Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review

Conference Paper · November 2019

CITATIONS
0

READS
429

3 authors:

N. Nanayakkara
Charles Sturt University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Malka N. Halgamuge
University of Melbourne
146 PUBLICATIONS **973** CITATIONS
SEE PROFILE

Ali Syed
Charles Sturt University
20 PUBLICATIONS **161** CITATIONS
SEE PROFILE

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

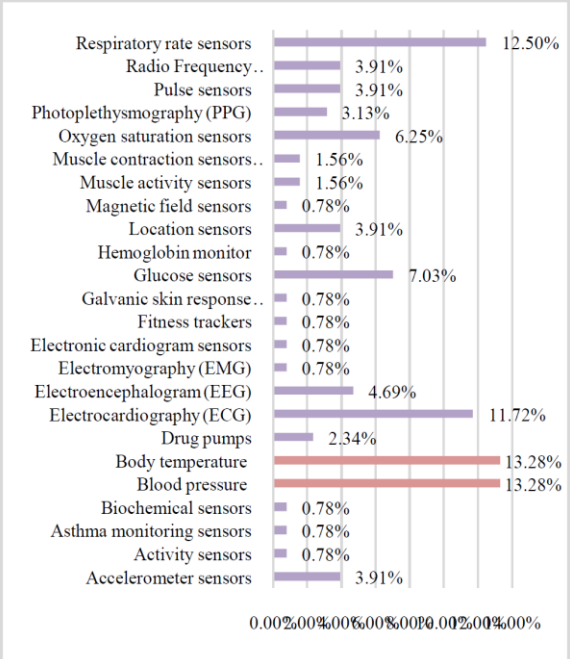

Fig.1. Wearable Sensor

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.

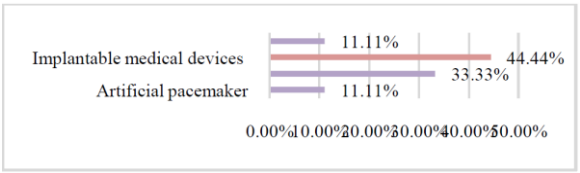

Fig.2. Implantable Sensors

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.

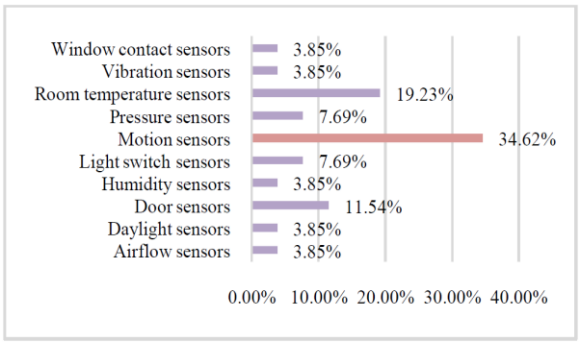

Fig.3. Ambient Sensors

3.1.4. Stationary Sensors

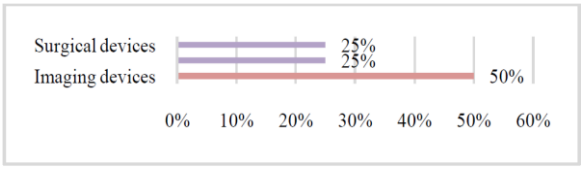

Fig.4. Stationary Sensors

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

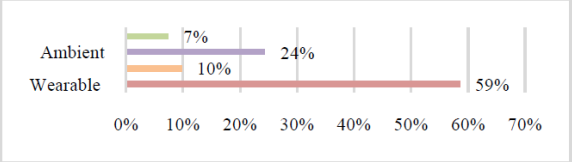

Fig.5. Different Sensor Types

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.

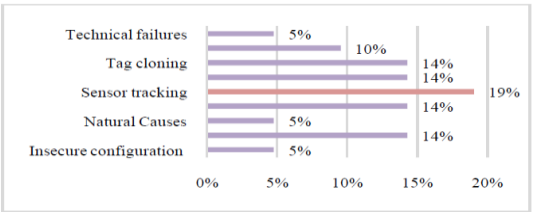

Fig.6. Perception Layer Threat

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.

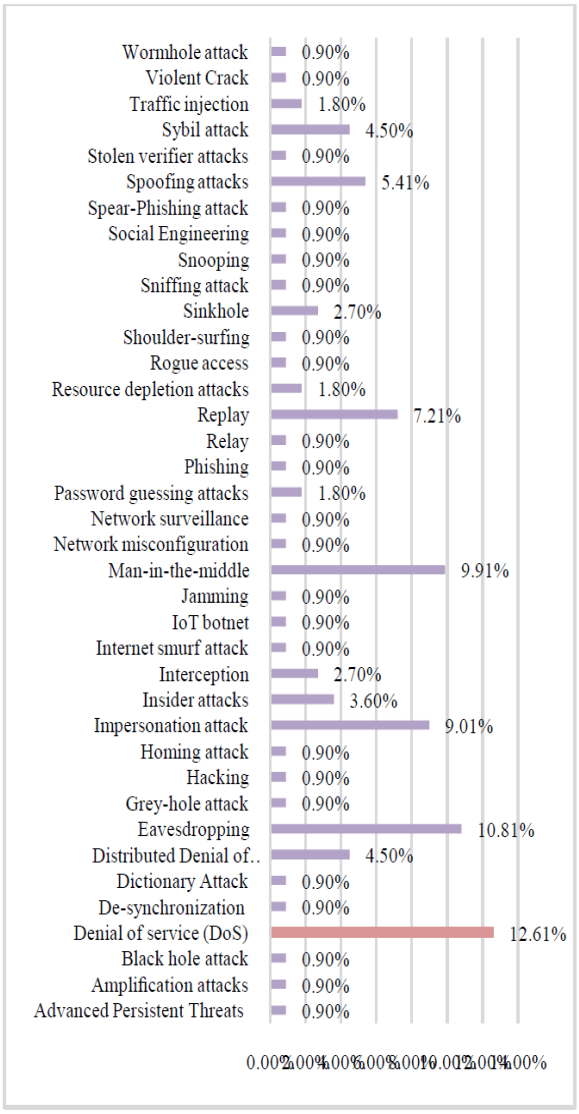

Fig.8. Network Layer Threats

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.

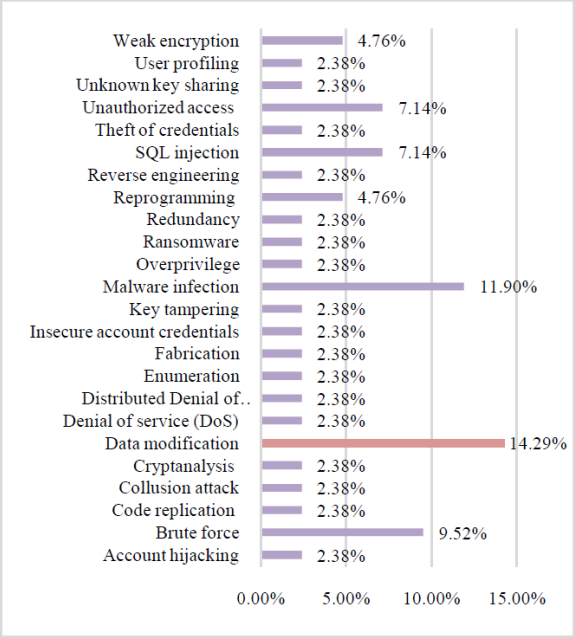

Fig.9. Application Layer Threats

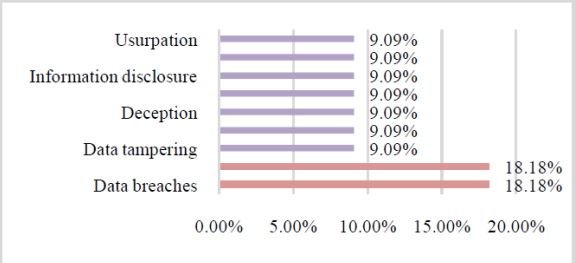

Fig.10. Business Layer Threats

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.

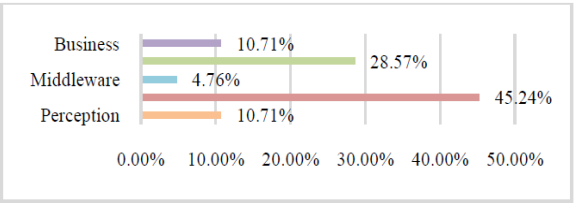

Fig.11. Threats in Different Layers

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.

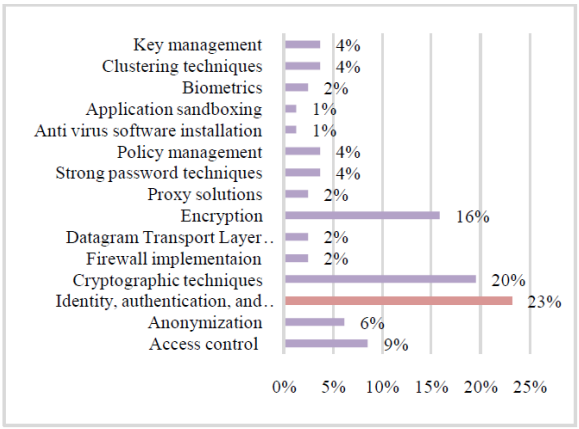

Fig.12. Proposed Solutions

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.

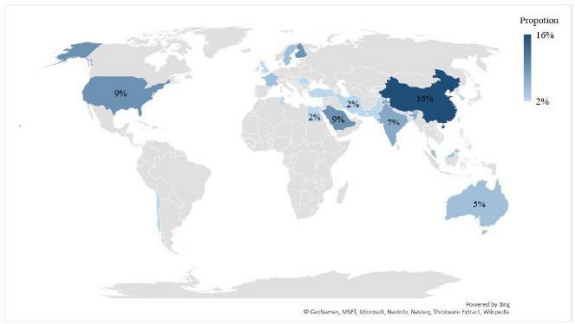

Fig.13. Proportion of Countries

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.

★★★

Supplementary Materials

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

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

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

1. MATERIAL & METHODS

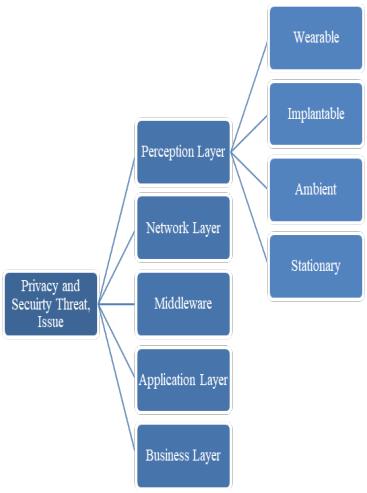

Fig.S1. Data Collection Attributes

Table S1: Layers

Attribute	Description
Perception Layer	Acquire and collect data through different physical equipment, devices or sensors and then transfer data to the network layer (Alsubaei et al., 2017; Tao et al., 2014)
Network Layer	Responsible for connecting all devices allow health data to be collected, stored and routed toward the destination and network addressing (Alsubaei et al., 2017; Qi et al., 2017)
Middleware	Facilitates responding to the demands by controlling collecting, and filtering received data and perform service discovery and provide access control to the devices (Alsubaei et al., 2017; Qi et al., 2017)
Application Layer	Act as an interface between end users and IoMT devices (Alsubaei et al., 2017; Qi et al., 2017)
Business Layer	Handles the business logic and supports the business process (Alsubaei et al., 2017)

Table S2: Sensors

Attribute	Description
Wearable Sensors/ Devices	Wearable sensors/ devices that enable accurate, continuous, real-time monitoring of a patient's physiological conditions and motion activities (Alsubaei et al., 2017; Baker et al., 2017; Majumder et al., 2017; Qi et al., 2017)
Implantable Sensors/ Devices	Sensors/ devices that fit inside the patient's body and incorporates with wireless communication to transmit measurements (Alsubaei et al., 2017; Konstantas, 2007)
Ambient Sensors/ Devices	Sensors/ devices that sense the patient's surrounding area and monitor patient's activity patterns (Alsubaei et al., 2017; Qi et al., 2017)
Stationary Sensors/ Devices	Sensors/ devices that holds patient data usually manage by medical staff, not the patient (Alsubaei et al., 2017)

A. Collection of raw data

Table S3: Sensors

Wearable	Implantable	Ambient	Stationary	Total
24	4	10	3	41

Table S4: Threats

Perception	Network	Middleware	Application	Business	Total
9	38	4	24	11	84

Table S5: Raw Data

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
1	He et al., 2018	Patients' general health data monitoring system	Cloud Computing	Blood pressure Respiratory rate sensors Glucose sensors Pulse sensors Electroencephalogram (EEG)		Room temperature sensors Humidity sensors			Denial of service (DoS) Violent Crack Dictionary Attack Password guessing attacks Shoulder-surfing Phishing				Identity Authentication Password strength evaluation method
2	Zhou et al., 2018	Patients' general health data monitoring system	Cloud Computing	Location sensors Blood pressure Respiratory rate sensors Body temperature				Insecure configuration Insecure protocols	Distributed Denial of service (DDoS) IoT botnet		Malware infection Overprivileged		Context based permission Safety consciousness Anonymous protocols Lightweight trusted execution
3	Rauf et al., 2018	Patients' general health data monitoring system	Cloud Computing Fog Computing	Blood pressure Body temperature Electrocardiography (ECG) Oxygen saturation sensors		Motion sensors		Tampering devices Tag cloning Sybil attack Jamming Interception and interference	Distributed Denial of service (DDoS) Denial of service (DoS) Man-in-the-middle Jamming Interception Wormhole attack Sinkhole Internet smurf attack Resource depletion attacks Sybil attack Black hole attack Homing attack		Reprogramming Theft of credentials Distributed Denial of service (DDoS) Denial of service (DoS)		Low network latency Properly authenticated end devices Legitimate intermediary devices Encrypted communication Encrypted storage of data Cryptographic techniques
4	Sun et al., 2018	Patients' general health data monitoring system	Cloud Computing		Implantable medical devices				Man-in-the-middle Spoofing attacks Denial of service (DoS) Traffic		Brute force Unauthorized access		Access Control Data Encryption Trusted Third Party Auditing Data Search Data Anonymization

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
									Injection				
5	Salahuddin et al., 2018	Patients' general health data monitoring system	Cloud Computing Fog Computing	Electrocardiography (ECG) Oxygen saturation sensors Photoplethysmography (PPG)					Traffic injection Denial of service (DoS) Hacking Network surveillance				Secure communication protocols Homomorphic encryption
6	Luo et al., 2018	MobiCare MEDiSN	Cloud computing						Eavesdropping Impersonation attack		Collusion attack	Data leakage Data breaches	Framework called Privacy protector for secure data collection
7	Almulhim & Zaman, 2018	MEDiSN	Cloud computing	Respiratory rate sensors Electrocardiography (ECG)					Impersonation attack Man-in-the-middle		Unknown key sharing		Secure group-based lightweight authentication scheme
8	Nausheen & Begum, 2018	Patients' general health data monitoring system	Cloud computing	Accelerometer sensors Respiratory rate sensors	Embedded cardiac Artificial pacemaker						Reverse engineering Key tampering	Data tampering Data breaches Data theft	Solutions against potential vulnerabilities by protecting mobile applications using obfuscation and return oriented programming techniques.
9	Farahani et al., 2018	Patient-centric IoT eHealth ecosystem	Fog Computing	Electrocardiography (ECG) Respiratory rate sensors Glucose sensors Blood pressure Body temperature Pulse sensors Hemoglobin monitor Photoplethysmography (PPG)		Motion sensors		Tag cloning Jamming	Man-in-the-middle Eavesdropping Sybil attack Denial of service (DoS) Sniffing attack Spear-Phishing attack Spoofing attacks Sinkhole		SQL injection Malware infection Brute force		Robust cryptographic algorithms Key management system Identity, authentication, and authorization management Secure booting Application sandboxing Whitelisting Fine-grained access control capability of resources Password enforcement policies Secure pairing protocols
10	Chaudhury et al.,		Cloud computing	Body temperature Respiratory rate sensors Electrocardiography		Room temperature sensors					Unauthorized access		Effective healthcare monitoring system

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
	2017, August			(ECG)									
11	Pulkis et al., 2017, August	Nursing Home Patient Monitoring System Monitoring and Mitigation of Eating Disorders In-Door Navigation System for Blind and Visually Impaired Person Insulin Dosage Administration for Diabetes Patients Hospital Information System	Cloud Computing	Accelerometer sensors Glucose sensors Respiratory rate sensors Oxygen saturation sensors Electrocardiography (ECG) Photoplethysmography (PPG) Body temperature Blood pressure		Light sensors Door sensors Motion sensors Room temperature sensors Pressure sensors		Physically destroying an IoT device	Eavesdropping Denial of service (DoS)		Data modification Reprogramming		Access control Cryptography Anonymization Obfuscation Tamper resilience of blockchain technology Asymmetric cryptographic algorithm
12	Alsubaei et al., 2017, October	Patients' general health data monitoring system	Cloud Computing	Location sensors Body temperature Blood pressure Electrocardiography (ECG) Photoplethysmography (PPG) Respiratory rate sensors Activity sensors Muscle activity sensors Fitness trackers Glucose sensors	Swallow able camera capsule Embedded cardiac	Motion sensors Room temperature sensors Pressure sensors Door sensors Vibration sensors Daylight sensors	Imaging devices Surgical devices	Side channel Tag cloning Tampering devices Sensor tracking	Eavesdropping Replay Man-in-the-middle Rogue access Denial of service (DoS) Sinkhole	Cross-Site request forgery Session hijacking Cross-site scripting	SQL injection Account hijacking Ransomware Brute force	Information disclosure Deception Disruption Usurpation	

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
				Electronic cardiogram sensors Oxygen saturation sensors Accelerometer sensors Biochemical sensors Drug pumps						(XSS)			
13	Baker et al., 2017	Patients' general health data monitoring system	Cloud Computing	Pulse sensors Respiratory rate sensors Body temperature Blood pressure Oxygen saturation sensors Electrocardiography (ECG) Electroencephalogram (EEG) Glucose sensors		Motion sensors			Man-in-the-middle Eavesdropping Impersonation attack Spoofing attacks Interception		Brute force		Encryption Standards (Elliptical Curve Hellman-Diffie (ECHD) algorithm/ Homomorphic encryption (FHE)) Access control policies (Biometrics) Signal scrambling A steganography-based approach to access control Fully homomorphic encryption (FHE)
14	Binu et al., 2017	Secure health monitoring for sports personnel	Cloud Computing	Electrocardiography (ECG) Blood pressure Muscle activity sensors Body temperature				Side channel	Replay Relay Spoofing attacks Denial of service (DoS)		Data modification		LEACH routing protocol Modifed HIP-DEX key exchange scheme Elliptic Curve Qu-Vanstone (ECQV)
15	Kumar et al., 2017	Patients' general health data monitoring system	Cloud Computing	Pulse sensors Blood pressure Respiratory rate sensors Body temperature					Insider attacks Replay Impersonation attack				Encryption Biometrics Two factor authentications
16	El Zouka, 2017	Patient Monitoring System (PMS)	Cloud Computing	Body temperature Electrocardiography (ECG) Respiratory rate sensors Blood pressure Glucose sensors Oxygen saturation sensors					Impersonation attack		Data modification Code replication		Unique cryptographic key Authentication algorithm (Registration/ Login/ Authentication)
17	Razzaq et al., 2017	Patients' location	Cloud Computing	Radio Frequency IDentification (RFID) Location sensors					Eavesdropping Denial of service (DoS) Spoofing attacks		Fabrication		Data authentication and authorization Access control Encryption Anonymous data transmission

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
									Man-in-the-middle				Firewall implementation Cryptographic techniques
18	Ifrim et al., 2017	Patients' general health data monitoring system	Big Data Cloud Computing	Electroencephalogram (EEG) Blood pressure Respiratory rate sensors Muscle contraction sensors (EMG) Electrocardiography (ECG)					Eavesdropping Impersonation attack Replay		Data modification		Data integrality Authentication Encryption Freshness protection
19	Qi et al., 2017	Personalized healthcare systems (PHS)	Cloud Computing	Body temperature Electrocardiography (ECG) Electroencephalogram (EEG) Blood pressure Radio Frequency IDentification (RFID) Accelerometer sensors Magnetic field sensors Galvanic skin response sensors (GSR)		Door sensors Window contact sensors Light switch sensors Motion sensors			Sybil attack		Malware infection		Encryption techniques Cryptographic scheme Privacy-preserving health data aggregation
20	Yang et al., 2017	Patients' general health data monitoring system and location	Cloud Computing Fog Computing	Radio Frequency IDentification (RFID) Location sensors Blood pressure Body temperature	Implantable medical devices			Side channel Physically destroying an IoT device	Man-in-the-middle Distributed Denial of service (DDoS) Eavesdropping Impersonation attack Replay Resource depletion attacks Amplification attacks		Cryptanalysis Malware infection		Cryptographic hash algorithms Digital signature Device's unique fingerprint Firewall implementation Anti-virus software installation Identity-based authentication scheme Datagram Transport Layer Security (DTLS)
21	Williams, & McCauley,	Personal health data monitoring system	Cloud Computing		Implantable medical devices		Smart utensils		Network misconfiguration Denial of service (DoS)		Weak encryption Redundancy		Policy-based access controls Authentication and identity management System integrity through security protection mechanisms

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
	2016, December												
22	Porambage et al., 2016	E-healthcare	Cloud Computing	Drug pumps Glucose sensors Respiratory rate sensors Blood pressure Body temperature Radio Frequency IDentification (RFID)		Airflow sensors Motion sensors		Sensor tracking			Malware infection User profiling		Cryptography Proxy solutions Privacy Policies
23	Almotiri et al., 2016	An intelligent Augmented Quick Health (AQH) health monitoring system	Cloud Computing	Glucose sensors Electrocardiography (ECG) Blood pressure Asthma monitoring sensors Body temperature Respiratory rate sensors				Natural Causes Technical failures	Denial of service (DoS)		Unauthorized access Data modification		Access control includes using unique user ID Encrypted storage and transmission of data Strong password Perform Audits
24	Alasmari & Anwar, 2016	Electronic Patient Health Information	Cloud Computing	Radio Frequency IDentification (RFID) Blood pressure Respiratory rate sensors Body temperature					Distributed Denial of service (DDoS) Man-in-the-middle		SQL injection		Multi-factor authentication Cryptographic keys
25	Sajid et al., 2016	Patients' general health data monitoring system	Cloud Computing						Spoofing attacks Insider attacks Replay Advanced Persistent Threats Distributed Denial of service (DDoS) Man-in-the-middle Social Engineering				Policy Management Test-bed architecture to ensure data integrity Attack-resilient algorithms Cryptographic techniques Authentication Encryption Risk Management Secure communication channels Proxy Solutions Network Segregation Log Analysis Network Traffic Analysis Regular Vulnerability Testing
26	Yuehong et al.,	Healthcare system Smart	Cloud Computing	Oxygen saturation sensors Electrocardiography		Motion sensors		Sensor tracking	Eavesdropping			Unauthorized access	Identification & authentication

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
	2016	rehabilitation		(ECG) Pulse sensors Accelerometer sensors Muscle contraction sensors (EMG)									
27	Elmisery et al., 2016	M-psychiatry system C-SMART Healthopia	Cloud Computing Fog Computing	Drug pumps Electroencephalogram (EEG) Glucose sensors	Embedded cardiac		Imagine devices		Sybil attack Insider attacks Eavesdropping				IBE-Lite scheme Cryptographic protocols Anonymity Network Clustering Techniques
28	Moosavi et al., 2016	Patients' general health data monitoring system	Cloud Computing Fog Computing	Respiratory rate sensors Body temperature Location sensors Oxygen saturation sensors		Room temperature sensors			Eavesdropping Snooping Grey-hole attack Sybil attack Impersonation attack Denial of service (DoS)			Data leakage	Elliptic Curve Cryptography (ECC) Mutual authentication and authorization Datagram Transport Layer Security (DTLS)
29	Gope & Hwang, 2016	BSN-Care	Cloud Computing	Electrocardiography (ECG) Electromyography (EMG) Electroencephalogram (EEG) Blood pressure Body temperature		Motion sensors		Sensor tracking	Replay Denial of service (DoS) Interception Impersonation attack Eavesdropping De-synchronization	Forgery attacks	Data modification		Lightweight Anonymous Authentication Protocol Authenticated encryption scheme offset codebook (OCB) mode Shadow identity with the emergency key pair One-time-alias identity with track sequence number
30	Ida et al., 2016, December	eHealth system	Cloud Computing		Implantable medical devices			Physically destroying an IoT device	Denial of service (DoS) Impersonation attack Insider attacks Man-in-the-middle Replay Stolen verifier attacks Password guessing attacks		Enumeration Insecure account credentials Weak encryption		Use embedded sensor network rather than wearable sensors Authentication and access control "Registration Authority" Watermarking techniques File retrieval and error recovery-based mechanism VIRTUS middleware The Constrained Application Protocol (CoAP) Elliptic Curve Cryptography algorithm (ECC) Patient-oriented PHR system on clouds

No	Citation	Healthcare Application	Methodology	Wearable	Implantable	Ambient	Stationary	Perception Layer	Network Layer	Middleware	Application Layer	Business Layer	Proposed Solutions
													PKI-Like Protocol Two-phase Authentication Protocol for Wireless Sensor Network Threshold Cryptography-based Group Authentication (TCGA) scheme Identity Framework Management Methods Data partitioning and scrambling method at the application layer Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways

2. DISCUSSION

In recent decades, many pervasive healthcare systems have been proposed, discussed and implemented (ENISA, 2016). IoT technologies have created innovative communication environment for those pervasive healthcare systems by interconnecting devices and platforms. The notion of the Internet of Medical Things (IoMT) has emerged when IoT components, infrastructures are integrating with traditional healthcare systems. However, there is a significant privacy and security risk in this IoT adoption since the IoMT deals with an extensive amount of information assets which ultimately affect patient's life. In this context, IoT based healthcare applications must meet preconditions of information security as they are conveying information of an extremely private nature for patients. Privacy and security conditions of confidentiality, integrity, availability, accountability, non-repudiation must be met in such systems since the end to end privacy cannot be achieved without them. In order to gain patient's trust regarding IoT based healthcare applications, potential security and privacy issues must be identified and robust security and control mechanisms need to be established to counter those issues (Sahi et al., 2018).

Security and privacy are the utmost important factors of IoT based healthcare application. Since the application holds and transmits personal sensitive data for patients, it should be able to preserve the privacy and security of personal information. Thus, understating the potential threats, attacks or risks of the IoT based healthcare applications could help raise the awareness among every stakeholder in IoT healthcare context. Many research studies were carried out to explore those potential threats and attacks. However, those studies were not able to present potential threat distribution at a glance and to present extensive findings according to the IoT layer. Further, those historical research studies published between 2016 and 2017 need to be updated and expand since the technology is evolving hacking capabilities also growing increasingly (Ida et al., 2016; Pulkkis et al., 2017; Gope & Hwang, 2016; El Zouka, 2017; He et al., 2018). Thus, we aim to present more widespread threat distribution among multiple layers in the IoT paradigm.

Further, the research findings have demonstrated 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. The findings are also supported by some previous studies (Baker et al., 2017; El Zouka, 2017). In addition to that, it was identified that the Denial of Service (DoS) is the most common threat in the network layer. However, some previous studies focused on identity authentication related threats and key guessing attacks only (El Zouka, 2017; He et al., 2018). We have identified that some other research studies also have generated similar results regarding the IoT healthcare context. Gartner (2018) has concluded that the wearable sensors will hold the key to present and future connected healthcare monitoring. During our study, we also have found that the wearable sensors are the most identified sensor device category in IoT healthcare paradigm. Further, Gartner has forecasted that the wearable sensor technology market will reach 500 million units by 2021 and 90% of wellness programs will include fitness trackers in 2021 (Pettey, 2018). In addition to that wearable sensors were identified as the most crucial component of IoT technology in order to track and monitor body parameters and movements. Apart from the identified wearable sensors, there will be more innovative wearable sensors integrated with future healthcare applications such as biometric garments which make wearable sensors more sophisticated compared to the other sensor categories. Some studies have predicted that the future wearable sensor could be hidden by adding a thin film inside person's favorite jewelry to measure biometric signals and/or activity levels (Vogenberg & Santilli, 2018).

In addition to that, we have identified that the network layer consists of the majority of security and privacy threats and denial of service is the most focused threat among those threats. However, we can find that some studies have generated contradictory results by stating power failures are the most critical threat in healthcare applications. They have stated that the power failure threat category such as server down, internet failure, service provider failures etc. has the highest likelihood among other threat categories (Maglogiannis & Zafiropoulos, 2006; Narayana Samy et al., 2010).

Besides that, a few remarks can be made on the study limitations. Due to the lack of appropriate recent studies in the IoT healthcare segment, the research database has to limit up to 30 peer-reviewed articles. Secondly, we have identified that the sensor technology is evolving day by day and many innovative sensors are adopting in IoT related applications. Further, attackers will find new threat avenues to breach sensitive data by exploiting loopholes in IoT applications. Thus, the results may not be fully comprehensive with present and evolving technology capabilities. However, this study has proven useful information about various sensor devices and potential threats that exist in the IoT healthcare context.

In this research, we investigate security and privacy threats in IoT healthcare context addressed in recent studies. We have explored different types of sensors such as wearable, implantable, ambient, and

stationary sensor usage in different types of IoT healthcare application-related to research context. In addition, we have studied and analyzed different privacy and security threats in different IoT layers as well as recommended solutions for those threats. We have identified that within the IoT healthcare segment, wearable sensors were able to gain the most attention as they are providing significant information about the human body. Consequently, we have found numerous potential threat avenues that have emerged to breach confidential health information generated in IoT based healthcare applications. It was found that the network layer could be easily compromised by the attackers through using various techniques. Based on our analysis, we have observed that the IoT healthcare related privacy and security concerns topic has gained significant attention in previous decades. Based on our study, we have identified several significant areas for future research directions.

REFERENCES

1. Alasmari, S., & Anwar, M. (2016, December). Security & privacy challenges in IoT-based health cloud. In Computational Science and Computational Intelligence (CSCI), 2016 International Conference on (pp. 198-201). IEEE.
2. Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016, August). Mobile health (m-health) system in the context of IoT. In Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on (pp. 39-42). IEEE.
3. Almulhim, M., & Zaman, N. (2018, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In Advanced Communication Technology (ICACT), 2018 20th International Conference on (pp. 481-487). IEEE.
4. 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.
5. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. IEEE Access, 5, 26521-26544.
6. Binu, P. K., Thomas, K., & Varghese, N. P. (2017, September). Highly secure and efficient architectural model for iot based health care systems. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 487-493). IEEE.
7. Chaudhury, S., Paul, D., Mukherjee, R., & Haldar, S. (2017, August). Internet of Thing based healthcare monitoring system. In Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual (pp. 346-349). IEEE.
8. 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.
9. Elmisery, A. M., Rho, S., & Botvich, D. (2016). A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. IEEE Access, 4, 8418-8441.
10. ENISA. (2016). Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport
11. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659-676.
12. Gope, P., & Hwang, T. (2016). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. IEEE Sensors Journal, 16(5), 1368-1376.
13. 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.
14. 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.
15. 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.
16. Konstantas, D. (2007). An overview of wearable and implantable medical sensors. Yearbook of medical informatics, 7(1), 66-69.
17. Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017, May). Identity privacy preserving biometric based authentication scheme for Naked healthcare environment. In Communications (ICC), 2017 IEEE International Conference on (pp. 1-7). IEEE.
18. Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems. IEEE Communications Magazine, 56(2), 163-168.
19. Maglogiannis, I., & Zafiropoulos, E. (2006, August). Modeling risk in distributed healthcare information systems. In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE (pp. 5447-5450). IEEE.
20. Majumder, S., Mondal, T., & Deen, M. J. (2017). Wearable sensors for remote health monitoring. Sensors, 17(1), 130.
21. Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Generation Computer Systems, 64, 108-124.
22. Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. Health informatics journal, 16(3), 201-209.
23. Nausheen, F., & Begum, S. H. (2018, January). Healthcare IoT: Benefits, vulnerabilities and solutions. In 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE.
24. Pettey, C. (2018). Wearables Hold the Key to Connected Health Monitoring. Retrieved from https://www.gartner.com/smarterwithgartner/wearables-hold-the-key-to-connected-health-monitoring/
25. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. IEEE Cloud Computing, (2), 36-45.
26. Pulkkis, G., Karlsson, J., Westerlund, M., & Tana, J. (2017, August). Secure and Reliable Internet of Things Systems for Healthcare. In 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 169-176). IEEE.
27. 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.
28. 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.
29. Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications (IJACSA), 8(6), 383-388.
30. Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., ... & Yaseen, A. (2018). Privacy Preservation in

e-Healthcare Environments: State of the Art and Future Directions. Ieee Access, 6, 464-478.
31. Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, 1375-1384.
32. Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2018). Softwarization of internet of things infrastructure for secure and smart healthcare. arXiv preprint arXiv:1805.11011.
33. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical Internet of Things: A review. Security and Communication Networks, 2018.
34. Tao, F., Zuo, Y., Da Xu, L., & Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Trans. Industrial Informatics, 10(2), 1547-1557.
35. Vogenberg, F. R., & Santilli, J. (2018). Healthcare Trends for 2018. American health & drug benefits, 11(1), 48.
36. Williams, P. A., & McCauley, V. (2016, December). Always connected: The security challenges of the healthcare Internet of Things. In Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on (pp. 30-35). IEEE
37. 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.
38. Yuehong, Y. I. N., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. Journal of Industrial Information Integration, 1, 3-13.
39. 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.