

Chapter 76

Blockchain and the Protection of Patient Information in Line with HIPAA

Colin DeLeon

Regent University, USA

Young B. Choi

Regent University, USA

ABSTRACT

Blockchains used for the protection of patient information can serve as a way for hospitals and other medical facilities to secure patient records. With more information threats targeting hospitals and other medical facilities, it is becoming more important for these organizations to improve the information systems that are charged with protecting their patient records. HIPAA regulations are in place to try and protect patient records and information, but the hospitals do not allocate enough funds to information systems so they are put at risk of attack. Blockchains can offer the type of protection that these medical facilities need without them having to worry about upgrading the technology every year. The Blockchain is not without its faults, and that can be seen in the attacks that take place against Bitcoin. Even with these attacks, the use of Blockchain would be beneficial to the hospitals and medical facilities.

INTRODUCTION

Medical records have become the target of more cyber-attacks. According to McLeod and Dolezel (2018) data breaches in hospitals have increased from only 18 incidents during the last quarter of 2009 to 351 in the first quarter of 2017 (p.57). In eight years that is an increase of 333 incidents. In any medical facility, the protection of patient information is of the utmost importance. In the United States, the laws that are in place are very strict about the protection of patient information. Loss of information can lead to many penalties towards a medical facility. Should a medical facility, such as a hospital or pharmacy be attacked and the information compromised, that will put the patients at risk. Organizations can face

DOI: 10.4018/978-1-7998-5351-0.ch076

costly fines from the breach of patient information. Securing this information is very difficult as much of the information is in transit and that makes it vulnerable. What then is a solution that can be implemented to protect this information? Blockchain can be a help to the medical community when it comes to protecting patient information. With the problems that hospitals face a solution needs to be brought about that will help the protection of patient information. Blockchain can serve as the very real solution to these problems. But to understand why Blockchain is the solution, managers must first understand what Blockchain is. The Blockchain is the technology behind the cryptocurrency Bitcoin. The use of Blockchain in Bitcoin is able to monitor the transactions between users. Use of Blockchain in Bitcoin serves as a security solution but what is Blockchain? Authors Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone (2018) discuss the technology of Blockchain they define Blockchain as:

...immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that community, such that no transaction can be changed once published... (p. iv)

The technology behind Bitcoin would help to monitor the transactions that occur in the medical community. Looking into how the Blockchain technology has been able to ensure the security of Bitcoin will better protect the patient information. With the help of The Blockchain, the number of incidents that occur should reduce. Implementing Blockchain will be a new way to secure patient files and that will deter attackers.

ANALYSIS OF THE PROBLEM

Hospitals and other medical facilities are becoming the target of many more attacks around the world. Patient information is a rich source of information. Without the information, hospitals are unable to function, and they can be closed down completely. HIPAA is the protection that the United States has implemented for patient information. According to the U.S. Department of Health and Human Services (2003), HIPAA was implemented 1996 with the Privacy Rule associated with it being revised and ready for implementation in August of 2002. This new law was to ensure that patients would have more control over their information, and that medical facilities would be held accountable for the information (pp.3). Should a hospital or medical facility be compromised they could face detrimental fines. McLeod and Dolezel (2018) mention one instance at the New York Presbyterian Hospital being fined 3.3 million dollars after 6800 patients' information was disclosed over the Internet due to "improperly configured web servers" and "lax policies for granting database access," (pp. 57). Here we can see the consequences of breaches of patient information in the United States and how rigorously this is monitored. In this particular case, the lack of updated protocols and technologies was the defining factor for this information being compromised.

The size of a hospital will affect the data breaches that occur. McLeod and Dolezel (2018) state that "Healthcare facilities should be aware that as they grow, they become more of a target and are more likely to be breached," (pp.68). With the growth of the medical facilities, the security of the information has to be evaluated and upgraded if needed Looking at the example of the New York Presbyterian Hospital, the breach was due to the outdated technology and lack of procedures for the patient information. Making

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/blockchain-and-the-protection-of-patient-information-in-line-with-hipaa/268666

Related Content

A Quantum Key Distribution Technique Using Quantum Cryptography

Meenakshi Sharma and Sonia Thind (2021). *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government* (pp. 263-271).

www.irma-international.org/chapter/a-quantum-key-distribution-technique-using-quantum-cryptography/268604

Mitigating the Spread of COVID-19 Using Internet of Things: A Holistic Approach

M. N. Suma and Rajanikanth Kashi Nagaraj (2023). *Contemporary Applications of Data Fusion for Advanced Healthcare Informatics* (pp. 215-237).

www.irma-international.org/chapter/mitigating-the-spread-of-covid-19-using-internet-of-things/327721

Energy-Efficient IoT-Based Wireless Sensor Network Framework for Detecting Symptomatic and Asymptomatic COVID-19 Patients Using a Fuzzy Logic Approach

Charles Rajesh Kumar J., Mary Arunsi B. and M. A. Majid (2023). *Contemporary Applications of Data Fusion for Advanced Healthcare Informatics* (pp. 25-51).

www.irma-international.org/chapter/energy-efficient-iot-based-wireless-sensor-network-framework-for-detecting-symptomatic-and-asymptomatic-covid-19-patients-using-a-fuzzy-logic-approach/327714

Lightweight Key Management for Adaptive Addressing in Next Generation Internet

Vinod Vijaykumar Kimbahun, Arvind V. Deshpande and Parikshit Narendra Mahalle (2021). *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government* (pp. 1890-1914).

www.irma-international.org/chapter/lightweight-key-management-for-adaptive-addressing-in-next-generation-internet/268696

Identification of Student Groups for Smart Tutoring and Collaborative Learning Based on Online Activities Using Neural Networks

D. Kavitha, D. Anitha and C. Jeyamala (2023). *Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies* (pp. 120-140).

www.irma-international.org/chapter/identification-of-student-groups-for-smart-tutoring-and-collaborative-learning-based-on-online-activities-using-neural-networks/331007