Challenges Of Security And Privacy With IoT In Healthcare: An Overview

[1]Chukwu N. P., [2]Edeagu S. O., [2]Chijindu V. C., [2]Eneh J. N., [2]Ndu I. O., [2]Ahaneku M. A., and [2]Iloanusi O. N.

Department of Computer Engineering, Federal Polytechnic Ekowe, Bayelsa State.
Department of Electronic Engineering, University of Nigeria, Nsukka, Enugu State. Nigeria
chukwuemekapaul98@federalpolyekowe.edu.ng, samuel.edeagu@unn.edu.ng, vincent.chijindu@unn.edu.ng, nnenna.eneh@unn.edu.ng, ijeoma.okeke@unn.edu.ng, mamilus.ahaneku@unn.edu.ng, ogechukwu.iloanusi@unn.edu.ng

Abstract- The Internet of Things (IoT) have greatly improved our lives by transforming ordinary devices in our vicinities into smart and intelligent devices that are capable of sensing the activities within the environment, interact with other smart devices and respond reasonably to the changes in their immediate environment. In healthcare, specifically, IoT technologies have assisted immensely in the monitoring, observation and timely decision-making in the treatment processes of patients. Nevertheless, the improvements and conveniences brought by the IoT also come along with huge security and privacy issues. If these security breaches are ignored, they could pose serious unpalatable effects on the different aspects of our lives including fatal exposures of patients' vital data. This paper sheds the light on some of the security and privacy issues that the IoT in healthcare paradigm is exposed to, as well as some appropriate mitigating countermeasures.

Keywords: Security*; Privacy; Near Field Communication (NFC); IoT; Healthcare*

INTRODUCTION

The Internet of Things (IoT) is the physical and logical interconnection of all kinds of smart devices to a dedicated cloud network with the intent of achieving reliable consistency in smart coordination, intelligent monitoring and scalable operational administration [1]. These devices are made up of identifiers, sensors, health equipment, as well as software applications, which are connected together via the internet and therefore have the capacity to identify the source, collect, exchange and manage data. IoT devices have the ability of being remotely operated or controlled across existing network infrastructure. This creates an opportunity for seamless scalability, vis-à-vis, more direct integration of devices into computer-based systems, which results in improved efficiency, and accuracy. In the long run, it provides an economic benefit to the users.

It is on record that Symantec (an internet security organization) blocked more than 3.7 million cyber-attack attempts in 2018, with more than 1 million of those blocks occurring in the last two months of the year alone [2], and it has also been projected that the cost of cyber-attacks in such setting could reach about two Trillion USD by 2020 [3].

Moreover, IoT, no doubt, has become deeply rooted in the healthcare sector, and are most times referred to as "the Internet of Medical Things" (IoMT) [4]. These interconnected smart devices help in great measures to administer medical activities, outdoor healthcare, regular monitoring, careful observation as well as timely diagnosis of patients. Due to the importance and acceptability of IoT in healthcare and its services, government of nations as well as global institutions have been investing heavily on them; as a matter of fact, the number of connected devices around the world is projected to dramatically increase from 20.35 billion in 2017 to 75.44 billion in 2025 [5].

Spending on the Internet of things (IoT) is expected to soar from $698.6 billion in 2015 to nearly $1.3 trillion in 2019, according to an International Data Corporation (IDC) report [5]. Organizations in all sectors are upgrading their services through the use of IoT devices; for instance, smart televisions and Personal digital assistants (PDAs) in conference halls, intelligent machine-controlled sensors in industries, portable wearable devices in health institutions, etc. These smart IoT devices must be deployed with adequate security; otherwise, the organizations involved would be at huge risk.

The bitter result of an unprotected or compromised IoT cloud network can be fatally dangerous. IoT devices experience an average of 5,200 attacks per month thereby causing global businesses to lose so much revenue in the tune of over $500 billion yearly [2][6]. Moreover, it has been noted that medical devices are more susceptible to cyber-attacks than ever before. These attacks are not only financially injurious, but life threatening. From research, it was revealed that communications to and from medical equipment, example, pacemakers could be intercepted or altered, potentially causing injuries or even death of patients [7].

While IoT devices are gaining reputation in several organizations, healthcare is at the pinnacle, on the catalog of institutions at risk [8] of cyber-attacks. This is as a result of the quantity and the sensitive nature of personal information collated from Electronic Personal Records (EPR) [8]. To mitigate this challenge, stakeholders in the healthcare industry are consulting with cyber security experts to win the war of cybercrimes, which have the potential of exposing the lives of patients to great risks.

LITERATURE REVIEW

This section presents the review of related materials in challenges of security and privacy with IoT devices in Healthcare in general. The review surveys the various works done by researchers and tries to draw strength and weaknesses from them.

The security vulnerability inherent in an automated healthcare monitoring system for the elderly was discussed in [9]. After analyzing the risks involved, the authors identified the security measures that should be investigated in different monitoring systems. Some of the security attacks analyzed include, Man in the middle (MITM) attacks, the threats posed by Denial of Service (DOS) attacks, and how traffic analysis can occur. Others include Malware and social Engineering attacks. According to the authors, while MITM attack exploits a vulnerability in the key distribution of ZigBee network protocol; *DOS* uses a loop hole in ZigBee's association method for new devices connecting to the network. In addition, a cyber-attacker, could weaken the network by infusing a malicious software (malware) into the devices. In Social Engineering attacks, the human is the target and not the automated system.

To mitigate these attacks, the authors proposed some counter measures, which includes using Public Key Encryption (PKE) instead of symmetric encryption to foil MITM attack. A preventive measure for DOS problem is by filtering the incoming data traffic. Moreover, to guard against Malware, a firewall and a strong security on the wireless network would be a countermeasure to this. A system update is a good defense for social engineering attacks.

The risks associated with the Near Field Communication (an IoT technology widely used as a result of its short range frequencies) were discussed in [10]. These risks include but are not limited to eavesdropping, spoofing, phishing, relay attacks, data corruption, data modification and DOS attack. According to the authors, a cyber-criminal can eavesdrop on an IoT network, if there was no adequate secure protection during data transmission. Spoofing is made possible by compromising the contents of the NFC tag. The attacker could achieve this

by supplying fake email, domain name or even Universal Resource Locator (URL), thereby tricking the users into disclosing their access details.

Using the risk assessment method, the authors evaluated the NFC security risks and concluded that the highest security issue associated with NFC are data corruption and DOS attack.

However, they proposed an architectural guideline of solution through the use of MIDAS system to secure the NFC application; insisting that from the findings in the research, ECC and AES process are the most viable strategy to implement a reliable pathway in the Near Field Communication protocol. The advantages as well as the importance of IoT in healthcare were also enumerated in [10]. However, they were quick to deduce the vulnerability and security risks associated with IoT devices mainly as a result of interconnecting the devices from different vendors to very poorly secured web-enabled IT systems. Some possible risks include, but are not limited to unauthorized access that can lead to misuse of personal information; maliciously enhancing cyber-attacks on other systems; creating risks to personal safety; and privacy risks that arise from the collection of personal information, locations and physical conditions.

The authors proposed some security measures for the IoT in healthcare devices which are that security measures should be incorporated into the design of the IoT device, this includes analyzing the level risks involved before dispatching them to the end users. Again, to make sure that authentication is properly followed, device access is limited, firmware being sent to the device is verified, and device-to-device communication is monitored. Also, a defense in depth strategy should be implemented, where several layers of security is in place to protect against specific risks. In addition, ensure there are proper access control in place that limit unauthorized access to data, the IoT devices and the networks. In addition, test the security of the IoT device before it is put into production and monitor the security of the device throughout its life cycle. Not forgetting the need to establish culture of security, where the employees are trained to recognize vulnerabilities

Kumar and Patel, [11] surveyed, Internet of Things with architecture and design goals including security and privacy concerns at different layers in IoT. In addition, the authors identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform to improve IoT in years to come.

The concerns of major social implications like privacy and security were discussed in [12]. The authors analyzed the cause and effects of these two issues and maintained that without taking care of these issues, the necessary growth and development will face major obstacles in coming future.

O'Connor et al. [13] argued in their paper that the first phase for universal usability of IoT within the smart health domain is to ensure that the citizens who use this technology are sensitized on the pros and cons so as not to expose themselves to hackers. This paper also proposes some practical approaches which should be taken into cognizance when "designing and developing IoT for data collection and data sharing within the health domain."

The general security architecture of IoT devices were reviewed in [14] and [15] and in-depth analysis of how vulnerable these devices can be when connected to the Internet were conducted.

A system of mapping different applications such as early warning application system, patients' monitoring application system, etcetera, to the four layers of IoT device was

proposed in [16] and [17], thereby creating a huge defensive digital shied within the IoT cloud network.

The work in [18] focusses on security and privacy for low power and lossy networks. He identified the different security attacks on the three phases of the IoT devices vis-à-vis, manufacturing, installation, and operational. He proposed the protection against IoT attacks in different categories, namely, authentication, access control, confidentiality, integrity, and availability.

IoT-based architecture with either a single or multiple central servers that communicates with mobile devices through secured plural networks can be used for population health data capture and public health intervention whilst still maintaining strong privacy and anonymity for all participating individuals [19]. Again, it is worthy of note that, the aspect of public health usage most of the time does not require the same level of precise data that would often be required in other IoT applications [19]. For instance, the exact location and time of a measured sensor value is less important than the aggregate value over a period of time or the trend of change for a mass of people or community.

Summary of the Review

A lot of work has been done by researchers as regards the security and privacy of IoT in healthcare. Four different points were identified which are:

i. The indisputability of the dangers associated with IoT in healthcare

The Internet of Things is a smart technology with great benefits, nonetheless, it exposes industries to harsh cyber threats [20]. For health institutions to actualize the full potential of the IoT, they have to be adequately prepared to protect sensitive information between devices in a network.

ii. The rationale behind IoT security threats

The main reason behind these cyber-attacks is that healthcare institutions have millions of smart devices connected to their network, thereby creating a high probability of security gaps which are attractive targets for cybercriminals [21].

Besides this, Organizations, especially healthcare institutions, could be a bit ignorant of the data-flow as well as the particular location of data from IoT devices and therefore lack the ability to take control it. This huge knowledge gap of data forms a very wide surface for cyber-attacks.

In addition to these, there is proliferation of personal IoT devices, which most times are brought in by patients as well as health workers and inadvertently overlooked by hospital security system. This, no doubt would compromise the security architecture of the organization's IoT network. Suffice to say that healthcare IoT devices contain valuable Patient's Personal Private Health Information (PPPHI), which hackers can exploit for huge profit.

iii. Strategies of security attacks

Only recently, quite a huge number of the major IoT security system breaches have been aided and abated by insiders. From an IoT survey conducted in 2017 by Accenture, "18% of healthcare employees are willing to sell confidential data to unauthorized parties for as little as $500 to $1,000" [22]. It is no doubt, a thriving "business". Apart from PPPHI theft by cyber-criminals, through compromised IoT devices, the organization's network could be attacked through Denial-of-Service Attacks (DoS) and interfering with the physical safety of

the IoT devices, exposing patients' health records and sometimes falsifying their diagnostic data thereby leading to wrong prescription by the healthcare givers [23].

iv. Countermeasures to Security and Privacy issues with IoT in healthcare

To mitigate these security attacks in IoT in healthcare, three main countermeasures can be utilized, namely, Absolute Data Confidentiality (ADC), Dynamic Information-Integrity (DII), and Reliable Authorized-Accessibility (RAA) [20] and [24]. While ADC checkmates the level of information access in the IoT devices; DII guarantees the trustworthiness and accuracy of the data in the IoT devices. On the other hand, RAA ensures authorized and authenticated access to the IoT network and information within the devices [25].

CONCLUSION

The implication of security and privacy with IoT in healthcare has been reviewed in this paper. We stated the major reasons behind these attacks which include, but not limited to security gaps caused by undue multiple connections of smart devices to the healthcare institutions' networks; ignorance on the management of data-flow within IoT devices; rapid increase in the connection of personal IoT devices by unauthorized persons to the network.

In order to alleviate these cybersecurity attacks in IoT in healthcare, we proposed three countermeasures, namely, Absolute Data Confidentiality (ADC), Dynamic Information-Integrity (DII), and Reliable Authorized-Accessibility (RAA). The Internet of Medical Things (IoMT) as its fondly called has come to stay, but the risks and vulnerability of the technology must not be treated with 'kid glove'.

REFERENCES

[1] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare," *EAI Endorsed Trans. Pervasive Heal. Technol.*, vol. 4, no. 14, pp. 1–7, 2018.

[2] Symantec, "Internet Security Threat Report VOLUME 21, February 2019," *Netw. Secur.*, vol. 21, no. February, p. 61, 2019, doi: 10.1016/S1353-4858(05)00194-7.

[3] M. Medwed, "IoT Security Challenges and Ways Forward," p. 2995298, 2016.

[4] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain," *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017, doi: 10.12720/jcm.12.4.240-247.

[5] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, 2019, doi: 10.1109/JIOT.2018.2847733.

[6] N. K. Popli, "ABS International Journal of Management THE HARMFUL EFFECTS OF CYBER CRIME IN BUSINESS AND ECONOMIC SUSTAINABILITY," vol. V, no. I, pp. 74–76.

[7] E. Mcmahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing Medical Device Vulnerabilities on the Internet of Things," pp. 176–178, 2017.

[8] L. E. Branch, L. E. Branch, and W. Virginia, "Cyber Threats and Healthcare Organizations : A Public Health Preparedness Perspective A Public Health Preparedness Perspective Department of Occupational and Environmental Health Sciences," 2018.

[9] D. T. Handler, L. Hauge, A. Spognardi, and N. Dragoni, "Security and privacy issues in healthcare monitoring systems: A case study," *Heal. 2017 - 10th Int. Conf. Heal. Informatics, Proceedings; Part 10th Int. Jt. Conf. Biomed. Eng. Syst. Technol. BIOSTEC 2017*, vol. 5, pp. 383–388, 2017, doi: 10.5220/0006224603830388

[10] M. M. Singh, K. Aina, A. Ku, and R. Hassan, "Near Field Communication (NFC) Technology Security Vulnerabilities and Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures," no. December, 2018, doi: 10.14419/ijet.v7i4.31.23384.

[11] J. S. Kumar and D. R. Patel, "A Survey on the Internet of Things: Security and Privacy Issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014. [12] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, 2012, doi: 10.1007/s10916-010-9449-4.

[12] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, 2012, doi: 10.1007/s10916-010-9449-4.

[13] Y. O'Connor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by Design: Informed Consent and Internet of Things for Smart Health," *Procedia Comput. Sci.*, vol. 113, pp. 653–658, 2017, doi: 10.1016/j.procs.2017.08.329.

[14] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," *Proc. - 2015 IEEE World Congr. Serv. Serv. 2015*, pp. 21–28, 2015, doi: 10.1109/SERVICES.2015.12..

[15] K. K. Patel, S. M. Patel, and P. G. Scholar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 1–10, 2016, doi: 10.4010/2016.1482.

[16] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2018, doi: 10.1016/j.future.2017.04.036.

[17] J. Steward, "Northumbria Research Link," *Nrl.Northumbria.Ac.Uk*, vol. 24, no. August, pp. 23–35, 2002, doi: 10.1108/17410391111097438.

[18] D. P. F. Dr. Ovidu Vermesan, "An Overview of Privacy and Security Issues in the Internet of Things," *River Pulisher Ser. Commun.*, vol. 291, no. July 2012, pp. 1–40, 2015, doi: 10.5480/1536-5026-34.1.63.

[19] R. Steele and A. Clarke, "The Internet of Things and Next-generation Public Health Information Systems," *Commun. Netw.*, vol. 05, no. 03, pp. 4–9, 2013, doi: 10.4236/cn.2013.53b1002.

[20] S. Patients, D. Against, G. Threats, and B. Cybersecurity, "The current threat landscape for the EoT," pp. 1–12, 2020, [Online]. Available: https://global.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-cybersecurity-healthcare.pdf.

[21] https://www.gartner.com/newsroom/id/3165317 [Accessed:17-Jan-2020]

[22] https://hackernoon.com/how-to-secure-healthcare-facilities-against-iot-security-

threats-ab28dd284cac[Accessed:19-Jan-2020]

[23] https://www.gartner.com/newsroom/id/3165317 [Accessed:17-Jan-2020]

[24] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA[Accessed:20-Jan-2020]

[25] https://www.forbes.com/sites/forbestechcouncil/2019/03/01/prognosis-for-health-care-iot-six-predictions-for-2019/#28bee5a1fdd[Accessed:03-Oct-2019]