Cybersecurity Threats on Smart Healthcare Devices

Faculty of Science, Engineering and Technology
Swinburne University of Technology
Hawthorn, Australia

Abstract— The recent trends of embracing IOT for real-time data collection and improved services has given rise to serious cybercrimes. Previously, this nature of attacks was mainly targeting enterprises like retail industry. However, the attack horizon is now expanding to healthcare industry with recent empowering to use smart medical devices and health information systems for better connectivity and personalized medical services. The healthcare exploitation carries the risk of destructive consequences on patients' health. In this paper, we discuss the potential threats associated with networked healthcare systems and devices, identify security void. Also, discuss potential approaches to study vulnerabilities and threat realization to proceed towards tentative solutions for mitigation. This paper will analyses recent researches to address this issue and discuss their strength and limitations.

Keywords—healthcare devices, cybersecuirty, threats

I. INTRODUCTION

Recent healthcare technologies provide plethora of benefits in terms of extending healthcare services to remote level, enhancing medical decisions and using more personalized treatments based on real-time data collection (Ahmed et.al 2019). It includes integrated healthcare information system that store electronic health records, implantable smart devices, monitoring devices, telehealth technology etc (Coventry et.al 2018). The integration of smart medical devices, mobile applications, central systems and networks has become a necessity for medical sector. Currently, at least 10-15 devices are connected to each hospital bed in America (Coventry et.al 2018). These interconnected devices range from insulin pumps, heart monitors, pacemakers, cardiac, neurological implantable devices etc.

Though interoperability of these technologies is bringing promising changes to healthcare sector, it poses critical challenges in terms of cybercrimes. The medical wonders associated with these devices has made the world to trade-off security and data integrity. Mainly, security breaches of any sort could lead to life-threatening consequences. The connected systems exchange information leading to increased exposure and vulnerability to security breaches. Here, it is pertinent to understand the nature of these security breaches, which includes, corruption of patient's data, inserting malicious code to implantable devices, manipulating monitoring data, modification of day-to-day patient data by cyber intruders, resulting in wrong decisions, misleaded medication and treatments (Mcleod et.al 2018). Although, healthcare has same security risk vectors like other sectors, yet the impact is more dangerous. The prevention of cyber-attacks in medical technology is hard and incurs significant amount of investments.

Evidently, by the emergence of these technologies the security risks and cyber security management were given considerable attention. However, cybersecurity management specifically in medical sector is not suffice and has already led to serious attacks (Coventry et.al 2018). Recent advancements have transformed devices into individually running information systems containing embedded operating systems, communication mechanism to make them operatable in non-medical environments (Sametinger et.al 2015). It allows easy access to transmitted data making it a prime vulnerability. Cyber agents can use them as a medium to initiate attacks of more compromising nature. The most suitable example is of former U.S vice president Dick Cheney, who had to replace his wirelessly connected implantable cardioverter defibrillator with another electromechanical device (Camara et.al 2015).

In order to prevent cyber intrusions and protect sensitive data it is important to develop security countermeasures, in the interim patients' safety is under serious threat. This paper strategically frames this issue to identify exploitable vulnerabilities and factors significant for proposing tentative solutions. The rest of the paper is organized as follows: section II explains adopted research method, section III illustrated study purpose, followed by literature review in section VI, section V represents method review and finally conclusion in section VI.

II. RESEARCH METHOD

In this paper, a structured qualitative analysis research approach was utilized. This method enabled a precise exploration and multifaceted description of the issue under study. Also, it allowed to understand the severity and urgency of the problem. Firstly, research combinations were developed based on stated keywords at the start. IEEE, EBSCO and ScienceDirect were three main databases selected based on the advanced and precise search parameters offered. The timeframe was limited to 2015-2019, as cybersecurity is a field with constant changes and previous work was opted out to enhance reliability and up-to-date insights. The results yielded a huge volume of articles , that were first screened on basis of

peer-reviewed criteria then further screened out based on the relevance of abstracts Peer-reviewed articles are more reliable and unbiased. At the end, seven articles were finalized which precisely served the purpose of this paper.

III. Motivation

Recently, major cybersecurity incidents took place that affected general public, hospitals and medical institutes. On analysis it was revealed that adverse events have increased in number over the years and 90% reports have notified devices' exploitation (Sametinger et.al 2015). There were 351 security breaches reported in early 2017 (Mcleod et.al 2018). The most popular cyber-attack is "Ransomware", it is a method of encrypting data for extortion of money also called digital blackmail (Ahmed et.al 2019). A similar attack was launched called "WannaCry". Other attacks, like pacemaker hacking, corrupted patient information, disabling incidents of critical devices pin down the significance of framing these problems, deeply study the targets to identify threat vectors and explore possible counter measures. Similarly, in Stine et.al (2017), authors narrated a report published by authorities stating how x-ray machines or blood gas analyzers are being used to access medical networks. By reviewing recent incidents, there are specific key elements that needs to be considered. First and foremost, why is medical industry vulnerable? What are the motives behind these cyber-attacks? Also, it is important to identify nature of these attacks and their intensity. Furthermore, what role does authorities play? Based on these discussions further research can be carried out on how can cyber resilience be achieved for healthcare to move forward?

IV. Related Work

A. Healthcare Sector Vulnerability

In medical perspective, majority of the technological advancements were focused on optimizing treatments. Little attention was given to the possible risks associated with it. Though, security frameworks exist, there are several factors that complicate managing cyber security in healthcare sector. To enable easy access to patient's daily progress and medications or symptoms, health staff is provided with minimal authorization access to the devices, that are operable in open environment (Coventry et.al 2018). It makes them vulnerable and traceable. To enable remote medical care, constant monitoring via smart devices work as pivot point for attackers to access main hospital networks. Similarly, with vast adaptation of mobile applications and their integration to a central medical system increases risks of breaches (Ahmed et.al 2019). Moreover, the software used are unresponsive to the life-long changing landscape of cyber threats. The attacks are becoming more sophisticated that existing security protocols are unable to cater them.

Furthermore, the employees are under trained to operate smart technology and identify susceptible activities. Moreover, by the integration mobile applications accessibility has been extended to external environmental and these transmissions can be easily manipulated.

B. Motives of Cyber-Attacks

It is understandable to why cyber agents attack industrial or governmental networks but the motivation behind targeting medical sector is shocking. Main reasons are financial and political gain compromising national security. Moreover, stolen patient data can be used as false identity to use for fraudulent insurance claims or to sell drugs illegally. The stolen identities can be used to open bank accounts. To summarize, cybercriminals could use this data and networks to intrude into further secretive networks, for many diabolical reasons.

C. Potential Cyber-attacks to Healthcare

The reported attacks in literature are classified as internal and external, which can further be categorized into direct and indirect based on the source and impact (Luna et.al 2016). In internal threats, employees, defective equipment are counted as direct threats. The direct threats identify a target to exploit and is posed in straightforward, explicit way. While, indirect threats are harder to trace because they are posed on a weak point and real motives are masked. In internal threats, the main threat agents are weak central system that can be accessed through serial ports, connected devices etc. On the other hand, external threats can be classified as conditional threats, where systems are directly targeted to access, modify and manipulate data with intended extortion (Camara et.al 2015).

Ransomware as well as hacking are the most popular kinds of cyberattacks, in 2017 cyber intrusion called WannaCry hacked computers in eleven different countries, locking millions of patient data in exchange of bitcoin ransom (Ahmed et.al 2019). The denial-of-service is one the most crippling cyber-attacks, also known as malwares. A UK medical institute suffered serious consequences when an unknown malware was injected into the system resulting in disrupted services, cancelled operations and appointments (Luna et.al 2016). Another observed attack is called Medical Device hijack, in which a malware is added into a device. This is an example of an external indirect threat that uses diagnostic equipment, life supporting equipment, infusion pumps etc as weak links to enter hospital network and spread across the entire system without being detected. Furthermore, it could be intended to critical infrastructure failure. Despite a comprehensive discussion presented in these articles, cyber threats must be studied in a technical sense to explore more relevant solutions. One of the limitations in this paper is detailed study of cybercrimes themes, as it is beyond the scope of study.

D. Role of Regulations and standards

The regulation of medical devices is critical towards safety. Authorities have released a set of guidance for software developers and device manufacturers that included an element

security in it (Mcleod et.al 2018). Also, in 2014 another set of regulations were released for pre-sale device inspection to ensure the design has met cybersecurity standards (Luna et.al 2016). Similarly, on governmental level bills has been proposed to address this issue, special code of federal regulations was released by U.S government that cover the element of security of healthcare devices. In terms of device safety, FDA proposed three regulatory classes based on the security level required for different classes of devices. If high risk is associated the device's design shall abide regulatory class III (Sametinger et.al 2015). Moreover, WHO suggested that in order to enhance security risk management frameworks must be implemented (Sametinger et.al 2015), which includes explicit risk analysis during manufacturing and after sale monitoring stage. However, the covered literature was confined to the regulations proposed in America and little information could be found on other countries.

E. Tentative Solutions

It is imperative for experts to develop a profound cyber security management for healthcare sector. Of course, it cannot be completely countered but it is important to develop resilience. In Coventry et.al 2018, authors suggested to enable periodic software updates, detection process and basic cyber-maintenance steps to maintain integrity and safety. Cyber security management should be a vital part of medical devices and systems. They suggested that a cultural change is required to add security into patient care protocol. However, the proposed solutions are too generic, and question arises that cyber security management is a key part of product lifecycle that has been practiced for decades but still healthcare is vulnerable, why? It is suggestible that existing cyber security management metrics or frameworks are insufficient to handle today's more sophisticated cyber-crimes. On the contrary, authors provided a commendable cultural change solution that will allow re-evaluation of current medical technology and behavior of medical staff and patients towards it. By identifying cultural inefficiencies, it will provide a holistic approach towards security management. In Stine et.al (2017), authors discussed various risk management frameworks like, NIST, that have the potential to develop resilience. Similarly, authors in Mcleod et.al (2018) emphasized on risk management and government regulations. Moreover, in Ahmed et.al (2019), researchers further explained the cultural element stating that security culture of hospitals must be revised special staff trainings were suggested. These solutions will be further discussed in next section along with provided mechanisms in chosen articles. One major factor missing was architecture of the medical devices. These are IOT enabled devices and designed with low power capacity and limited storage memory to enhance their efficiency. It is important to consider technical factors and evaluate effectiveness of existing solutions.

V. METHOD REVIEW

Research is a formal approach towards finding facts and answers by collecting and analyzing data to extract structured information for explicit understanding of a problem or requirements in a field (Paul et.al 2015). In this area of study, most suitable methods are exploratory qualitative study and experimental study. In this section, three main methods used by researchers will be discussed.

A. Qualitative Content Analysis

In Luna et.al (2016), authors adopted a rigorous systematic method to document themes of potential threats and provide a comprehensive structure to facilitate future research works regarding cybercrime. They used EBSCO host, PubMed and ScienceDirect databases. They adopted a query-based approach to find specific literature on selected databases using different combinations of search terms. Also, the research was prioritized to peer-reviewed articles only. Moreover, the research scope was limited to US-based studies and within the time frame of 7 years (2008-2015). Finally, 19 selected articles were reviewed by each member of the team. Afterwards, they developed an abstraction representing internal and external threats. The results showed that major threat to healthcare was data breaches either directly or indirectly. They concluded that security measures are a necessity for the medical sector due to the sensitivity of this situation. Authors mentioned that based on the identified threat themes existing security measures implemented are insufficient to cope up with these threats.

To summarize, paper provides a starting point for research in cybersecurity risks for medical sector. Also, main limitation mentioned by authors was the size of sample data. To further illustrate, this study was focused on medical cyberthreat issues within U.S, whereas the technology infrastructure and its maturity level varies in developed and developing countries. The nature of threats could be more than what they identified in this paper. Another limitation was in the selection of search terms, that were, "privacy", "security" and "crime". The present medical services work in IOT environment, and this term should have been part of the research.

In Coventry et.al (2018), they conducted a narrative review. Firstly, they developed research questions covering main elements related to the topic. Afterwards, they used PubMed database to find articles using keywords "cybersecurity" and "healthcare". Authors applied a timeframe of six years. They used references of collected articles to expand their research. Finally, articles were filtered based on their abstracts by the main researcher. They used the final collection to find answers with concrete arguments and evidence for their research questions. From the findings they concluded that healthcare technologies will turn into murder weapons in near future.

The research method is commendable as it was more structural as compared to other previous study. However, the screening

was performed by one member hence making reliability of collected questionable.

B. Scenario-based Research

Authors in Sametinger et.al (2015), conducted a scenario-based research. They used an illustrative example of pacemakers to develop understanding of factors associated with cybersecurity of medical devices. Moreover, they conducted a risk assessment on pacemaker to distinguish between various risk elements and degree of vulnerability with each element. Finally, they identified key challenges associated with developing security countermeasures. They further classified these discussions based on challenges associated software security and hardware security. Furthermore, they discussed non-technical aspects, like, security awareness adopting countermeasures. This study was limited to the analysis on pacemakers, there is no surety whether it is generalizable in case of other kinds of devices used as design and functionality varies.

On the contrary, in Camara et.al (2015) conducted a study on security issues associated with implantable medical devices (IMDs). Authors identified factors used to analyze security mechanisms in terms of their compatibility, advantages and pitfalls. They studied four types of IMDs, that includes, cardiac devices, neurostimulators, drug delivery system and cochlear implant. They highlighted main adverse events associated with each type. These events refer to the consequences of attacks, like, heart failure, injury, deafness, serious neuronal effects etc. Afterwards, authors explicitly discussed devices' usage scenarios. In these scenarios they identified the involved entities, interactions between these devices and medical systems. Furthermore, threat model was used in which they highlighted six main security threats against security constructs. Like, authentication, integrity, confidentiality, authorization and availability. For instance, denial-of-service is related to "availability" where battery is drained, or they are remotely switched off. Furthermore, they discussed the types of cyber attackers
Authors highlighted the limited capabilities of these IMDs, that includes, energy, storage and computing capabilities. The most commendable element in this study, two identified operational modes of IMDs; emergency and normal mode. For instance, in normal mode time-consuming authorization can be used, while, in emergency medical personnel require quick access to the device and these security requirements could risk patient's life. Therefore, these trade-offs are essential factors to be considered in designing security frameworks. Finally, researchers proposed some tentative solutions to protect medical services in terms of advantages and challenges associated with each solution. This study was a true justice to its title, it undoubtedly gives a comprehensive discussion.

C. Experimenal Study

In Mcleod et.al (2018), binary logistic regression was used to assess a security breach factors model. They developed hypothesis to study relationships between exposure, security level and organizational factors with occurrence of data breaches. Data was collected from Healthcare Information and Management Systems Society (HIMSS) database and from Department of Health and human Services (DHHS) data breach reports, using SQL queries. This study is focused on cyber-attacks in U.S. The authentic sources justify the reliability of sample data. The dependent variables were occurrence of breaches. While independent variables were level of security, exposure and organizational factors. These variables were constructed based on Swiss Cheese Model (SCM), which suggests that each adverse event can lead to multiple failures. They studied relationships of independent variables with dependent variable individually and collectively. Furthermore, they used a 20% cut-off for filtering variables with missing values. As, variables with missing values are prone to errors hence, hindering accurate results. Then, they used three sets of values, original data values, estimated data values and finalized data values They calculated differences in each set's mean and standard deviation. This way they came up with cleaned and reliable dataset to examine the model. They applied a box-tidwell method to test that independent variables were linear to dependent variables, if the resulting value was greater than 0.05 it verified the linearity. The results showed significance of these factors in data breaches proving their developed hypotheses. However, authors mentioned that hypothesis-based testing involves greater number of variables increasing the risk of errors. Also, the reporting requirement in DHHS database resulted in excluding small breaches, hence the breaches were underreported.

In Stine et.al (2017), authors proposed a risk scoring system to assess the impact in case a device was compromised. The assessment relies on data collected from security questionnaire designed on the concept of STRIDE model. In this model, each possible threat is associated with a security property as explained by Camara et.al (20150. Main assessment objectives were to simplify threat assessment process in a cost-effective and accurate way by providing easily understandable results. The proposed assessment system has two key aspects. First, study adversaries in case of a medical device being compromised. Second, evaluation of the security level of device. They used list of potential adverse events provided by SANS institute. Authors highlighted that in order to generate error-free results it is important to reduce the number of categories used in assessment. Therefore, they used five main potential events. They used logical progression to list potential diagnostic outcomes of the device. Finally, they used a decision matrix to record values. Also, they developed scaling system based on outcomes' severity. Furthermore, the test was conducted on four different scenarios. For example, a medication delivery device with network abilities and remote

connection. The assumption was that delivered medicine was life-threatening if improper dosage was taken. Authors developed a base score equation and used scale system results to calculate a base score for the outcomes. The final value was 9, which infers that this device prone to risk and must be moved to second phase of scoring system that is to check security capability. As suggested by many authors, risk assessment is a critical part for security countermeasures and the proposed scoring systems is a commendable contribution in this regard.

VI. Conclusions and Future Recommendations

It can be concluded that many commendable attempts have been made to develop deep insights to this problem and propose ways to optimized cybersecurity in healthcare. However, these practices are exhaustive and costly.

Although, the countermeasures are not cost-effective but for safety sake they are crucial. To optimize the research, it is suggestible to explore the concept of digital forensics in cybersecurity management. It is a broad term referring to monitoring, detecting, recovering and preserving digital systems and cyber networks. It provides a longitudinal approach towards developing cyber resilience. This need to further study in terms of technological aspects of healthcare devices. It means whether embedding digital forensics readiness could affect functionality of devices in terms of power usage and computing limitations? To what extent, forensics can preserve data, detect attacks and responsiveness towards threats?

Word count: 3506

References

[1] Ahmed, Y., Naqvi, S. & Josephs, M., 2019, 'Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems, *13th International Symposium on Medical Information and Communication Technology (ISMICT), IEEE*, pp. 1-9, viewed 31 August 2019, < https://ieeexplore-ieee-org.ezproxy.lib.swin.edu.au/document/8744003 >

[2] Camara, C., Peris-Lopez, P. & Tapiador, J.E., 2015, 'Security and privacy issues in implantable medical devices: A comprehensive survey', *Journal of biomedical informatics*, vol.55, pp.272-289.

[3] Coventry, L. & Branley, D., 2018, 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward', *Maturitas*, ScienceDirect, vol.113, pp.48-52.

[4] Luna, R., Rhine, E., Myhra, M., Sullivan, R. & Kruse, C.S., 2016, 'Cyber threats to health information systems: A systematic review', *Technology and Health Care*, vol.24, no.1, pp.1-9

[5] McLeod, A. & Dolezel, D., 2018, 'Cyber-analytics: Modeling factors associated with healthcare data breaches',*Decision Support Systems*,ScienceDirect, vol.108, pp.57-68.

[6] Sametinger, J., Rozenblit, J.W., Lysecky, R.L. & Ott, P., 2015, 'Security challenges for medical devices', *Communications of the ACM*, EBSCO, vol.58, no.4, pp.74-82.

[7] Stine, I., Rice, M., Dunlap, S. & Pecarina, J., 2017, 'A cyber risk scoring system for medical devices', *International Journal of Critical Infrastructure Protection*, vol.19, pp.32-46.