Cyber threats to health information systems: A systematic review

D. Pradeep Sudeep

Research Scholar, Full-time PhD, Andhra University

ABSTRACT

The cyber world is a network of connected computing environments and technologies. The entire world is now connected to cyber and using the services of cyber-security. Healthcare is a department which requires a lot of attention while it is used in securing the data of the healthcare provider or patients. Misuse of patient data can lead to high vulnerability and data theft. This particular paper presents a systematic analysis which deals with the modern-day cyber-security breaches of healthcare and conventional approaches utilized to solve them. In modern days, healthcare technology has a huge potential to enhance the clinical outcomes but security is a prime concern due to rapid increase in theft. It is recognized like an attentive goal of cybercrime due to these three different reasons such as: rich valuable data with less defensive approaches, ransomware attacks and attacks on medical devices. The breaching of medical data reduces trust of the patient and also threatens the patients due to crippled health care systems. Legislation rules and regulations are required to cumbersome the cyber-security attacks by considering healthcare, an integral part of the system. In addition, appropriate risk management processes are required to be incorporated in the healthcare system to prevent the data from cyber-attack.

1. INTRODUCTION

The terms used frequently in this sense at the start of the millennium would be "Computer Security," "I.T. Security," or "Information Security." While these words had nuanced distinctions recognized by experts operating in this room, they were tangible enough to be relevant to the broader population. There could be general discussions and schemes depending on widespread knowledge of what these words mean [1].

In computers and computer networks, an attack is trying to disclose, modify, hinder, destroy, steal, or achieve illegal access to or make use of an asset with any legal permission. A Cyber attack is an aggressive strategy aimed at securing data systems, services, and infrastructure, computer systems or personal server equipment. The term attacker can be defined as an individual or process who, possibly with criminal intent, tries to access information, features or other limited system regions without permission. It is completely depends on the circumstance; cyber-attacks can be part of cyber-warfare or cyber-terrorism. A cyber attack has an ability to use at national and state level any one person, group of people, society, or organizations. A cyber-attack possibly will be initiated through an unidentified resource [2].

A cyber-attack can rob, change, or ruin a designated destination by logging into a vulnerable system. Cyber-attacks can variety from placing spyware on a personal computer to trying to ruin all countries ' facilities. Legal specialists aim to restrict the usage of the word to events that cause physical harm, distinguish it from more routine data beaches and broader hacking activities.

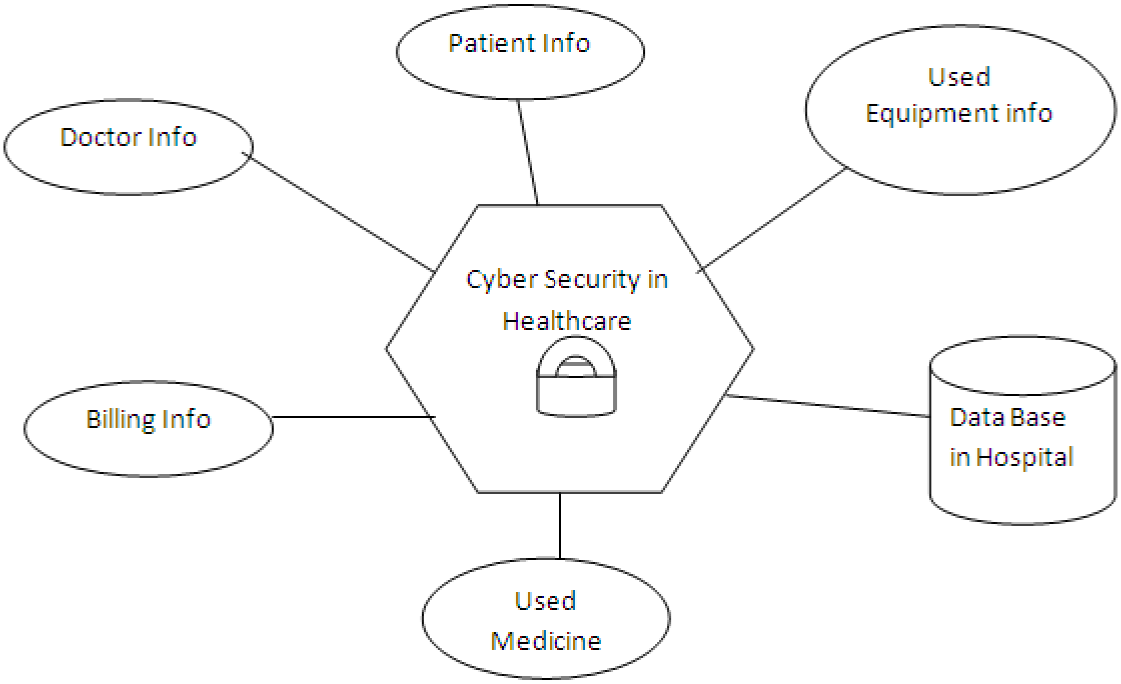

Fig 1.1: Security Threats in Health Care

1.1 Cyber Threats in Health Information system

Electronic healthcare technique is widespread all over the world and generates enormous potential for improving clinical outcomes and are responsible for the delivery of transforming. Though, they involve growing worries about the safety of healthcare information and equipment. Increased interconnection to current computer platforms has exposed medical equipment to new security holes to cyber-security. For two critical reasons, healthcare becomes the very attentive destination for cybercrime: it contains huge amount of valuable data, and its defenses are not strong. The security hired in cyber breaches involving theft health information and ransomware assaults on clinics and may include assaults on implanted life. Ultimately, cyber-security is essential to patient safety but it has in the past been careless. New laws and rules are in a position to promote transition. This makes cyber-security a necessary factor of patient safety. Changes in animal conduct, technologies, and procedures need a portion of a holistic approach to medical devices. Violations can minimize patient trust, disrupt health systems, and try to intimidate human[3].

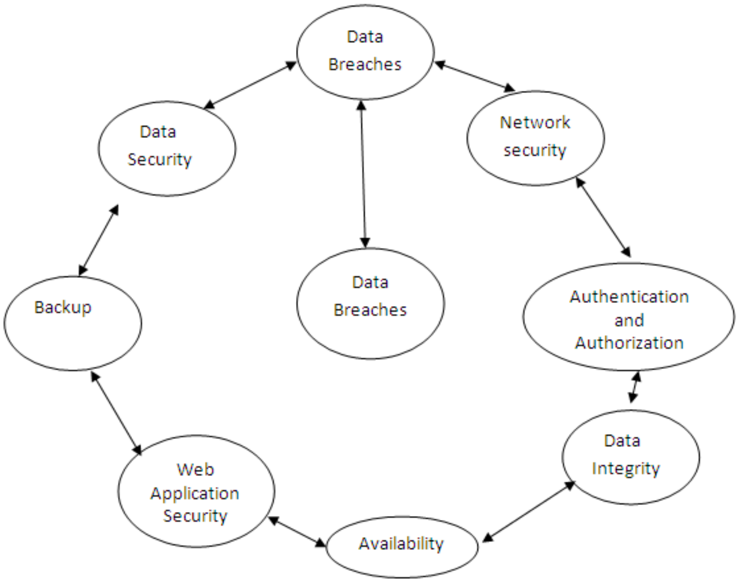

Fig 1.2: Data Breaches in Cyber security

Healthcare becomes mainly focused industries among various famous technologies at the moment. Reports show the development of assaults and the increase in the theft of medical identity— with millions of medical documents robbed worldwide. Breaches may arise from hacking, malware, and threats to insiders. The term hacking is explained as not allowable access to a computer system to grow information and it may become the cause of disruption. Malware ("evil code") relates to programs intended to penetrate pcs without user permission and involves dangers such as viruses and ransom ware. Hacking is described as illegal way to access data from computer devices to retrieve information or to be the reason of disruption. Malware ("evil code") relates to programs intended to penetrate pcs without user permission and involves dangers such as viruses and ransom ware [4].

As healthcare systems proceed to develop, so is their interconnectivity. While traditionally separately, many are now incorporated into the hospital network. There are presently 10–15 linked appliances in U.S. clinics per room. Interconnection has many advantages— e.g., effectiveness, decrease in mistakes, automation, and distant tracking. These advantages transform the therapy of both acute and temporary long-term circumstances. Interconnected technology outside the clinical environment allows health professionals to monitor and adjust embedded devices without the need for hospital visits or invasive procedures. EHRs can enhance customer welfare by creating health information more widely accessible. Unfortunately, interconnection presents new vulnerabilities to cyber safety [5]. Cyber-security is about protecting computer networks and information that cause disruption, it may be unplanned or meaning-less disruption. There are increasing issues that cyber-security in Healthcare is not adequate, resulting in the absence of confidentiality and data security in health information.

1.2 Needs of Security Threats in health

In general, individuals believed that no one was encouraged to attack healthcare systems and that safety steps were not essential. There is no internet security insurance organization. Traditionally, the focus was –and understandably so –on the therapy of nurses. Several issues due to which cyber security becomes complicated and enhanced sensitivity over time are:

- The increase in wired or linked technology used to offer well-organized techniques for patient treatment, particularly under severe conditions. This provides different techniques for connecting medical devices. Easily accessible devices often increase the likelihood of being found by perpetrators.
- A specified device could provide a potential entry location for more extensive patient networks bypassing the firewalls. There is also an inclination to be a momentary delay between an attack and recognition of violations, helping to increase sensitivity further.
- More focus on keeping customers secure and adding more continuing customer surveillance outside the clinical setting. More tools used in the broader healthcare setting improve the risk of breaches.
- Mobile customer phones (e.g., smart phones) are commonly used; making it challenging to protect environmental documentation from the potential dangers presented by public-purpose systems [5].

2. METHOD

2.1 Reason for Targeting Healthcare:

Although Healthcare involves the vulnerabilities to make use of, attackers need to be inspired to continue with the attacks. The inspiration involves the capacity for economic and political benefit and possibly taking life in the type of cyber warfare. Financial knowledge is the strongest part of these inspirations. Healthcare data considerably needs to kept more secure as compared to the any other data. The valuation of a complete collection of health check testimonial could be higher than$1000. Stolen medical identities can be used by assuming someone's identity or insurance credentials to obtain healthcare services and prescription medication. Uses apply to advanced organized crime theft.

In recent years, by filing fraudulent allegations and selling drugs on the dark web, fraudsters have gained billions. There is even enough documentation in health information to generate new accounts on bank, secure loans, or obtain passports. There is also political value in the information contained inside the health organizations. Such as, the Anti-Doping Agency of World was targeted, and the documents of influential athletes were made public. Huge numbers of people access NHS websites, making them the main website for authoring propaganda, e.g., NHS websites have been hacked by cyber terrorists and images of the Syrian civil war have been uploaded. Over the previous century, we have seen countless journals talking about the opportunities for medical devices to be used as a portion of a global cyber war strategy. National state performers could interrupt Healthcare in a foreign nation by preventing access or prosecuting people through their medical equipment, or by collecting sensitive information. Those with cyber security abilities enjoy the challenge of identifying and exposing security vulnerabilities in networks and medical equipment. For example, in 2016, an individual security vulnerability scan was able to obtain a database containing information from persons enrolled with the Australian Blood Donor Operation. In short, Healthcare is aimed because of the capacity for economic or political profit, or to reveal vulnerabilities by cybercriminals, bug militants, and political leaders [6]

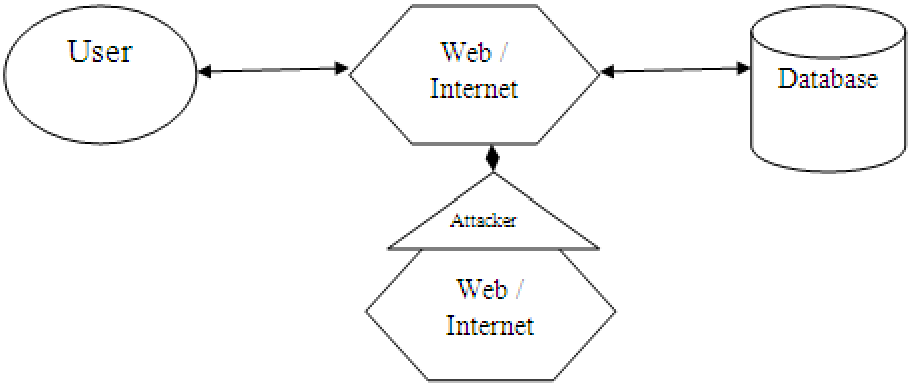

Fig 2.1: Attack on User-Database

2.2 Current scenario in health care cyber attack

As of 2015, hacking has become the leading cause of infringements of health data. Malware, including ransom ware, is also a problem. Hackers proceed to bring the benefit of strict safety to rob medical health records, refuse access to insurance facilities, or trigger deliberate damage. Over the previous few years, the health industry has seen a drastic rise in the amount and magnitude of information breaches. Violations lead to economic failure, loss of credibility, and decreased patient safety. In Australia, every citizen's medical card amount is allegedly for purchase through the dark web. The average price of each medical record lost or taken containing private and sensitive data as $380 has been reported recently. Continued advertising connected with significant breaches may jeopardize nurse confidence, leading to less readiness to disclose information. This is especially difficult for clients with stigmatic circumstances such as circumstances of male or mental health. The scale of the 2017 WannaCry assault was unexpected despite providing notices and accessibility of security patches (many not mounted). WannaCry effected greater than 300,000 computers devices throughout the world requiring users to pay ransoms by bitcoin.[8]

In linked machines like MRI which are used as scanners and water holding refrigerators, fifty U.K. clinics and other countries encountered system-wide lockouts, errors in-hospital treatment, and reduction of the feature. This assault was not explicitly aimed at healthcare organizations, but the harm was prevalent. This assault was not explicitly aimed at healthcare organizations, but the harm was prevalent. While the U.S. press discussed the situation of Medical Center of the Hollywood Presbyterian closed down for 10 days until it received a ransom of $17,000.

The Act in 1996 of U.S. Health Insurance Portability and Accountability (HIPA) introduced safeguards to guarantee the protection of individual electronic health information. The Security Rule needs protected companies to keep adequate and sensible administrative, technical, and physical safeguards to guarantee the confidentiality, honesty, and accessibility of EHRs that generate, obtain, retain, or communicate. Also coming into force in the U.K. in May 2018 is the upcoming General Data Protection Regulation (GDPR). The GDPR aims to complement the privacy of data rules in all over Europe to safeguard against information breaches and privacy. The GDPR seeks to achieve this by resolving differences in the present legislation published in the 1990s before organizations carried vast electronic information. The GDPR refers to all private information retained by an organization. A portion of the new legislation, all infringements that may pose a threat to the liberties and constitutional rights of citizens must be recorded to the Information Commissioner's Office (ICO).Health information breaches would probably fit into this class. Therefore, they will need to be notified to the ICO around within 72 h of the infringement happening[9].

Non-compliance risks fines of up to € 20 million. Other modifications include the need for all procedures to have a data protection agent and the implementation of additional ' transparency and precise handling ' legislation to be included in patient privacy reports. This recent legislation will considerably boost the price of infringements (owing to penalties introduced) and may assist raise understanding of privacy issues and the need for enhanced cyber security. As the NHS progresses towards its aspiration of EHRs, there are worries regarding the privacy of patient and approval and information exchanging with other organizations.

Patients must be provided a choice as part of the domestic data opt-out system to opt out of sharing their information for purposes other than their care. Under the GDPR, any request for data from an external organization, including the purpose of requesting the data, must be made in a clear and easily accessible language. This will enable clinicians to maintain information preferences of patients. That being said, it has been suggested that infrastructure modifications are necessary before EHRs become a helpful fact. For instance, two laboratories can evaluate the same thing using very distinct scales owing to the NHS using distinct suppliers and distinct systems; making it hard for two distinct laboratories to share information in any significant manner. As far as medical devices are concerned, the U.S. Food and Drug Administration (FDA) take liability for cyber-security involving product of the medical manufacturers. The FDA has released pre-market and post-market rules containing suggestions for managing cyber-security hazards of medical devices on the complete life cycle of items. This involves promoting individuals to disclose cyber-security problems and rendering it compulsory for producers and computer customer equipment to record any computer malfunction if it presents a safety danger [10].

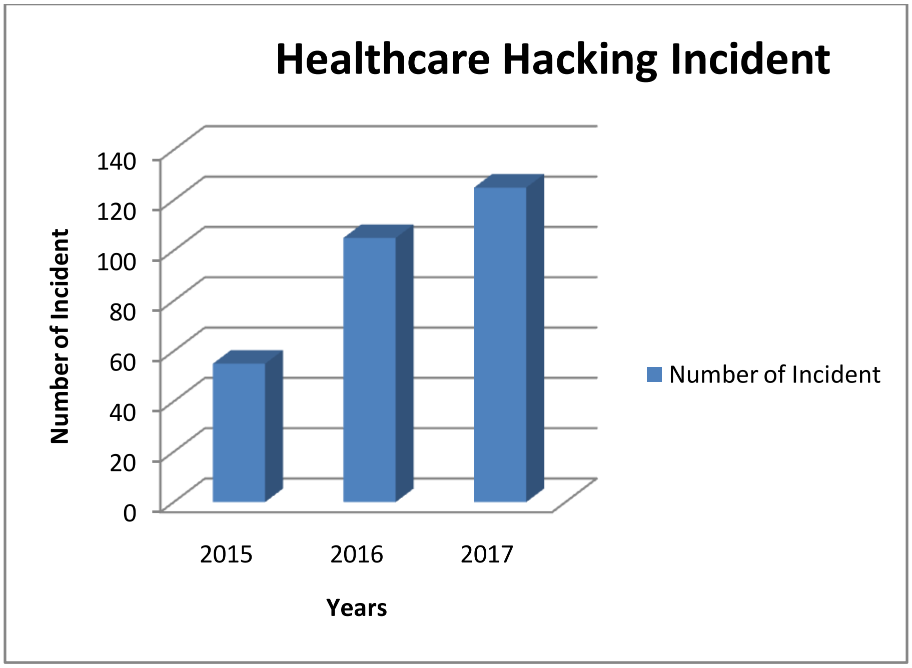

Fig 2.2: Number of Incident occurs in the recent year [12]

S. No	Author	Method	Description
1.	Gibbs ad M (2018)[6]	Proposed detail information about the National Health Services information system and also suggested different security threats in the health care field.	NHS enforce a password policy that users must have to create passwords at least eight characters in length, as well as forbidding any NHS-managed computer to run password cracking tools.
2.	Dodel et al. (2017)[7]	Proposed a Health Behavior Model in which the perceptions regarding accusations and perceptions of conduct as the primary determinants of preventive behaviors related to health.	After different simulation on the security threats concluded that the user who uses different protection system to protect their personal computer is difficult to attack by the security threats and it has higher efficiency than others
3.	Rathod et al. (2018)[8]	Proposed a novel electrocardiogram protectionmethod which used the Legendre approximation attached with multi-layer perception model for the protection of data with the help of three levels of security for data.	After the simulation on the proposed electrocardiogram protection technique, the outcome shows efficiency is about 99% for the security threats.

4	Seyed Mostafa Safavi et al. (2018)[9]	Proposed the uprising block-chain technique that can add to these elements and how its components can help Healthcare develop safely.	Due to the presentation of the massive amount of information and records, it needs to ensure security and privacy. In this, they showed block-chain based solutions and its critical towards make home in future and care about health on the basis of ideal framework.
5	N.Komo et al. (2019)[10]	Proposed an upgrade of the NIST cybersecurity method which is used to create a hybrid security framework for the security of Healthcare.	The suggested hybrid security framework are IoMTs endpoint software, which is highly used in a different country for the protection of the security attacks in Healthcare with a high accuracy rate and efficiency.
6	Jaime et al. (2019)[11]	Suggest an Onion router and a block-chain structure for the security enhancement of the cyber attacks in Healthcare	Detailed the information about the reason and the security framework for the protection of Electronic Healthcare Records(EHR) and also analyses the impact of the security attack on the healthcare organization.

3. How can the healthcare sector move forward?

There is no 100 percent efficient method to avoid all cyber-security breaches, but cyber-security must be a component of the risk management process, and cyber resilience must be assured. Cyber resilience is a holistic perspective of cyber danger that aims at culture, individuals, and procedures as well as technology. Several variables have been recognized as a way of improving the environment: at least, basic cyber hygiene must be preserved, see the 10 measures from the National Cyber Security Centre. This involves periodic, safe backups (vital for maintaining resilience and being prepared to restore rapidly if assaulted) and maintaining software up-to-date to guarantee security patches are in location. It is necessary to maintain confidentiality [9].

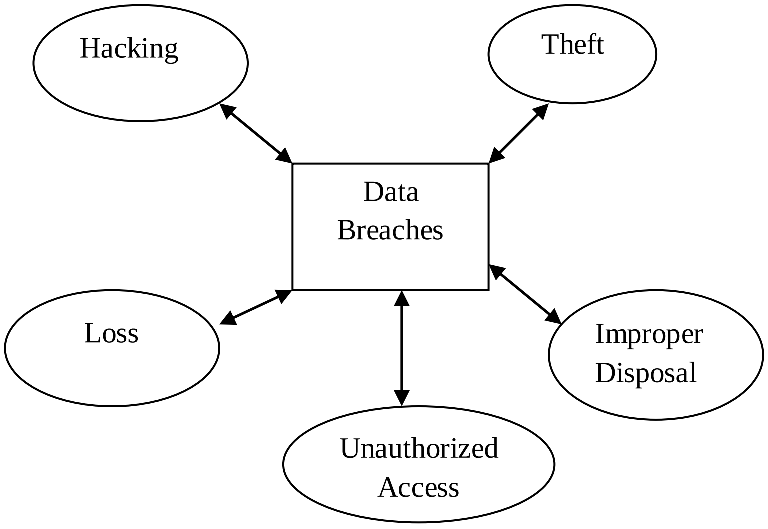

Fig 3.1: Data Breaches

This can be accomplished by anonym zing data (including pictures), removing patient identifiers when used for study reasons, and restricting entry to internet patient information. This needs investment in technologies and procedures that promote safe information transition (e.g., e-mail processing and internet information security).Security must be a vital component of the lifecycle of the item. This involves contemplating from the outset the trade-offs between safety and other conditions.

Appropriate benefits should ensure that prospective devices and networks have strong safety from the beginning and that they are not eventually placed in a' bolt on' fashion. This could be driven by safety standards for information management that take into consideration the unique healthcare context that remains to prioritize accessibility over confidentiality. Any standards, regulations, or instructions must relieve the pressure and prevent staff from being encouraged to engage in unsafe workarounds.

Cyber-security should be a significant element of hospital therapy culture as it is essential to substitute simple and insecure processes with more secure, significant techniques. This means not only being seen as secure (for example, complying with laws) but also building security into the culture. This may involve sufficient checks and implementation by certified organs. The traditions has been changed necessary from the top to down, and the metrics be supposed to be applicable using the Commission of Care Quality or identical to ensure active engagement. Efficient security culture can improve staff working as a' natural firewall' that can assist safeguard electronic property. This involves employees not being registered here like a superintendent of domain; no exchanging of login qualifications, and periodic personnel preparation to convey the hazards posed by inadequate safety behaviors and how safety can be achieved without compromising customer treatment. More advanced safety logins (e.g., retinal processing, fingerprints, facial recognition) may be used to avoid the exchanging of logins and passwords. Security staff training is also needed.

Cyber insurance is a quickly increasing company with projected worldwide revenues of $7.5 billion by 2020. With the profits connected with cyber breaches, more businesses are switching to insurance. Suitable insurance rewards can motivate security changes. Protection against the effects of cyber-attacks can be a component of the liabilities insured against, just as clinics are insured against criminal negligence allegations.

CONCLUSION

Healthcare technologies are prevalent in nature and provide a better role in securing the people lives. But, due to increase of cyber-attacks, healthcare systems are vulnerable to security. In this paper, a systematic review has been presented for the cyber-security attacks on healthcare industry. The current scenario of cyber-attacks in the industry of healthcare becomes the reason to provide and description of existing protection methods to secure the healthcare industry elaborated well. The cyber-attacks are common and focused on breaching the healthcare information due to large amount of information which is valuable and sensitive. However, if the healthcare information has been attacked then human lives may be at risk. Thus, an attack could be a loss of functioning components within intensive care departments. There are still no efficient methods developed which securely avoids the cyber attacks. Therefore, various risk management processes has been introduced to enhance the security level and reducing the vulnerability of cyber-attacks.

REFERENCES

[1] Nkomo, D., & Brown, R. (2019). Hybrid Cyber Security Framework for the Internet of Medical Things. In *Blockchain and Clinical Trial* (pp. 211-229). Springer, Cham.

[2] Coventry, L., &Branley, D. (2018). Cybersecurity in Healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, *113*, 48-52.

[3] Rathore, H., Fu, C., Mohamed, A., Al-Ali, A., Du, X., Guizani, M., & Yu, Z. (2018). Multi-layer security scheme for implantable medical devices. *Neural Computing and Applications*, 1-14

[4] Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., ...& American College of Cardiology. (2018). Cybersecurity for cardiac implantable electronic devices: what should you know?. *Journal of the American College of Cardiology*, *71*(11), 1284-1288.

[5] Anderson, S., & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?. *Computer Standards & Interfaces*, *56*, 134-143.

[6] Gibbs, M. (2018). Evaluating Cyber Threats to the United Kingdom's National Health Service (NHS) Spine Network. In Information Technology-New Generations (pp. 39-42). Springer, Cham.

[7] Dodel, M., &Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. Computers in Human Behavior, 68, 359-367.

[8] Rathore, H., Fu, C., Mohamed, A., Al-Ali, A., Du, X., Guizani, M., & Yu, Z. (2018). Multi-layer security scheme for implantable medical devices. Neural Computing and Applications, 1-14.

[9] Safavi, S., Meer, A. M., Melanie, E. K. J., &Shukur, Z. (2018, November). Cyber Vulnerabilities on Smart Healthcare, Review, and Solutions. In 2018 Cyber Resilience Conference (CRC) (pp. 1-5). IEEE.

[10] Nkomo, Danisa, and Raymond Brown. "Hybrid Cyber Security Framework for the Internet of Medical Things." In Blockchain and Clinical Trial, pp. 211-229. Springer, Cham, 2019.

[11] Ibarra, J., Jahankhani, H., &Kendzierskyj, S. (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. In Blockchain and Clinical Trial (pp. 115-137). Springer, Cham

[12] Health care cybercrime report https://www.hipaajournal.com/largest-healthcare-data-breaches-2017