SECURITY AND PRIVACY OF INTERNET OF MEDICAL THINGS (IOMT) BASED HEALTHCARE APPLICATIONS: A REVIEW

[1]NIPUNI NANAYAKKARA, [2]MALKA N. HALGAMUGE, [3]ALI SYED

[1,3]School of Computing and Mathematics, Charles Sturt University, Melbourne, Victoria 3000, Australia
[2]Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia
E-mail: [1]nipuni.rajaguru@gmail.com, [2]malka.nisha@unimelb.edu.au

Abstract - Recent technological advancements have significantly transformed an individual's perception of the traditional way of carrying out day to day operations. Internet of Things has to be turned out to be a growing trend in various segments in the present world, including the healthcare context. However, this rapid revolution towards IoT has also created several uncertainties and questions over the security of data which is stored in various connected things. With the number of things such as sensors and devices is growing, preserving robust security and privacy of sensitive data becomes more challenging. These security and privacy issues are resulted from deteriorating the effectiveness of Internet of Things (IoT) based healthcare services and adversely impact on individual's sensitive health information. Since data in the healthcare field is critical and sensitive; security and privacy safeguarding of the IoT healthcare paradigm makes matters even more problematic. In order to gain a widespread idea about the risks and threats related to IoT healthcare application, this study reviews a variety of relevant previous publications. The primary goal of this article is to provide insights into multiple sensors devices used in IoT healthcare context and the potential security and privacy issues in different IoT layers. Data are collected from 30 peer-reviewed publications on IoT based healthcare applications published between 2016 and 2018. We have considered numerous threats, attacks, and risks that can affect different layers in IoT based healthcare applications such as (Perception Layer, Network Layer, Middleware, Application Layer, and Business Layer). We have also considered different types of sensor devices which are used in IoT based healthcare applications. For the analysis, we categorize the sensor devices as wearable, implantable, ambient and stationery. Further, we analyze the proposed solutions stated in previous articles to obtain out the most recommended solutions that can mitigate threats and risks in IoT based healthcare application context. Our results show that the network layer is the most vulnerable layer to numerous security and privacy threats and attacks. And the applications layer is the second most vulnerable layer, and wearable sensors were utilized in the majority of IoT based healthcare applications. In addition, China and the USA have the most significant focus on security and privacy of IoMT based healthcare applications. This study intends to enhance awareness among application designers, developers and users such as healthcare professionals and patients by allowing them to identify and quantify potential IoT healthcare application-related threats and risks.

Keywords - Internet of Things (IoT), Sensors, Threats, IoT Layers, Encryption, Cryptography

I. INTRODUCTION

Health is one of the primary human needs for a better life. Improving healthcare services can enhance the quality of people's lives in any society. In recent time, many healthcare providers have adopted IoT technologies to improve treatment processes, enhance communication between parties, reduce errors during the processes, manage drugs, diseases, lower costs and ultimately improve the efficiency and effectiveness of the healthcare processes (Alsubaei et al., 2017). According to the Statista (The Statistics Portal), the number of IoT units adopted in the healthcare sector in European Union (EU) will increase up to 25.8 million units by 2025 (Statista, 2018).

However, the number of connected devices and the massive amount of sensitive data collected by those devices have raised new challenges in terms of data security and privacy. Along with the rapid evolution of IoT, cyber-attacks have also improved, and it has introduced a new attack and threat avenue to the entire healthcare industry.According to the Department of Health and Human Services Office for Civil Rights of United States, the number of reported privacy and security breaches in the healthcare sector continue to increase at about 10% each year since 2010(U.S. Department of Health and Human Services, 2018).

Many studies have investigated the various privacy and security concernsand system vulnerabilities of IoT in cloud and fog computing contexts related to IoT based healthcare applications (Ida et al.,2016; Yang et al.,2017; Rauf et al., 2018; Amaraweeraet al., 2019; Chandrasiri et al.,2019; Ekanayake et al., 2018). In contrast, Alsubaei et al., (2017) have reviewed detailed security and privacy taxonomy of Internet of Medical Things (IoMT). Their research has identified and classified the potential security and privacy risks related to IoMT on IoT layer, Impact, Intruder Type, Attack Method, Compromise Level, CIA Compromise, Attack Level, Attack Origin and Attack Difficulty (Alsubaei et al., 2017). Further, Zhou et al., (2018) have explored 8 IoT features i.e. Interdependence, Diversity, Constrained, Myriad, Unattended, Intimacy, Mobile and Ubiquitous and privacy and security effect for each feature (Zhou et al., 2018.

In this study, we have found that the IoT healthcare applications consist of different types of layers and different sensor devices. Some authors have identified and analyzed security and privacy issues

based on four different layers in the IoT architecture, namely, Network Layer, Perception Layer, Application Layer, and Transport Layer (Yang et al.,2017; Alsubaei et al., 2017; Rauf et al., 2018). Further, Qi et al., (2017) have stated those layers as Network Layer, Sensing Layer, Application Layer and Data Processing Layer. (Qi et al., 2017). In contrast, Ifrim et al., (2017) have identified three different layers, namely Sensing Layer, Network Layer and Application Layer. (Ifrim et al., 2017).

Further, various authors have identified different types of sensors in IoT healthcare applications. Such as Ifrim et al., (2017) have classified them into two categories, namely wearable and implantable devices, based on how the devices are connected. In addition to that Qi et al., (2017) have categorized them as wearable sensors and ambient sensors. Furthermore, Alsubaei et al.,(2017) have stated another broader classification on sensors, namely wearable, implantable, ambient and stationary (Alsubaei et al., 2017).

During this study, we have identified that many researchers have recommended various privacy and security preserving approaches to counter identified issues in IoT healthcare paradigm. These recommendations are mainly included with implementing password strengthen mechanism to prevent unauthorize access to the IoT based healthcare applications (He et al., 2018),strong general security standards and policies that can ensure privacy and security in IoT devices (Yang et al., 2017) and a risk-based trust management model for handling different security and privacy threats and attacks in an IoT based healthcare environment (Rauf et al., 2018). Further, El Zouka (2017) presents a secured lightweight user authentication scheme which can protect sensitive health data exchange in the cloud platform (El Zouka, 2017). In addition to that, to strengthen the physical security of IoT sensor devices, some of the authors have proposed lightweight privacy-preserving authentication protocols. These solutions have developed by considering the ideal physically unclonable functions (Gope et al., 2018; Gope & Sikdar., 2018).

However, IoT based healthcare service providers and all other stakeholders are still struggling to find out the most critical privacy and security issues to address. Most suitable solutions to counter those issues remain open since the technology capabilities are evolving day by day, and attackers are getting more powerful. The historical findings may not be enough to address the present IoT issues. Thus, traditional security and privacy protection mechanisms need to be reconsidered and redesigned to ensure the effectiveness and efficiency of healthcare services.

In order to point out valuable directions for further research and provide useful references for researchers, we are trying to investigate, identify and classify all the possible privacy and security threats and risks of current IoT based healthcare services in this study.The study has attempted to explore the potential security and privacy issues related to IoT Healthcare applications operate on cloud and fog computing architectures and proposed solutions that can mitigate those issues.

II. MATERIAL & METHODS

Thirty Peer-reviewed publications dated from 2016 to 2018 were collected as raw data to analyze the research, and those publications were selected form IEEE and Springer databases.

This research focuses on exploring security and privacy issues in IoT based healthcare applications. As shown in Figure S1, our study investigated on Perception Layer, Network Layer, Middleware, Application Layer and Business Layer. Table S1 illustrates those IoT layers and their roles in an IoT based application (Please refer Supplementary Material Document for Figure S1 and Table S1). Further, the study examined four different sensor categories, as shown in Table S2,namely wearable Sensors, Implantable Sensors, Ambient Sensors, and Stationary Devices. (Please refer Supplementary Material Document for Table S2).These attributes deliver the most significant contents of the publications related to the research topic.

A. Collection of raw data

In order to gain knowledge about the research topic, 30 different peer-reviewed articles were observed. During the study, 41 different sensor devices have been identified from the published articles, and Table S3 demonstrates the number of different sensor devices used in IoT based healthcare applications. Further, 86 different threat and risks also recognized by reviewing published articles.

Table S4 shows the number of threats identified under each IoT layer. The raw data collected depicts in Table S5. (Please refer Supplementary Material Document for Table S3, Table S4 and Table S5).

B. Data inclusion criteria

During the study, we have developed Table S5 to construct the data inclusion criterion. We have used the attributes which are mentioned in the material and methods section in order to develop Table S5. Comparison of data is achieved through that table. We have gathered data by analyzing 30 peer-reviewed articles which were published related to privacy and security challenges in IoT based healthcare applications in recent years (2016 to 2018). Some of the initially selected articles have been excluded from the study due to the following reasons; the articles provide insufficient data in the data comparison table, and the articles were not published in recent years.

C. Analysis of raw data

Upon completing the comparison, we were able to construct results under four different topics, namely sensors, threats, solutions and countries. We were able to find out the popularity of various sensor devices used in different IoT based healthcare applications in recently published articles. To achieve that initially, we listed the sensor devices found in the articles under individual sensor types. After that, we analyzed the list in order to find out the number of repetitions of each sensor device. Finally, we translate the calculated figures into percentage values and construct the charts in order to demonstrate the results. Similarly, we undertook the same methodology in order to find out the number of threats under each layer and find out the recommended solutions by authors. In order to find out the countries that have been studied IoT healthcare privacy and security issues, we have carried out an analysis and presented the results on the basis of their country of origin on a map.

III. RESULTS

In this section, we draw the following statistical diagrams of IoT healthcare-related security and privacy research papers under three main topics, namely, Sensor, Threat, Solution and Countries.

3.1. Sensor Analysis

3.1.1. Wearable Sensors

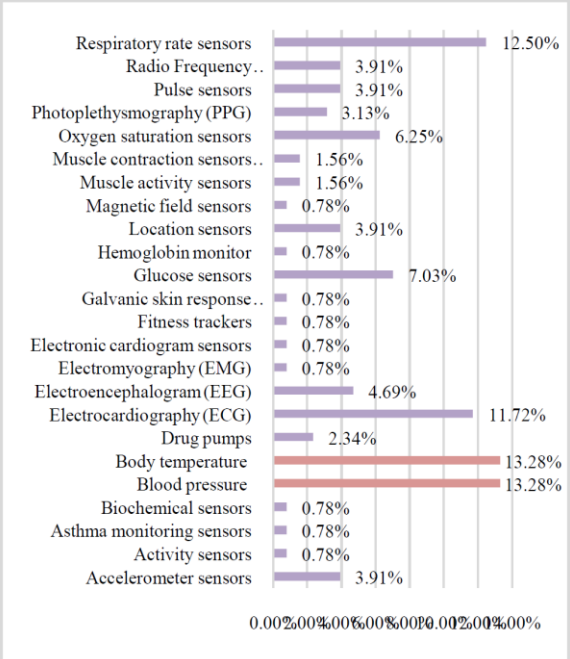


Fig.1. Wearable Sensor

Figure 1 illustrates the percentage of wearable sensors mentioned in different applications in recently published papers. We found that many IoT based healthcare-related studies comprise body temperature sensors and blood pressure sensors. Further, Electrocardiography (ECG) and respiratory rate sensors have also gained significant attention in recent IoT healthcare applications.

3.1.2. Implantable Sensors

Figure 2 shows the number of implantable sensors mentioned in recent studies. As can be seen in the figure, some of the studies have used the term 'implantable medical device' in their papers without specifying the device name. During the study, we have identified that the implantable sensors did not have much attention in recent decades. According to the Australian Government, Department of Health Therapeutic Goods Administration (2012), many adverse events have reported involving implantable medical devices (Australian Government Department of Health Therapeutic Goods Administration, 2012). Further Food and Drug Administration (FDA) has stated that in 2010, due to toxic metallic debris in metal hip implants, many people had to face risky surgeries to remove them. In this context, FDA is enforcing regulations on IoT implantable devices (Lind, 2017). These restrictions and regulations could be the reason behind the lack of discussions in recent IoT studies regarding implantable devices.

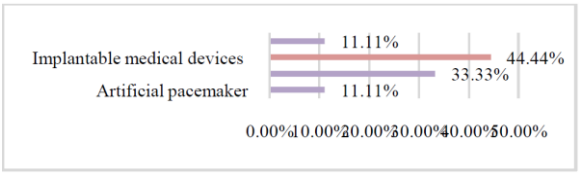


Fig.2. Implantable Sensors

3.1.3. Ambient Sensors

Figure 3 depicts the percentage of ambient sensors mentioned in recent studies. We found that motion sensors gained the greatest attention in IoT healthcare application-related studies. Mainly those studies are about patient monitoring systems and in-door navigation application scenarios.

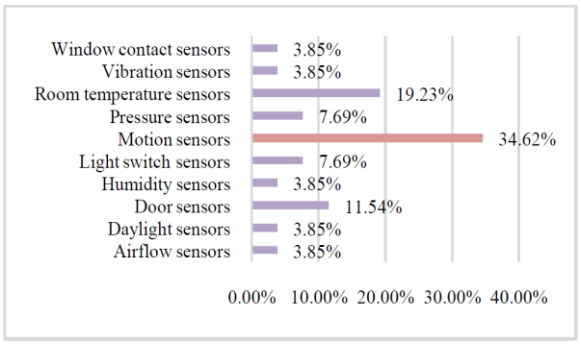


Fig.3. Ambient Sensors

3.1.4. Stationary Sensors

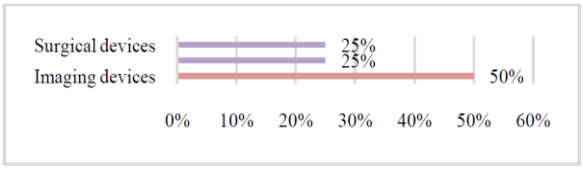


Fig.4. Stationary Sensors

Figure 4 shows the percentage of stationary sensors mentioned in recent studies. During the study, we found that imaging devices such as x-ray and Magnetic Resonance Imaging (MRI) gained the greatest attention in IoT healthcare application-related studies.

3.2.5. The Percentage of Different Types of Sensors Identified in Previous Studies

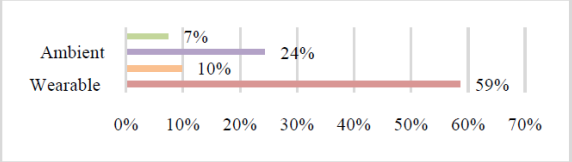


Fig.5. Different Sensor Types

Figure 5 illustrates the percentage of different types of sensors identified in previous studies. According to Table 3, we have identified a total of 41 different sensor devices. Based on Table 3, Figure 6 illustrates the percentage values for each sensor device category. We found that most sensor devices fall under the wearable category, and the least amount of sensor devices are under the stationary category.

3.2. Threat Analysis

3.2.1. Perception Layer Threats

Figure 6 demonstrates the percentage of perception layer threats identified in different IoT healthcare applications in recently published papers. We found that sensor tracking is the most commonly identified threat in the IoT perception layer. Further, tag cloning, side channel, physical harm, and jamming threats have also been identified as potentially significant threats in the perception layer.

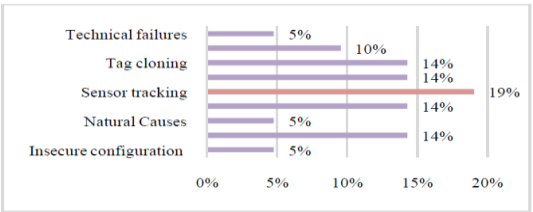


Fig.6. Perception Layer Threat

3.2.2. Middleware Threats

As shown in Figure 7 we found four different threats in four different application scenarios. Each threat has been addressed in only one study.



Fig.7. Middleware Threats

3.2.3. Network Layer Threats

Figure 8 illustrates the percentage of the number of network layer threats recognized in different IoT healthcare applications in the previous studies. As shown in the figure, most of the studies emphasized DoS attacks on IoT healthcare applications. Further, eavesdropping, man-in-the-middle, and impersonation attacks have also been identified as the second most significant threats in the network layer.

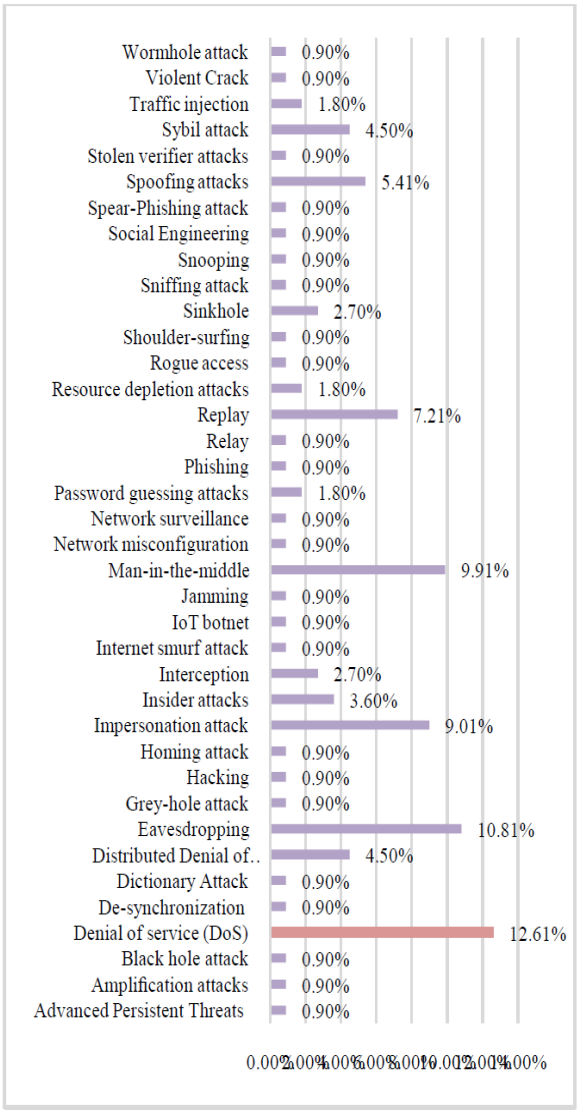


Fig.8. Network Layer Threats

3.2.4. Application Layer Threats

Figure 9 depicts the percentage of application layer threats recognized during the study. According to the figure, we have identified that the data modification threat has gained the most attention in recent studies. Further, malware infection and brute force attacks have also gained significant attention in recent studies.

3.2.5. Business Layer Threats

Figure 10 shows the percentage of business layer threats identified in previous studies. We found that most threats have gained similar level focus except data leakage and data breaches. Majority of studies have focused on data leakage and breaches.

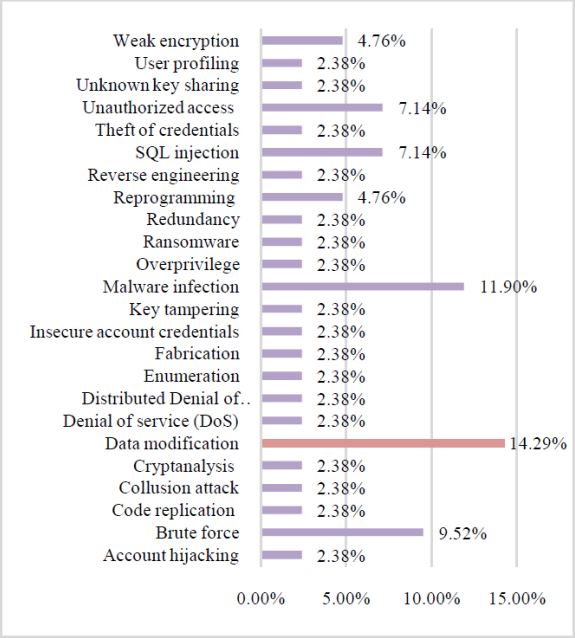


Fig.9. Application Layer Threats

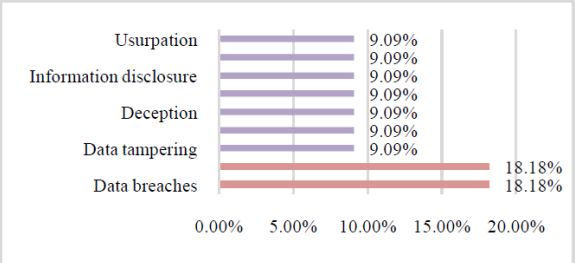


Fig.10. Business Layer Threats

3.2.6. The Percentage of Different Types of Threats Identified in Previous Studies

Figure 11 illustrates the total threat count that has been addressed in previous studies according to their affected IoT layer. As shown in the figure we found that the most threats fall under the network layer and the least amount of threats are under middleware category. Further, we found that similar threat count under business and perception layers.

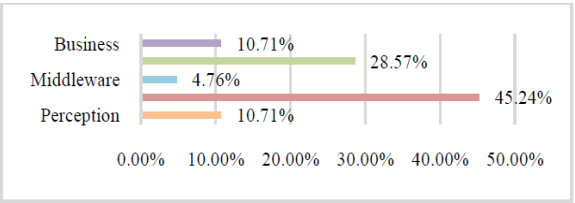


Fig.11. Threats in Different Layers

3.3. Proposed Solutions

During the analysis, we have counted the different types of security solutions in order to find out the most significant security and privacy solution, which is recommended by different IoT based healthcare application scenarios. According to Figure 12, identification, authentication and authorization management practices were identified as the most recurrent security solution in IoT healthcare applications. Further, cryptographic techniques are also recommended by many studies.

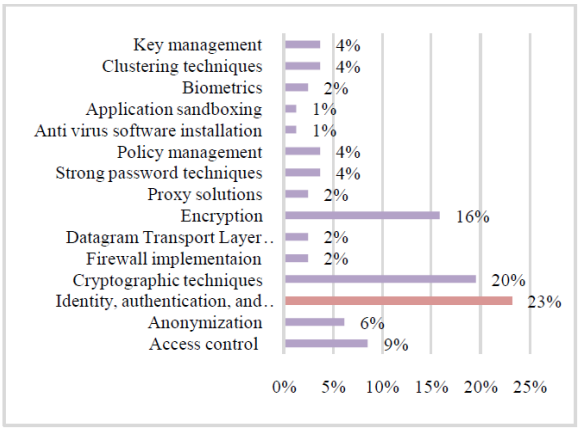


Fig.12. Proposed Solutions

3.4. Percentage of Countries Involved in IoT Studies

Figure 13 shows the percentage of IoT healthcare privacy and security related research studies carried out in different countries. Our observation found that China and USA have involved in most research studies focused on the security and privacy of IoMTbased healthcare applications. Further, Australia, Malaysia, Sweden, and France have also involved in IoT related studies.

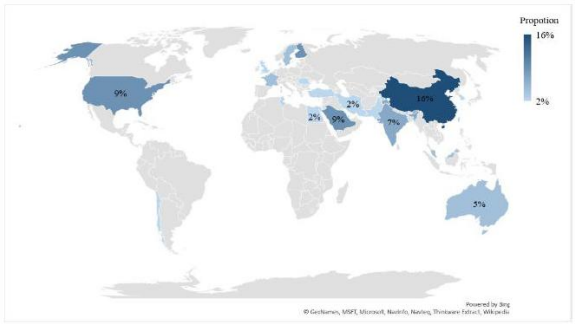


Fig.13. Proportion of Countries

Our research demonstrates that the significant research areas including sensors and privacy and security threats on IoT healthcare segment, which was highlighted by previous research studies. The study shows the sensor device proportions used in previous IoT based healthcare studies and previous research hotspots in IoT security. The survey can help in providing a better understanding for the previous research background of IoT based healthcare sensors, security and privacy issues, and solution to design better IoT based applications which can offer better security for sensitive data. On the one hand, due to the rapid technology evolution, there might be innovative sensors which can produce new health data. On the other hand, new hackers' skills may create new or unknown threats that need to be considered in future studies. Thus, we can find that developing a system which can guarantee end-to-end security and privacy would be a significant

achievement in IoT-based healthcare segment and it should be considered as the goal for future researchers in this area. Moreover, this ongoing research aims to develop a risk assessment to support decision making and investigate security standards, best practices that regulate security and privacy requirements for IoT based healthcare applications. By this work, we hope to enhance the awareness of every stakeholder in the IoT healthcare context.

In this study, we have explored the multifaceted architecture of IoT based healthcare applications. Although there are numerous research studies regarding the IoT platform, there is a significant research gap in the existing studies. Most of these studies usually focus on a particular area and rarely consider other research areas, which ultimately result in proposing solutions to address a specific problem or concern and failing to address the broader IoT context. Thus, there are always certain issues still need to be addressed. Further, continually growing and changing information technology capabilities enables new threat vectors. In this context, we have explored most recent publications and illustrated a broader picture of IoT healthcare application related privacy and security concerns, sensor device usage and recommended privacy solutions.

IV. CONCLUSION

With the recent trend in adopting IoT technologies for healthcare applications, the security features in healthcare have attracted the attention of several researchers and security experts. Lack of security and privacy in IoT healthcare applications could pose great life-threatening risks. Since technology is growing day by day, still there are many threats and risks that have not been entirely addressed. In this study, we have expected to provide widespread idea about IoT based healthcare application sensors and related security and privacy issues. The network layer seems to be the most vulnerable layer to various security, and privacy threats and attacks on the Internet of Things (IoT) based healthcare services. Wearable sensors were utilized in the majority of IoT based healthcare applications. China and the USA have the most notable focus on security and privacy of IoMT based healthcare applications.

AUTHOR CONTRIBUTION

N.N. and M.N.H. conceived the study idea and developed the analysis plan. N.N. analyzed the data and wrote the initial paper. M.N.H. helped to prepare the figures and tables and finalizing the manuscript. All authors read the manuscript.

REFERENCES

[1] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017, October). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In Local Computer Networks Workshops (LCN Workshops), 2017 IEEE 42nd Conference on (pp. 112-120). IEEE.

[2] Amaraweera, S. P., & Halgamuge, M. N. (2019). Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues. In Security, Privacy and Trust in the IoT Environment (pp. 153-179). Springer, Cham.

[3] Australian Government Department of Health Therapeutic Goods Administration. (2012). Implanting medical devices. Retrieved from https://www.tga.gov.au/implanting-medical-devices 2012.

[4] Chandrasiri, G. P., Halgamuge, M. N., & Jayasekara, C. S. (2019). A Comparative Study in the Application of IoT in Health Care: Data Security in Telemedicine. In Security, Privacy and Trust in the IoT Environment (pp. 181-202). Springer, Cham.

[5] Ekanayake, B. N., Halgamuge, M. N., & Syed, A. (2018). Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). In Cognitive Computing for Big Data Systems Over IoT (pp. 139-174). Springer, Cham.

[6] El Zouka, H. A. (2017, October). An authentication scheme for wireless healthcare monitoring sensor network. In Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), 2017 14th International Conference on (pp. 68-73). IEEE.

[7] Gope, P., & Sikdar, B. (2018). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. IEEE Internet of Things Journal.

[8] Gope, P., Lee, J., & Quek, T. Q. (2018). Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. IEEE Transactions on Information Forensics and Security, 13(11), 2831-2843.

[9] He, D., Ye, R., Chan, S., Guizani, M., & Xu, Y. (2018). Privacy in the Internet of Things for Smart Healthcare. IEEE Communications Magazine, 56(4), 38-44.

[10] Ida, I. B., Jemai, A., & Loukil, A. (2016, December). A survey on security of IoT in the context of eHealth and clouds. In Design & Test Symposium (IDT), 2016 11th International (pp. 25-30). IEEE.

[11] Ifrim, C., Pintilie, A. M., Apostol, E., Dobre, C., & Pop, F. (2017). The art of advanced healthcare applications in big data and IoT systems. In Advances in mobile cloud computing and big data in the 5G Era (pp. 133-149). Springer, Cham.

[12] Lind, K. D. (2017). IMPLANTABLE DEVICES: REGULATORY FRAMEWORK AND REFORM OPTIONS. Insight.

[13] Qi, J., Yang, P., Min, G., Amft, O., Dong, F., & Xu, L. (2017). Advanced Internet of Things for personalised healthcare systems: A survey. Pervasive and Mobile Computing, 41, 132-149.

[14] Rauf, A., Shaikh, R. A., & Shah, A. (2018, February). Security and privacy for IoT and fog computing paradigm. In Learning and Technology Conference (L&T), 2018 15th (pp. 96-101). IEEE.

[15] The Statistics Portal. (2018). Number of Internet of Things (IoT) units in healthcare in the European Union (EU) in 2017, 2020 and 2025 (in millions). Retrieved from https://www.statista.com/statistics/691848/iot-units-in-healthcare-in-the-eu/

[16] U.S. Department of Health and Human Services. (2018). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[17] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[18] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal.

★★★