International Journal of Engineering Research and Applications *www.ijera.com*
ISSN: 2248-9622, pp. 55-57

RESEARCH ARTICLE OPEN ACCESS

A framework to suggest critical methods for solving IoT security problems in healthcare

Omar Yahye Adam, S B Goyal
City University, Malaysia

ABSTRACT
Internet of things revolutionizing many aspects of our life, including the healthcare environment. As patients become more connected and generate more data, clinicians can identify and address their needs more efficiently. Until recently, access to the internet was limited via devices like desktop, tablet, or smartphone but now with the internet of things (IoT), practically all devices and objects can be connected to the internet and monitored remotely. Since healthcare information and data are highly confidential, it is essential to ensure that healthcare networks and data generated by IoT are secure. However, many of the (IoT) healthcare devices have poor security, and cybercriminals are taking advantage of it by gaining access to all devices that are connected to them. Thus, this study aims to investigate IoT data protection with particular attention to the healthcare environment and medical devices. The study will use quantitative data techniques to investigate the main aim. With the help of results pertaining to the study, a framework or critical methods will be suggested to solve IoT security problems in the healthcare industry.
Keywords: IoT, Healthcare, Cybercriminals, Data Protection

I. INTRODUCTION

Internet of things or (IoT) is a giant network with connected devices, these devices gather and share data about how they are used and the environment in which they are operated. It's all done using sensors; sensors are embedded in every physical device. It can be a mobile phone, electrical appliances, barcode sensors, traffic lights, and almost everything you encounter in day-to-day life (Riazul Islam, S. M., Daehan Kwak, Humaun Kabir, M., Hossain, M., & Kyung-Sup Kwak., 2015). When IoT devices share data over the cloud and analyze it, they can transform our businesses, stamina, and world in countless ways (Atlam, H. F., Walters, R. J., & Wills, G. B., 2018). Besides the fact that the most attractive application areas for the IoT are healthcare and hospitality but, as we gather more connected things, we expose patients' sensitive data and put it at more risk of serious security incidence and more significant impact on health. Comprehensive studies have been made to the IoT security issues; however, little research has focused on IoT security in healthcare (E. Park, J. H. Kim, H. S. Nam, and H. J. Chang., 2018). This paper aims to explore the impact of IoT in healthcare, security issues, and solutions.

II. REVIEW OF THE LITERATURE

The advantages of IoT and the data that it produces are going to be enormous. HP security research evaluated and found that 70% of what we call IoT devices are vulnerable to an attack. Many of today's lifesaving devices are connected to the internet, and because of that are at riskof being hacked. We have to find a way to do security differently.

A security vulnerability has most often been seen when more devices are connected to the internet. Mirjana Maksimović (2016) mentions that if more intelligent devices are linked to the internet, the potential privacy implication and a general false sense of security associated with weak key management and data compromise become critical. Mirjana also addresses that the rapid development of IoT healthcare contains the risk of security and privacy. Thus, the internet of things won't be realized within the healthcare industry unless data integrity and security are designed and built into the IoT's very foundations.

From storage solution to accessing data remotely, IoT and cloud computing build an integration but, Baker, S. B., Xiang, W., & Atkinson, I. (2017) states that the security is a vital issuein cloud-based systems. The study has noticed the importance of authorized access parties, including doctors, nurses, specialists, and other emergency services. Moreover, no attention has been paid to the advance methods of solving IoT security issue.

Many different approaches have been proposed to solve the smart hospital security issue by European Union Agency for Network and Information Security (ENISA), 2016. The study also

makes further recommendations to enhance the level of information security in smart hospitals. However, no attention has been paid to block-chain technology. *In this paper, we make a further contribution by showing that block-chain technology is considered a possible solution to improve the level of security in IoT healthcare devices.*

Today we're in a situation where every IoT device or smart device comes with its own interface, app, topological structure, security model and cryptographic techniques. In the context of use heterogeneous devices in IoT-based healthcare network, significant security and data privacy will be an issue.Nazir, S., Ali, Y., Ullah, N., & García-Magariño, I. (2019).

III. PROBLEM STATEMENT AND HYPOTHESIS OF THE STUDY

The study's main aim is to evaluate whether there is a need for the security of IoT devices in the healthcare sector. Besides this, the study's central ideal is to focus on IoT devices used in the healthcare sector, e.g. blood pressure and heart rate monitoring cuffs, glucometer, etc. Moreover, the study will also try to justify the objectives mentioned below:

- To understand the relationship between IoT and healthcare services.
- To evaluate the need for IoT devices in the healthcare sector.
- To analyze whether there is a need for the security of IoT devices in the healthcare sector.
- To determine the impact of IoT devices on the growth of the healthcare sector.
- To secure data transfer generated by IoT healthcare devices from different kinds of attacks.
- To use blockchain technology for solving the IoT's most critical security-related problems.

IV. RESEARCH METHODOLOGY (SOLUTION APPROACH)

Research Methodology is an essential component of the research framework as it acts as a guiding tool for the different stages of a study. The current study will utilize an ***interpretivist research philosophy***. This is because it propagates the idea that truth, belief, and knowledge can be objective in nature. Further, the study will utilize a ***quantitative research approach*** to gaining objective data. Moreover, a ***descriptive research design*** will be implemented. Descriptive research design, as opposed to other designs, is more compatible to delineate the available set of information based on the sequence in which it occurs independently in nature. Finally, the study will use a deductive reasoning approach. The inductive reasoning approach follows a top to bottom approach wherein a more precise conclusion is reached from a generalized phenomenon. Followed by this, the study will use a ***primary data collection*** method. Through this primary source, the data collected will be in the quantitative form which will justify the aims and objectives of the study. The main sources of data will be taken from healthcare workers and hospital management staff where IoT devices are used for security purposes. For this purpose, questionnaires will be developed that will be distributed among the healthcare working staff and hospital management using IoT for security purposes. With the help of convenience sampling, the respondents for the study will be selected and the process of data collection will proceed. Moreover, the collected data will be analyzed with software analysis techniques or content analysis depending on the data collected. Later, with help of the descriptive analysis technique, the inferences of the results will be elaborated with supporting literature justifying the aims and objectives of the study. Besides this, secondary data will be used from the existing research available to justify and support the current aims and objectives of the study.

V. RESEARCH SCHEDULE

A definite research schedule helps in order to move ahead with the research process in a standard and definite process without missing any step of research. The components required to complete this research are as follows:

a) Formulate Research Strategy, Research Design, and Select Methods
b) Literature Review
c) Data Collection and data Analysis
d) Write dissertation report

VI. EXPECTED IMPACT

Proposed work will build the confidence of the patient about their data security. It will generate a new revolution among health industry to get customer satisfaction. In the healthcare industry, patient and customer satisfaction and customer data play an essential role in retaining the customer and getting a customer's recommendation.

VII. CONCLUSIONS

This health care industry is prone to many kinds of risk. The most dominant of which is the risk associated with the privacy of the data provided by the people. Thus, it is the duty of the hospitals to search for options that come with services that offer a hundred percent security. The hospitals need to implement a complete risk management system. This study is directed towards searching for ways

that could help this industry be free of the risk that is associated with IoT services.

REFERENCES

[1]. Atlam, Hany F., et al. "XACML for Building Access Control Policies in Internet of Things." *IoTBDS*. 2018.

[2]. Atlam, Hany F., Robert J. Walters, and Gary B. Wills. "Internet of nano things: Security issues and applications." *Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing*. 2018.

[3]. Atlam, Hany F., Robert J. Walters, and Gary B. Wills. "Intelligence of things: opportunities & challenges." *2018 3rd Cloudification of the Internet of Things (CIoT)*. IEEE, 2018.

[4]. Atlam, Hany F., Robert J. Walters, and Gary B. Wills. "Fog computing and the internet of things: a review." *big data and cognitive computing* 2.2 (2018): 10.

[5]. Cottrill, Caitlin D., et al. "Sensing the City: Designing for Privacy and Trust in the Internet of Things." *Sustainable Cities and Society* 63 (2020): 102453.

[6]. Islam, SM Riazul, et al. "The internet of things for health care: a comprehensive survey." *IEEE access* 3 (2015): 678-708.

[7]. Maksimović, Mirjana, et al. "Do It Yourself Solution of Internet of Things Healthcare System: Measuring Body Parameters and Environmental Parameters Affecting Health." *Journal of Information Systems Engineering & Management*, vol. 1, no. 1, 2016. *Crossref*, doi:10.20897/lectito.201607.

[8]. Baker, Stephanie B., et al. "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities." *IEEE Access*, vol. 5, 2017, pp. 26521–44. *Crossref*, doi:10.1109/access.2017.2775180.

[9]. Nazir, Shah, et al. "Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review." *Wireless Communications and Mobile Computing*, vol. 2019, 2019, pp. 1–20. *Crossref*, doi:10.1155/2019/5931315.

[10]. Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015.

[11]. Mavropoulos, Orestis, et al. "Apparatus: A framework for security analysis in internet of things systems." *Ad Hoc Networks* 92 (2019): 101743.

[12]. Park, Eunjeong, et al. "Requirement analysis and implementation of smart emergency medical services." *IEEE Access* 6 (2018): 42022-42029.

[13]. Patil, Harsh Kupwade, and Ravi Seshadri. "Big data security and privacy issues in healthcare." *2014 IEEE international congress on big data*. IEEE, 2014.

[14]. Sicari, S., et al. "A policy enforcement framework for Internet of Things applications in the smart health." *Smart Health* 3 (2017): 39-74.

[15]. Tarouco, Liane Margarida Rockenbach, et al. "Internet of Things in healthcare: Interoperatibility and security issues." *2012 IEEE international conference on communications (ICC)*. IEEE, 2012.

[16]. Tehranipoor, Fatemeh, et al. "Investigation of the Internet of Things in Its Application to Low-Cost Authentication Within Healthcare." *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI). Poster*. 2017.

[17]. Tehranipoor, Fatemeh, et al. "Exploring methods of authentication for the internet of things." *Internet of Things*. Chapman and Hall/CRC, 2017. 71-90.

[18]. Wortman, Paul A., et al. "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain." *2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*. IEEE, 2017.

[19]. Yousuf, T., Mahmoud, R., Aloul, F., &Zualkernan, I. (2015). Internet of things (IoT) security: current status, challenges and countermeasures. *International Journal for Information Security Research (IJISR)*, *5*(4), 608-616.