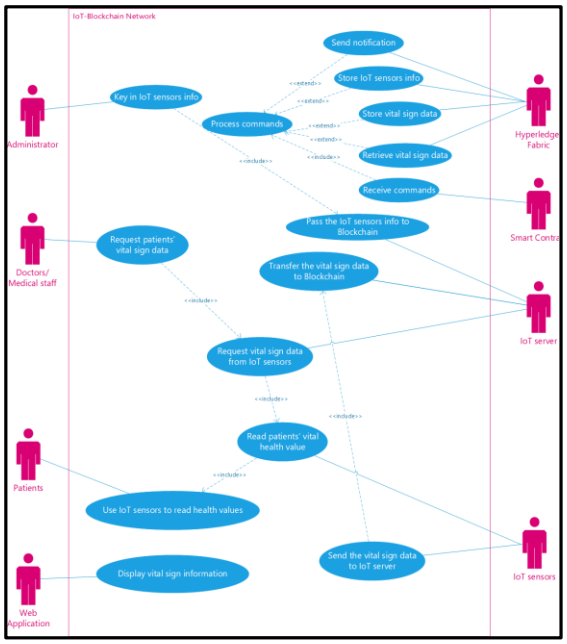

Fig. 1. Use case diagram for the IoT-blockchain network.

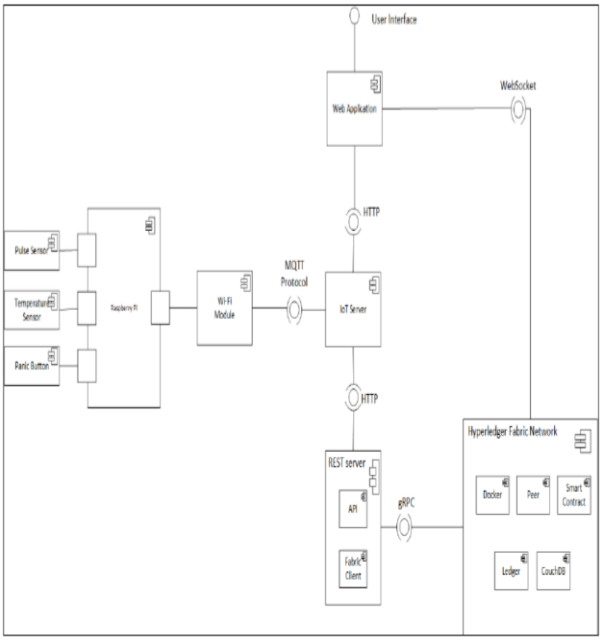

Fig. 2. Component diagram.

C. Phase 3: Implementation

In this development process, Ubuntu Linux has been used to develop and implement the Hyperledger Fabric network. Docker Engine [4-5] is the industry's de facto container runtime that runs on various Linux and Windows operating systems (Docker, 2020a). It does have some tools and a universal packaging approach that wraps up all the dependencies of the application inside a container that will be run on a Docker Engine. 'Docker container image is a lightweight standalone, executable package of software that includes everything needed to run an application' (Docker, 2020b). Having a Docker Engine allows you to easily pull the images with the command provided and start the docker container runtime. It is used to pull the published release fabric images such as fabric-tools, fabric-ca, fabric-peer, ordered, etc. that had been deployed by the Hyperledger Fabric community.

Visual Studio Code was used to develop the chain code, also known as Smart Contract, of the Hyperledger Fabric network using the Node.js programming language. It was also used to develop the web application using Express.js, which is a framework for Node.js, and Pug as the templating engine. Cloud MQTT acts as a broker to receive messages from its publisher client and publish the messages received to its subscriber client. It plays an important role in the MQTT protocol, which is a communication protocol for IoT devices. Without the broker, the messages published could not be successfully sent to the subscribers.

Raspberry Pi [6] is a mini single motherboard that serves as a platform for programming IoT devices. It is used to control the sensors and run the necessary code for the proposed system. The proposed system includes several sensors, such as a temperature sensor, a pulse rate sensor, and a push button. These sensors are used to gather data related to the user's body temperature, heartbeat, and user interaction with the IoT system [7-8]. The temperature sensor is responsible for measuring the body temperature of the user. The pulse rate sensor measures the user's heartbeat in real-time. The push button serves as an input device for users to interact with the IoT system. The sensors collect valuable data, which is then transmitted to the broker using the MQTT protocol [9]. This allows subscribers to receive and process the information for various applications, such as health monitoring or environmental control.

D. Phase: Testing

To guarantee that the testing procedure is carried out efficiently, a test plan is developed. It also serves to guarantee that the methodologies used are appropriate for the proposed system's testing. Unit, integration, and functional testing of the proposed system are all included in the testing. The study examined the connection of Internet of Things (IoT) devices, servers, and brokers, as well as the data integrity between MQTT clients (IoT devices and servers) and brokers. Testing from the Internet of Things system to the web application via the blockchain network was fully included in the scope of the proposed solution. The test plan includes specific test cases for each component of the Internet of Things system, including the MQTT clients, servers, and brokers. Additionally, the testing process ensures that data integrity is maintained throughout the connection between these components. The proposed solution also encompasses comprehensive testing from the Internet of Things system to the web application via the blockchain network to ensure seamless integration and functionality.

At the end, user evaluation is compiled from comments and feedback from users who had never seen the suggested system before. The purpose is to learn about their opinions and reviews of the system, as well as how they feel about it. The author chose to hold a face-to-face meeting to introduce the suggested system to consumers because it is a novel system in comparison to the "traditional" system because it leverages blockchain technology to improve the Internet of Things system. Additionally, the suggested approach requires the network administrator to register the user directly and requires the user to use the offered IoT sensors; as a result, the only method available for evaluating users is in person. This approach ensures that consumers can have a hands-on experience with the system and provide immediate feedback [9-12]. Furthermore, conducting face-to-face meetings allows us to address any concerns or questions that consumers may have, ensuring a better understanding of the system's functionality and benefits.

IV. Results and Discussion

The setup of this proposed system is depicted in Fig. 3. The Raspberry Pi 3 B+ motherboard was selected because it allows wireless connections, which enables to establish a wireless connection with the motherboard. For monitoring a patient's health, two main sensors were utilized: a temperature sensor and a pulse rate sensor. The temperature sensor is designed to accurately measure the patient's body temperature and transmit the data to the Raspberry Pi 3 B+ motherboard. This allows for continuous monitoring and detection of any abnormal fluctuations in temperature. The pulse rate sensor, on the other hand, is responsible for monitoring the patient's heart rate. It uses advanced optical technology to capture the blood flow in the patient's fingertip and convert it into pulse rate data. This information is then transmitted wirelessly to the Raspberry Pi 3 B+ motherboard for real-time analysis and monitoring.

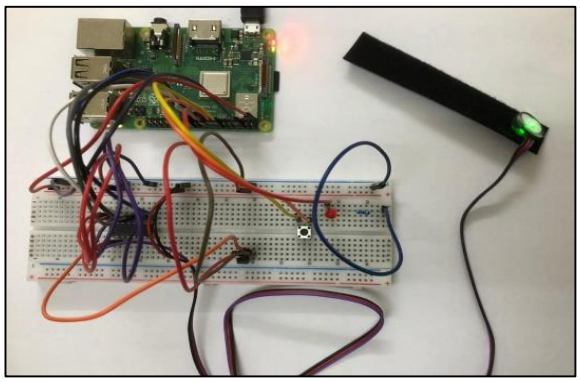

Fig. 3. Setting up the sensors.

One of the key features of the proposed system is the utilization of wireless connections. These wireless connections allow for seamless communication between the sensors and the Raspberry Pi 3 B+ motherboard. By eliminating the need for physical cables, the system becomes more flexible and portable, enabling the patient to move around freely without any constraints. Additionally, wireless connections enable remote

monitoring of the patient's health. This means that healthcare professionals can access and analyze the patient's data from any location, providing timely interventions and reducing response time in critical situations. Furthermore, wireless connections also minimize the risk of tripping or tangling with cables, ensuring the safety and comfort of the patient.

The proposed system includes an emergency push-button sensor, which serves as a vital component for ensuring patient safety. This sensor is strategically placed within reach of the patient, allowing them to hit the button in the event of an emergency. When the button is pressed, a signal is immediately sent to the Raspberry Pi 3 B+ motherboard, triggering an alert. This alert can be programmed to activate various responses, such as notifying healthcare professionals, sending emergency messages to designated contacts, or even initiating an automatic emergency response system. By incorporating this emergency push-button sensor, the proposed system provides an extra layer of safety and reassurance to the patient, enabling immediate response and intervention in critical situations.

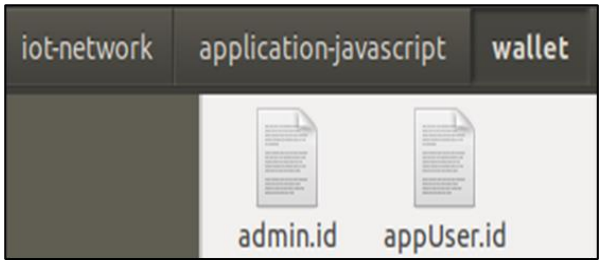

Fig. 4. Wallet of blockchain holding user ID.

The proposed system includes an emergency push-button sensor, which serves as a vital component for ensuring patient safety. This sensor is strategically placed within reach of the patient, allowing them to hit the button in the event of an emergency. When the button is pressed, a signal is immediately sent to the Raspberry Pi 3 B+ motherboard, triggering an alert. This alert can be programmed to activate various responses, such as notifying healthcare professionals, sending emergency messages to designated contacts, or even initiating an automatic emergency response system. By incorporating this emergency push-button sensor, the proposed system provides an extra layer of safety and reassurance to the patient, enabling immediate response and intervention in critical situations. To register an authorized user on the blockchain network, the system administrator follows a specific registration process. This process typically involves verifying the identity of the user and confirming their authorization to access the system. Once the user's identity is verified, the system administrator generates a unique ID for the user, which is then stored in the blockchain network's wallet as in Fig. 4. This ID serves as a digital representation of the user's authorization and allows them to securely access the blockchain network.

By using Hyperledger Fabric technology, the overall security of the system is significantly enhanced. One way this is achieved is using a private blockchain, which ensures that only authorized users have access to the network. This reduces the risk of unauthorized access and potential security breaches. Additionally, Hyperledger Fabric provides a tamper-proof record of all user IDs, meaning that any attempts to modify or manipulate the system can be easily detected and prevented. This transparency further strengthens the integrity of the solution and ensures that the system remains secure.

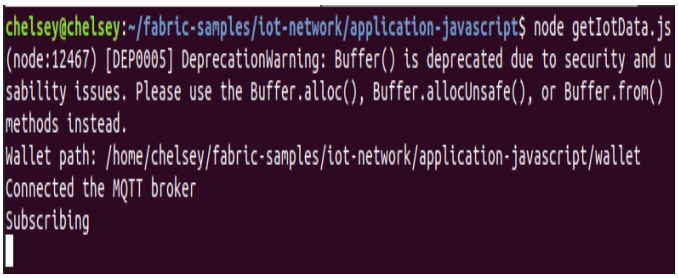

Fig. 5. IoT Server running on a blockchain network.

With reference to Fig, 5, the IoT server is subscribing to the MQTT Broker. MQTT Broker is a lightweight transport protocol that executes messages using a publish or subscribe message queuing scheme (MQTT Documentation, 2021). The MQTT Broker, using a publish or subscribe message queuing scheme, acts as a mediator between the IoT server and the sensors. When the sensors collect personal health data, they publish this data to the MQTT Broker. The IoT server, which is subscribed to the MQTT Broker, receives the published data from the sensors. This mechanism allows for efficient and reliable communication between the IoT server and the sensors, ensuring that the personal health data is transmitted securely and without interference. Blockchain technology enhances the security of the system by providing a decentralized and immutable ledger. When personal health data is collected by the sensors, it is recorded as a transaction on the blockchain. This transaction is then added to a block, which is linked to the previous block in the chain, creating an unbroken record of all data exchanges. The decentralized nature of the blockchain means that there is no single point of failure or vulnerability for hackers to exploit. Additionally, the immutability of the ledger ensures that once data is recorded, it cannot be manipulated or altered, providing an extra layer of security against unauthorized access or tampering.

Fig. 6. A web server running on a blockchain network.

Fig. 6 shows a web server running on a blockchain network. To address privacy and security concerns, the Internet of Things server and a Web server that operate on blockchain technology are only accessible by registered users. As a result, there was a significant decrease in the number of outside attacks on users' personal health data, including those by hackers and attackers.

Blockchain technology is known for its decentralized and immutable nature. As a result, it is less likely that unauthorized access or manipulation will occur to the personal health data stored on the Internet of Things server and Web server. Additionally, the use of cryptographic algorithms in blockchain ensures that the data remains encrypted and secure, further protecting the privacy of the users' personal health information.

Fig. 7. Email sent when the button is pressed.

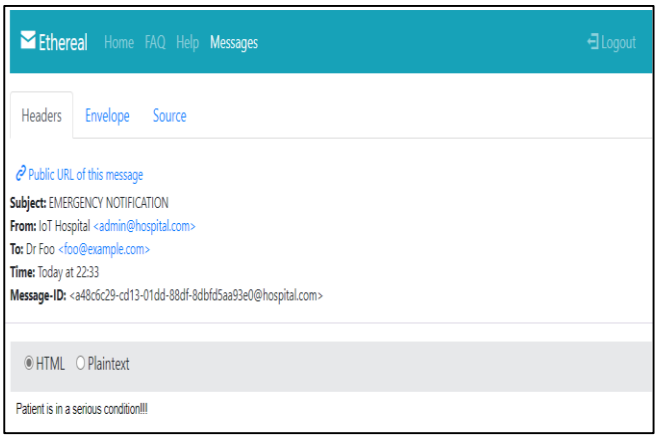

Fig. 8. Example Mailbox sent when user press the button.

Through a secure authentication process that authorized healthcare professionals can quickly complete, the implemented system permits emergency access [13-14]. This ensures that access to personal health data is balanced between privacy and security concerns and the need for timely medical intervention. A sample of notifying medical staff via email when a patient or user clicks the emergency button can be seen in Fig. 7 and Fig. 8. With this feature, the medical team would know that their patient was in critical condition and act accordingly. This feature enhances the response time and effectiveness of the medical team, potentially saving lives in emergency situations. It also ensures that the communication is secure and reliable, as the decentralized and immutable ledger guarantees the authenticity and integrity of the notifications sent to medical staff.

V. Conclusion and Future Enhancement

The system was created and tested to have good efficiency. To lower the possibility of being attacked by hackers or other attackers trying to retrieve user data while it was being transmitted, the Internet of Things server and the Web server were successfully operating on the blockchain network. In addition, the use of the Certificate Authority by the membership service was crucial in granting users access to the Blockchain Network. Finally, data was successfully transferred from the sensors to the blockchain network, enabling registered users to use the sensors to measure their health. The implementation of the blockchain network ensured that all data transmitted from the sensors to the network remained secure and tamper-proof. This provides users with peace of mind, knowing that their sensitive health information was protected from unauthorized access. Additionally, the successful integration of the membership service with the Certificate Authority streamlined the process of granting authorized users access to the Blockchain Network, enhancing overall system efficiency.

References

[1] 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/.

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

[3] Patel Nasrullah (n.d.) The 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.

[4] Lin, C., Nadi, S., & Khazaei, H. (2020, September). A large-scale data set and an empirical study of docker images hosted on docker hub. In 2020 IEEE International Conference on Software Maintenance and Evolution (ICSME) (pp. 371-381). IEEE.

[5] Ibrahim, M. H., Sayagh, M., & Hassan, A. E. (2021). A study of how Docker Compose is used to compose multi-component systems. Empirical Software Engineering, 26, 1-27.

[6] Raspberry Pi 3 Model B+ (2021) Raspberrypi.Org. https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/.

[7] Ren, Z., Liu, X., Ye, R., & Zhang, T. (2017). Security and privacy on the internet of things. Proceedings of the 2017 IEEE 7th International Conference on Electronics Information and Emergency Communication, ICEIEC 2017, 140–144. https://doi.org/10.1109/ICEIEC.2017.8076530.

[8] Sadek, I., Rehman, S. U., & Codjo, J. (2019). Privacy and Security of IoT-Based Healthcare Systems: Concerns, Solutions, and Recommendations 17th International Conference, ICOST 2019, 3–17. https://doi.org/10.1007/978-3-030-32785-9_1.

[9] MQTT Documentation (2021): CloudMQTT. https://www.cloudmqtt.com/docs/index.html.

[10] 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) 10th International Conference on Electronics, Computers, and Artificial Intelligence, ECAI 2018, II, 1–4. https://doi.org/10.1109/ECAI.2018.8678952.

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

[12] Sadek, I., Rehman, S. U., & Codjo, J. (2019). Privacy and Security of IoT-Based Healthcare Systems: Concerns, Solutions, and Recommendations 17th International Conference, ICOST 2019, 3–17. https://doi.org/10.1007/978-3-030-32785-9_1.

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

[14] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618.