Undetectable Data Breach in IoT: Healthcare Data at Risk

Sophia Moganedi

CSIR, Pretoria, South Africa

SMoganedi@csir.co.za

Abstract: The introduction of Internet of Things (IoT has revolutionized the healthcare sector through the digitalization with an enormous amount of patient data that is collected, processed, stored and shared amongst different healthcare stakeholders. The IoT has improved the healthcare service delivery, thus allowing remote patient monitoring, early diagnosis, reduction of medical errors and effective decision making through the data generated by these IoT devices on a real-time basis. Although the IoT has shown a positive transformation in the healthcare sector, a number of challenges are presented, given that the health data is sensitive and its privacy should be preserved. The healthcare sector has become a target of attacks because of the amount of sensitive and personal data that is being collected and shared by these IoT devices. As a result, the healthcare sector has been experiencing major data breaches. Therefore, this paper aims to investigate the root cause of data breaches in the healthcare sector. Secondly, investigate the limitations of the IoT devices in detecting data breaches. Thirdly, investigate the limitation of the security and privacy methods that are used in the healthcare sector to secure the healthcare data and preserve its privacy. Lastly, investigate security measure that can be put in place for data breach detection in the healthcare sector. The final outcome of this paper will be to make security and privacy recommendations that can be used to mitigate or reduce the frequency of data breaches in the healthcare sector.

Keywords: Internet of Things, Security, Privacy, Healthcare, Data Breach

1. Introduction

The Internet of Things (IoT) in the healthcare ecosystems are based on a network of devices that are embedded with sensors and connect directly with each other to gather, process and share vital data. The explosion of the IoT and its ability to provide real-time monitoring and expedited access to care is one of the driving factors for its adoption in the healthcare sector (Patil & Seshadri 2014). As a result, the reliance on the IoT in the healthcare sector is increasing by the day to improve access to the healthcare services, increase the quality and most importantly reducing the costs (Niewolny n.d.). Furthermore, the IoT devices enable the medical professional monitor patients remotely and make recommendations remotely (Kulkarni & Sathe 2014), while frequent visits to the healthcare facilities for check-ups are been reduced. These devices can be more beneficial for hospitalized patients whose physiological status requires constant close attention. (Kulkarni & Sathe 2014) . The revolution in the healthcare data size is a challenges as it is no longer about the amount of data that is been collect, but the speed at which the data is generated and a complex varieties of data types (Youssef 2014). These IoT devices are becoming smaller and smaller with computer capabilities to collect an enormous real-time data, processing, storing and sharing this data. Although the IoT is designed to simply gather an enormous amount of data and exchange with other devices, however the underlying infrastructure is very complex (Fink et al. 2015). Despite all the benefits that are brought by the existence of the IoT in the healthcare sector, comes challenges of data breach. The increasingly invisible, dense and pervasive collection, processing and dissemination of data in the midst of people's private lives gives rise to a serious privacy concerns (JH Ziegeldorf, OG Morchon 2014).

2. Healthcare Data

Traditionally, healthcare data in healthcare sectors were paper-based and stand-alone systems that did not utilize digital technologies, if additional information or data analysis was required, this then meant that more man-power was required (Weng et al. 2016; Raghupathi & Raghupathi 2014). With the increasing use of the IoT in the healthcare sector, data has become digital resulting in the concept called electronic health records. The healthcare data that is collected and stored by the healthcare sector, which is known as health records is extensive and such data include sensitive personal data or personally identifiable information (PII) such as medication, illnesses, medical records and history, sexual information, biometric information, hospitalization, laboratory tests and other sensitive information that can be used to identify and individual (Kierkegaard 2012). The healthcare data that is collected is often transmitted to the cloud storage for long-term storage purpose and also for healthcare providers to be able to access that real-time information. The challenges arise, when

unauthorized party access such data for malicious purposes. Healthcare data shows a state of an individual's medical condition at a particular time. This data is then used to make medical-related decision and plan for treatment.

3. Healthcare Data Breach

Data breaches in healthcare represent a significant risk to the healthcare sector by putting patients at risk and possible deaths (Agaku et al. 2013). The access of the patient information by unauthorised party, identity theft, health insurance frauds and deaths may be the outcome of such activity (Johnson & Willey 2011). Furthermore, it may take years to correct such activities (Delgado 2011). Calculating the value of healthcare information in general is difficult, furthermore, calculating the effect of a potential loss of the healthcare data from a security breach is much more difficult (Huston 2001). Given the series medical data breaches and the lack of public trust , some countries have enacted laws requiring safeguards to be put in place to protect the security and confidentiality of the healthcare data as it is shared electronically, while giving patients some important rights to monitor their healthcare records and receive notification for loss and unauthorized acquisition of their health data (Kierkegaard 2012). Most data breaches are due to unauthorized data access by an insider of an organization, while others breaches are due to incorrectly configured healthcare systems (Lechler et al. 2011). Data breaches have been tracked by the Privacy Rights Clearinghouse since 2005 and has reported in October 2012 that more than 563 million records have been leaked (Wikina 2014). Failed security has resulted in massive data breach that led to the loss or compromise of millions of personally identifiable healthcare records (Thomson 2013). Historically, the security of information systems in general has not been seriously considered in many instances until a breach has occurred (Huston 2001). Healthcare information is sensitive and there is no way to withdraw the information about patient(s) once the information is exposed and resulting damage is done to that patient (Li 2014). Data breach in general result from different activities. The study by (Maksimović et al. n.d.) Present healthcare data breach types as follows:

- Theft
- Unauthorized access and disclosure
- IoT device loss
- System hacking and IT incidents
- Improper disposal of healthcare information

Healthcare data can be breached in various ways. However, regardless of how the data was breached, consequences are still harmful to the patients' whose information has been exposed. The IoT devices are becoming smaller and smaller by the day. Although, the purpose of this interconnected devices is simply to collect patient information, it becomes a challenge and a security concern when these devices cannot detect data breaches or any malicious activities that are performed on them.

4. Healthcare Data Protection Laws

It was not until 1996 with the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPPA) that medical information was made and integral part of privacy concerns requiring protection of healthcare data (Delgado 2011). Most healthcare centres are certified with HIPPA certification, however it is not a guarantee that patient records is secure and its privacy will be preserved (Patil & Seshadri 2014). The HIPPA act provides a framework of how healthcare entities will maintain, transmit and protect electronic healthcare data (Huston 2001). Furthermore, provide a set of rules and regulations, requiring that patients be informed of their privacy rights , that uses the protected health information not needed for treatment, payment or operations be limited and other consumers who are covered by entities (Kahn & Sheshadri 2008).However, the regulatory mandates and public concerns have dramatically increased the pressure for healthcare sectors to secure patient data and comply with these regulations (Kwon & Johnson 2014).

The compliance of the healthcare data protection legislations such as HIPAA, focus on providing a set security and privacy rules which do not focus on the implementation of the actual security to preserve the privacy of the stored healthcare data. HIPPA, has no control of how healthcare providers access and shared the healthcare data. It is rather the responsibility of the healthcare providers to ensure that they comply with the requirement of this legislation. One of the ways that data breaches can be reduced in healthcare sector is to understand the security behaviour and system users' compliance behaviour (Ayyagari 2017).

5. Healthcare Data Protection

Healthcare data is accessed by different stakeholder from healthcare sectors. Although, it is the responsibility of the healthcare providers to ensure that the IoT infrastructure that is used in the healthcare facilities are covered by the HIPPA and also comply with this act in term of protecting patients' healthcare records. In the IoT domain, patients also have a role to play in ensuring that their healthcare records are kept private and secure. This will then mean that patients need to ensure that they understand the IoT devices they use and what healthcare data is being collected by these devices and what information is been stored by these devices. Understanding the actual devices will enable the patients to be able to recognize an unusual activity besides the physical loss of their devices, should the device be hacked and information accessed from the storage of the actual device.

6. Conclusion

The Internet of Things has revolutionized the healthcare sector by enabling healthcare providers or professionals to monitor their patients remotely, make medical recommendation remotely. This kind of revolution benefits patients with chronic illnesses but cannot afford the healthcare services or rather cannot afford the frequent visits to the healthcare facilities. IoT has enabled the healthcare sector to have access to a real-time data, which is collected through the sensors embedded within the IoT devices. This accessing of real-time data allows healthcare providers to be able to make effective decisions, early medical diagnosis, plan treatment and monitor patients remotely. The data that is collected is extensive and it is regarded as sensitive and personal. Therefore, privacy of this data need to be properly preserved in order to prevent unauthorized parties from accessing the data , which might result is identity theft, medical insurance frauds and even deaths. HIPPA and other healthcare legislations that aim to provide set of rules on the protection of healthcare data are not enough to ensure that the privacy of healthcare data is preserved.

7. References

Agaku, I.T. et al., 2013. Concern about security and privacy , and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association,*, pp.374–378.

Ayyagari, R., 2017. An Exploratory Analysis of Data Breaches from 2005-2011 : Trends and Insights. , 6548(October).

Delgado, M., 2011. The Evolution of Health Care IT : Are Current U . S . Privacy Policies Ready for the Clouds ? In *Services (SERVICES), 2011 IEEE World Congress on*.

Fink, G.A. et al., 2015. Security and Privacy Grand Challenges for the Internet of things. In *Collaboration Technologies and Systems (CTS), 2015 International Conference on*. pp. 27–34.

Huston, T., 2001. SECURITY ISSUES FOR IMPLEMENTATION OF E-MEDICAL RECORDS. *COMMUNICATIONS OF THE ACM*, 44(9), pp.89–94.

JH Ziegeldorf, OG Morchon, K.W., 2014. Privacy in the Internet of Things: threats and challenges. *International Journal of Applied Engineering Research*, 9(22), pp.5968–5974.

Johnson, E.M. & Willey, N.D., 2011. Usability Failures and Healthcare Data Hemorrhages. In *COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES*. pp. 35–42.

Kahn, S. & Sheshadri, V., 2008. Privacy and Security in a Digital Environment. In IEEE.

Kierkegaard, P., 2012. Medical data breaches : Notification delayed is notification denied. *Computer Law & Security Review*, 28(2), pp.163–183.

Kulkarni, A. & Sathe, S., 2014. Healthcare applications of the Internet of Things : A Review. *International Journal of Computer Science and Information Technologies*, 5(5), pp.6229–6232.

Kwon, J. & Johnson, M.E., 2014. Health-Care Security Strategies for Data Protection and Regulatory Compliance Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems*, 30(2), pp.41–66.

Lechler, T., Wetzel, S. & Jankowski, R., 2011. Identifying and Evaluating the Threat of Transitive Information

Leakage in Healthcare Systems. In *Proceedings of the 44th Hawaii International Conference on System Sciences*. pp. 1–10.

Li, J., 2014. *Data Protection in Healthcare Social Networks*, Texas.

Maksimović, M., Vujovi, V. & Perišić, B., A Custom Internet of Things Healthcare System.

Niewolny, D., How The Internet Of Things Is Revolutionizing Healthcare.

Patil, H.K. & Seshadri, R., 2014. Big data security and privacy issues in healthcare. In *Big Data (BigData Congress), 2014 IEEE International Congress on*. Anchorage, AK, USA: IEEE, pp. 775–778.

Raghupathi, W. & Raghupathi, V., 2014. Big data analytics in healthcare : promise and potential. *health information, science and systems*, 2(3), pp.1–10.

Thomson, L.L., 2013. Health Care Data Breaches and Information Security Addressing Threats and Risks to Patient Data. In pp. 2005–2013.

Weng, S. et al., 2016. Cloud Image Data Center for Healthcare Network in Taiwan. , 40.

Wikina, S.B., 2014. What Caused the Breach ? An Examination of Use of Information Technology and Health Data Breaches. *Online Research Journal: Perspective in Health information Management*, 11.

Youssef, A.E., 2014. A F RAMEWORK F OR S ECURE H EALTHCARE S YSTEMS B ASED O N B IG D ATA A NALYTICS I N M OBILE C LOUD. *International Journal of Ambient Systems and Applications (IJASA)*, 2(2), pp.1–11.