Concept Designs of Patient Information Security Using e-Health Sensor Shield Platform on Blockchain Infrastructure

Syahril Efendi
Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Sumatera Utara, Indonesia

Baihaqi Siregar and Heru Pranoto
Doctoral Program, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Sumatera Utara, Indonesia

Abstract

Innovation in a decentralized blockchain infrastructure can be used by medicine as a prerequisite for the exchange of patient data. Developments in the medical device industry that support the technology of the internet of things and wireless sensor networks also facilitate the examination of patient medical records that no longer require visits to the practice of doctors or hospitals which in some cases takes in a considerable time. Not to mention the consideration of traffic congestion and busy routine in the work. Patients can check their healthcare concerns using only sensors such as e-Health Sensor Shield Platform which then sends recording results through the transmission line to the data lakes. However, this patient's medical record data is very confidential and may only be accessed by certain parties only. This required the design of the concept of security in the transmission of data so that the data does not leak to parties who are not eligible. This paper attempts to provide an overview of the concept of using encryption with an asymmetric key for securing data from sensors to data lakes before forwarding to a decentralized, interconnected blockchain infrastructure.

Keywords Patient monitoring, information security, e-health sensor, blockchain, internet of things

All papers within this proceedings volume have been peer reviewed by the scientific committee of the Malikussaleh International Conference on Multidisciplinary Studies (MICoMS 2017).

1. Introduction

In the medical world, on a general clinical examination of a patient, the doctor will determine the status of a patient's condition that includes the determination of vital signs such as blood pressure, pulse rate, body temperature, and respiration. Sometimes the doctor isn't present. If this happens, then the diagnosis should be postponed until the doctor returns. To prevent delayed analysis of diagnostic results mentioned above, this information technology innovation is used. It includes the delivery of data from the side of the patient to the system

Emerald Reach Proceedings Series
Vol. 1
pp. 641–646
Emerald Publishing Limited
2516-2853
DOI 10.1108/978-1-78756-793-1-00100

online so that doctors elsewhere can provide diagnoses from a distance to patients who examined their health condition. By its very nature, healthcare organizations operate in an environment where visitors and the wider community cannot be completely excluded. In large healthcare organizations, the number of people moving through the operational area is significant. These factors increase the vulnerability of the system to physical threats. The likelihood of such threats occurring may increase as the object of assistance or emotional related or mental related may be present. Many health organizations are chronically underfunded and their staff is sometimes forced to work under significant pressure. This often results in an increase in the error rate, including incorrect execution of the procedures. Other consequences of these resource constraints are that systems are designed, implemented and managed too relaxed, or a system continues to function long after they should have been withdrawn. These factors can increase the potential of some types of threats and can exacerbate the vulnerability. On the other hand, clinical care continues to be a process that involves several professionals, technicians, administrators, caregivers, and volunteers, many of whom consider their work as a call. The dedication and diversity of their experience can often reduce exposure to vulnerability. The high level of professional training that many health professionals receive also differentiates health care from many other sectors by reducing incidents related to internal threats. The duplication of information in the health sector has improved health services.

Doubling information in the health sector has improved health services. However, it has dangerous side effects: the risk of information security. By 2016, health information security breaches relate to more than 27 million patient records, as reported by the Identity Theft Resource Center and CyberScout. The next few years are not expected to be better for the health industry. Given the sensitive nature of data on health services and the increased risk of information security, it is essential that health service providers have reliable and reliable information security services. The strategy should not only react and protect health data, but also predict and prevent cybercrime attacks. Hackers are increasingly diverting hospital data and health facilities into a computer crime called ransomware (Infoguard Cyber Security, 2017). There are many people who claim that cost reduction is the hardest factor for health facilities. The fact is to protect patient information is more important and a cost-intensive reduction. To protect health information, you need a robust information security strategy. Your virtual security service should be proactive. It should be able to detect and counteract the attack before it actually happens. A good information security service will take into account the provision and monitoring of health information. It will evaluate how data is captured, stored, used, managed, and transmitted across departments, in the cloud, in the system, in the data centre, and on the network. We will therefore provide customized information security solutions tailored to your structure.

The high demand for patient records on the black market has triggered numerous cyberattacks that have damaged the reputation and finances of healthcare institutions. According to the Federal Bureau of Investigation, electronic health records (EHRs) are much more valuable than financial data. EHRs can be sold for $50 on the black market, compared with only $1 for social security numbers or credit cards (Infosec Institute, 2018). The EHR conforms to the patient’s name, date of birth, policy number, diagnosis code, and invoice information. The wealth of this data can be used by scammers in a variety of ways, such as creating fake documents to purchase medical equipment or reselling drugs. Some cybercriminals combine patient numbers with fake providers and then file claims for health insurance companies. EHRs are considered more valuable as they are more difficult to detect. The theft of EHR lasts twice as long as normal identity theft. Unlike stolen credit cards that can be erased and fraudulent charges that are questionable, medical identity theft is more complex and therefore difficult to resolve. It also means that cybercriminals have more time to "empty " the information they get from the EHRs. High prices ordered by EHRs on the black market could also be the main reason why cyberattacks on health care institutions are increasing at an alarming rate. Of course, hackers can make more money when they turn to health institutions than banks and other finance companies.

One application that can be done by this technology is in the application of biometric sensors. Biometric sensors are sensors that combine the physical features of the human body with digital technology to produce information for medical personnel. The sensors connected to the e-Health Sensor Shield on Raspberry Pi which are then paired to the patient's body can be stratified by the patient's health condition, such as body temperature, airflow, blood oxygen, glucometer, electrocardiogram, blood pressure, patient position, muscle sensor, and galvanic skin response (Libelium Comunicaciones Distribuidas S.L., 2017). Information captured by these sensors then can be transmitted via communication channels such as a 3G data connection to the data lakes for further medical analysis purposes. In this e-Health devices like camera modules, mic, and speakers for medical features in the form of audio and video formats can also be added. Data can be stored as static medical records and can also be performed in real time to medical parties located at remote locations. Blockchain is a type of data structure that is used to create a digital transaction log and share it between a distributed network of computers. The distribution network may include smartphones, tablets, cloud resources, or local computer nodes. Blockchain is an algorithm and a distributed data structure designed to manage electronic money without a central administrator (Wilson, 2017). The potential of Blockchain for healthcare depends on the willingness of hospitals, clinics, and other organizations to contribute to the creation of the necessary technical infrastructure. For example, the blockchain of health care needs a way to provide convincing information about the identity of a patient to everyone who needs it, anywhere (Orcutt, 2017).

2. Problem identification

In February 2016, the hackers held data hostage belonging to the Presbyterian Hollywood Health Center in Los Angeles. The hospital ended up paying 40 bitcoins ($17,000) to get key data decrypted from the hackers. The incident resulted in a one-week down time for installation. In another case, South Shore Hospital in Massachusetts agreed to pay $750,000 in damages after allegations that the center was unable to secure important health data for approximately 80,000 patients.

Patient health status data are highly confidential that only the patient, the patient's family, and the medical officer should check the patient's health. The interconnection of remote health monitoring systems with blockchain technology is very potential to be applied today. But behind the convenience of the benefits of this information technology innovation, the sense of security for its users should also be taken into account. To prevent leakage of patient data captured by sensors attached to the patient's body, an information security policy is required. One of them is to encrypt the patient's recorded data and will be sent via public communication channels such as internet.

There are different types of health information that must be protected for confidentiality, integrity, and availability (Hamidovic and Kabil, 2011):

- Personal health information.
- The interpreted data come from information on personal health through different methods for identifying pseudonyms.

- Statistical and research data, including anonymous data derived from personal health information, by deleting personal identity data.
- Clinical/medical knowledge not related to specific treatment subjects, including clinical decision support data.
- Data of health workers, staff, and volunteers; information relating to the surveillance of public health.
- Audit trail data generated by a health information system containing personal health information or pseudonym data comes from personal health information or contains data on user actions in relation to personal health information.
- System security data for health information systems, including access control data and other system configuration data related to health information security.

3. Previous research

In 2007, the Estonian government initiated the national implementation of a release chain to protect all EHRs in the country with keyless signature infrastructure for large-scale authentication. Estonia has virtually eliminated the need for a health information exchange system, a database of complaints or electronic medical records. This made the entire population much "smarter" and created a broad base of trust to access patient records. In 2016, this government allows the exchange of patient data, cross-border electronic services and electronic prescriptions (Afshar, 2017).

Matthias Mettler (2016) shows that Blockchain offers various possibilities for use in healthcare, for example, in the management of public health, user-oriented medical research, based on the personal data of patients and counterfeit medicines. The immense potential of this technology is evident everywhere, where until now the third party trust was needed to manage market services. With Blockchain, direct transactions are suddenly possible, thanks to which a central player, who controls the data, earns commissions, or even intervenes reprehensibly, can be eliminated. This disruptive nature, which is the basis of Blockchain technology, will strongly influence the balance of power among existing health workers. It will also promote new digital business models and digital health initiatives.

In the future data and intermediaries can be avoided, this technology opens new doors on how market interactions can be done in healthcare. Therefore, Blockchain has great potential for the future and will show disruptive changes in the health sector. Ariel Ekblaw *et al.* (2016) report that the MedRec prototype provides a proof-of-concept system that shows how decentralization principles and blockchain architectures can contribute to secure and interoperable EMD systems. Using Ethereum's Smart Contracts to organize a content access system across multiple sites and storage providers, the MedRec authentication registry provides access to medical records while patients receive registration, careful monitoring, and data exchange.

4. Concept designs

The concept of this system is to ensure that an encrypted procedure has been performed, before connecting to the blockchain infrastructure, to the data of patients caught by sensors connected to the e-Health platform, with the aim that this confidential patient health data may be protected from data theft such as man-in-the-middle attack. The asymmetric key is used as the key to this proposed concept. General architecture can be seen in Figure 1.

Patients data collected in data lakes are then submitted to blockchain infrastructure. In the blockchain itself has been running SHA-256 encryption function that is used as a secure

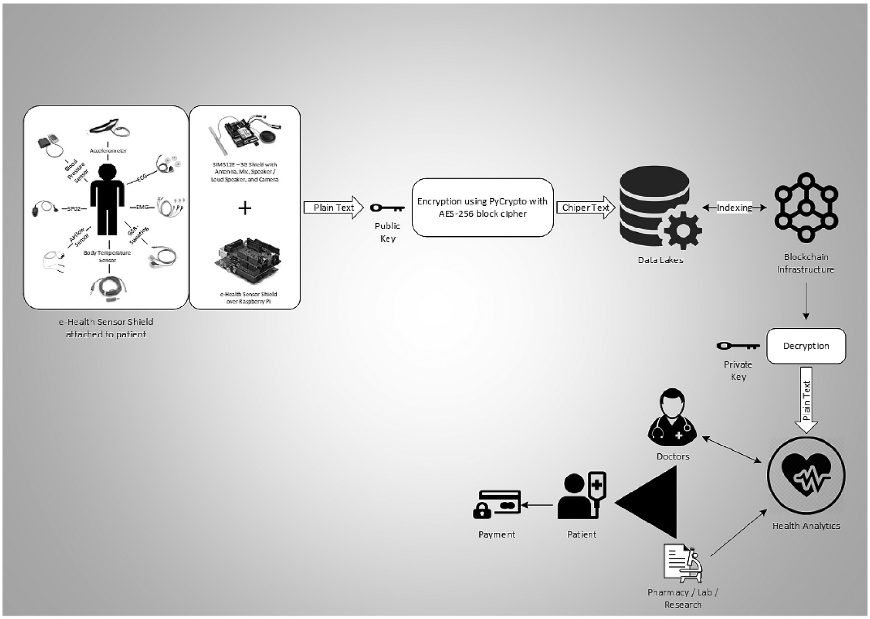
Accelerometer
Blood Pressure Sensor
ECG
SPO2
EMG
Airflow Sensor
GSR - Sweating
Body Temperature Sensor
SIMS12E – 3G Shield with Antenna, Mic, Speaker / Loud Speaker, and Camera
+
e-Health Sensor Shield over Raspberry Pi
e-Health Sensor Shield attached to patient
Plain Text
Public Key
Encryption using PyCrypto with AES-256 block cipher
Chiper Text
Data Lakes
Indexing
Blockchain Infrastructure
Decryption
Private Key
Plain Text
Doctors
Health Analytics
Payment
Patient
Pharmacy / Lab / Research

Figure 1.
General Architecture

delivery of data between nodes are interconnected and decentralized. Patient data can then be used as an analytical material for doctors and research laboratories to make decisions about what the health or illness of the patient is. As well as the pharmaceutical department to provide appropriate medication if needed.

5. Conclusions

Although the health industry is using Internet-based technologies more slowly than other industries, the Internet of medical products is poised to change the way people keep people safe and healthy solutions to reduce healthcare costs in the years to come. The Electronic Health Sensor, one of the Internet's medical devices, can not only help healthcare professionals monitor and inform, but it also provides health professionals with real data to identify problems before they can become critical.

The electronic health sensor could be a better way to take care of our elderly and has enormous potential to help cope with the rising costs of care. Devices with electronic health sensors can help monitor vital functions and cardiac function by monitoring glucose and other body systems and activities. Older people often forget to take prescribed medications on time and devices with electronic health sensors can help them remember and record when they take medications. In addition, portable diagnostic devices can facilitate routine blood and urine tests for the aging population. Portable diagnostic devices can analyze and report the results of these tests without the need to visit the consultation room. The online health sensors offer many possibilities to help caregivers to ensure the safety of their loved ones through portable devices that learn the routine of the person using the device and can give a warning if something goes wrong and warn if older people have passed their limits, which is often a concern for patients with memory care. A connected medical device provides objective reports on real activity, while independent providers must rely on the patient's subjective relationships to describe in detail how they feel. Similarly, electronic health detection devices help to regulate the patient's behavior and activity outside the office, so that the provider has real data to refer to the patient's therapeutic recommendations and to do so. It happens later when a patient leaves a medical center. As the number of connected devices increases, IT systems must determine how to handle transparent and secure data loading. In order for the functions of the e-Health sensors to be truly transformative, healthcare organizations must find out how all the collected data can be turned into ideas that inform the action. With the development of this transformation, hospital administrators, manufacturers, and suppliers will have to work together to promote the cultural transformation of medical care. For this reason, the initial design of the blockchain technology infrastructure has been proposed.

References

Afshar, V. (2017). "Blockchain Innovation in Healthcare and Life Sciences". Available: https://www.huffingtonpost.com/entry/blockchain-innovation-in-healthcare-and-life-sciences_us_59c91296e4b0b7022a646c4b

Ekblaw, A. Azaria, A., Halamka, J.D. and Lippman A. (2016). "A Case Study for Blockcha in in Healthc are: 'MedRec' Prototype for Electronic Health Records and Medical Research Data". Available: http://dci.mit.edu/assets/papers/eckblaw.pdf

Hamidovic, H., & Kabil, J. (2011). An Introduction to Information Security Management in Health Care Organizations. *ISACA Journal*, 5, 2–3.

Infoguard Cyber Security. (2017). "Why is Information Security Important for the Healthcare Sector". Available: http://www.infoguardsecurity.com/information-security-important-healthcare-sector/

Infosec Institute. (2018). Top Cyber Security Risks in Healthcare. Available: http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare

Libelium Comunicaciones Distribuidas, S.L. (2017). "e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi [Biometric / Medical Applications]". Available: https://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical

Mettler, M. (2016). Blockchain Technology in Healthcare The Revolution Starts Here. IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), (pp. 1–2). Chicago.

Orcutt, M. (2017). "Who Will Build the Health-Care Blockchain?" Available: https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/.

Wilson, S. (2017). "How it Works: Blockchain Explained in 500 Words". Available: http://www.zdnet.com/article/blockchain-explained-in-500-words/

Corresponding author

Syrahril Efendi can be contacted at