Cyber Security threats and mitigations in the Healthcare Sector

Research · July 2022

DOI: 10.13140/RG.2.2.11552.05124

1 author:

Pasindu Bandara Aththanayaka
Sri Lanka Institute of Information Technology
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Cyber Security threats and mitigations in the Healthcare Sector

Aththanayaka P.A.G.P.B.
IT20021252
Computer System Engineering Department
(Cyber Security)
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it20021252@my.sliit.lk

***Abstract*—When conversing about cyber security involvement in any industry, there should be anything that is connected to a network which means an IoT mechanism. Internet of Things (IoT) is one of the biggest trends in the world at the moment. It has made life easier for every human in the world. Globally, IoT networks are growing rapidly as they connect billions of devices and exchange potentially sensitive information. The introduction of the Internet of Things (IoT) into the healthcare sector makes a great impact on the entire healthcare industry. The connection between the healthcare industry and IoT technology is referred to as H-IoT (Healthcare IoT). From the small wearable devices like step tracking bracelets to the large and complex programs like robotic surgeries, IoT has been able to create a large and positive impact on the healthcare industry. But as in every technology, there are some drawbacks in healthcare IoT as well. Since a lot of IoT tools and mechanisms are not developed concerning security measures, attackers can identify vulnerable targets and exploit them. Such exploits could affect devices and systems throughout the network. Latest solutions such as malware analysis systems can be considered as the technologies that are making effort to defend such kinds of situations to mitigate the threats against healthcare IoT. This review paper is concerned about the cyber security threats and mitigation methods in the health sector.**

Keywords— Cyber Security, IoT, Healthcare, Cloud Computing, Threats

I. INTRODUCTION

Over the last several decades, Global communication, connectivity between people, and the progression of technological development around the globe have accelerated rapidly. Although there are a huge number of advantages acquired and to be acquired from the novel technological appliances, there are numerous and significant drawbacks as well. DDoS attacks, Malwares, MITM attacks, and data theft can be considered as some of the major threats that arose based around the new technologies. According to the SANS Health Care Cyber Threats report, it requires billions of dollars annually to reduce such kinds of threats [1]. Furthermore, the healthcare industry is especially vulnerable to the threats which are associated with confidential information leakage. H-IoT (Healthcare IoT) devices collect health-related data and process with them to make decisions. These kinds of technologies are already in the healthcare industry and improving our daily lives. For example, a patient can wear a device with a sensor that has the ability to establish with other devices within a considerable range. Although these kinds of features are made for the healthcare professionals such as Doctors and nurses to get their patients' health records. The connection established between the patient's device and the other devices can be used by unauthorized people in order to monitor that particular patient's information such as the movement of the patient. Additionally to that attackers are also tempted to sell illegally collected health records to third parties. According to Riley Walters, 90% of health organizations are facing at least one cyberattack since the year 2012 [2]. The target of most of these attacks was medical records and billing systems. Health records are beginning to digitize can be considered as the main reason for this situation. The more health records are digitized, the more cyber-attacks will happen.

II. RESEARCH STATEMENT

It is no secret that the advancement of technology is doing a great service to the daily lives of all of us. It has had a positive impact on all industries and is doing a great service to the health sector as well. But with the advancement of technology, it is common for disadvantages to arise among its advantages. For example, while the new technology has the advantage of being able to computerize existing paper-based documents in the healthcare industry, the technology itself has greatly increased the risk of information being stolen. The Internet of Things, a new facet of technology, is making a significant contribution to the healthcare sector. At the same time, its disadvantages are increasing. The purpose of this review paper is to provide a detailed analysis of the adverse conditions affecting the health sector mentioned above. Further, the purpose of this article is to provide an in-depth analysis of the cyber security threats under the following subheadings.

- How IoT and SDN technologies are making an impact on healthcare industry
- Detected vulnerabilities in healthcare industry

- Potential threats to healthcare industry
- Countermeasures that can be taken
- Popular cyber security attacks happened in the healthcare industry

III. REVIEW OF THE LITREATURE

A. Usage of IoT in Healthcare Sector

The Internet of Things (IoT) is a new concept that emerging and spreading in the world at this moment [1] [2]. Basically, it is a collection of software, sensors, and other electronic components and networks that enables the creation of a connection between the physical and digital world. In healthcare Internet of Things which is known as H-IoT, is doing a significant set of tasks. Most of the H-IoT devices and the systems extract data from human bodies via sensors then send that data into servers utilizing the cloud computing features, and finally analyze the collected data using the technologies such as machine learning and interpret accurate information to the health care professionals' end. That end device can be a smartphone that enables health care professionals to make decisions in a short amount of time at a considerably low cost. In the near future, active healthcare internet of things connections will go high.

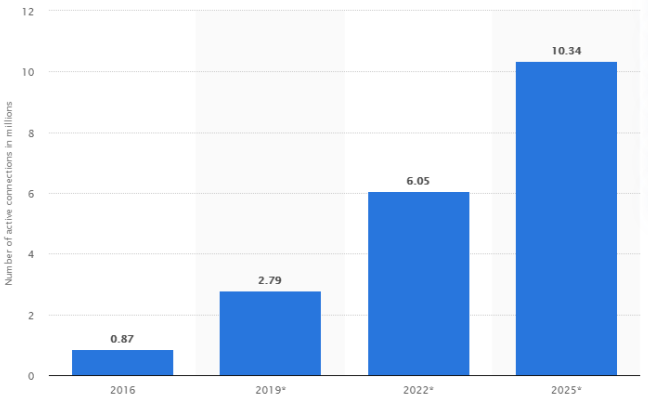

Fig. 1. – Number of predicted active connections

The increasing demand for IoT leads the healthcare industry to build smart hospitals to use IoT technologies. Internet of Things includes a set of unique and modern technologies like tracking, communication, wired and wireless transmission, and sensor identification [3]. The implementation of IoT can be a package of integrated devices. Famous consumer-oriented fitness tracks like the apple watch Samsung watch and Fitbit can be considered the best examples of that [4].

IoT already has a wide range of applications in different areas of the healthcare sector. In today's world, it is a bit difficult for everyone to meet a physician personally to have their regular health checkups. When considering elderly persons, it is well noticed that they often suffer from several diseases at one time. Therefore they might seek emergency healthcare services regularly. To solve that problem, the concept of pervasive healthcare was introduced [5]. Apart from that with the advancement of IoT technology, people are used to buying wearable devices to monitor their heart rate, ECG, and blood sugar level. It will allow users to count their blood pressure, oxygen saturation and other information about their body and this will help the users to early detect and diagnose diseases [6].

Fig. 2. – Architecture of wearable IoT devices

Due to the increment of chronic diseases, chronically ill patients including elderly people should be continuously monitored with proper diet plans and medicine management. Monitoring patients' actions using IoT is emerged with the concept known as ontology and fuzzy logic [7].

Telemedicine is another application of IoT which is proposed by the researchers for the patients' who are living in rural areas where they cannot easily reach the hospitals in a case of emergency. A mobile care unit which is known as the MCU is an example of a telemedicine system. It is designed to monitor and act according to the actions of the patient. This framework is built using the C# language. This framework is using two methods to transmit the psychological data of patients. When the situation is normal, it sends data through the internet, and in the case of an emergency, it transmits data through the cellular network [8].

B. Usage of SDN in Healthcare Sector

Many healthcare organizations are moving forward with the new technologies. As a result of that they tend to upgrade their network accommodate new healthcare related technologies. Software defined networking which known as SDN can be considered as the ideal way to powerup and update healthcare networks while avoiding the disruption. Using Software defined networking, healthcare organizations can gain number of benefits as well [9] including,

- Save money on network infrastructure.
- Reduce the complexity of the network.
- Additional security added through enhanced intelligence.
- Centralized network management.

C. Latest technologies used in Healthcare Sector

1) Radio-Frequency Identification

Radiofrequency identification which known as RFID is a technology that has the ability to transfer data using a tag attached to particular objects via radio waves. Basically, it uses to identify and manage tools and equipment. In the health sector, RFID is used to prevent drug counterfeiting, and simplify the clinical process [10].

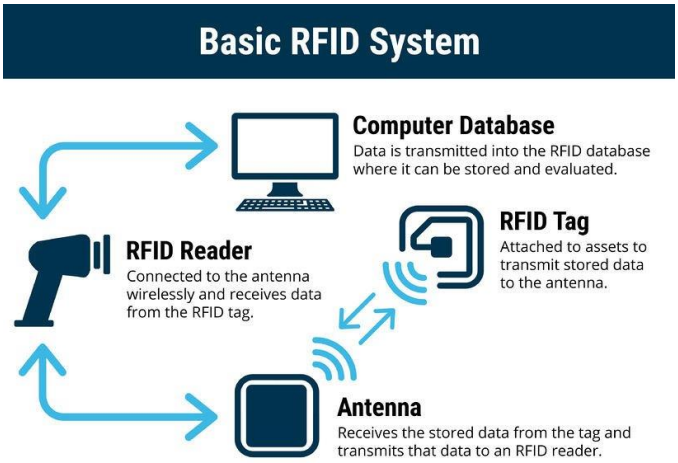

Fig. 3. – RFID cycle of process

2) Edge Computing

Edge computing is a sophisticated network architecture that allows the placement of computational and storage resources in a particular radio access network. This architecture helps to improve the network accuracy and the content delivery process to the users [11].

3) Cloud Computing

Combining cloud computing with IoT devices will enable the sensor technologies to collect patients' records including images, documents, and videos, and store them securely in clouds. This method will totally reduce the physical storage methods [12].

4) Augmented Reality

Augmented reality known as AR technology makes thousands of possibilities in the healthcare industry. Surgical visualization, visualizing patient information, Curing PTSD, speedup the patients' recovery, and making medical presentations more realistic are some of the possible tasks to do using AR technology. Already there are some AR technology embedded tools and systems which are utilized by health care professionals to ease their tasks [13].

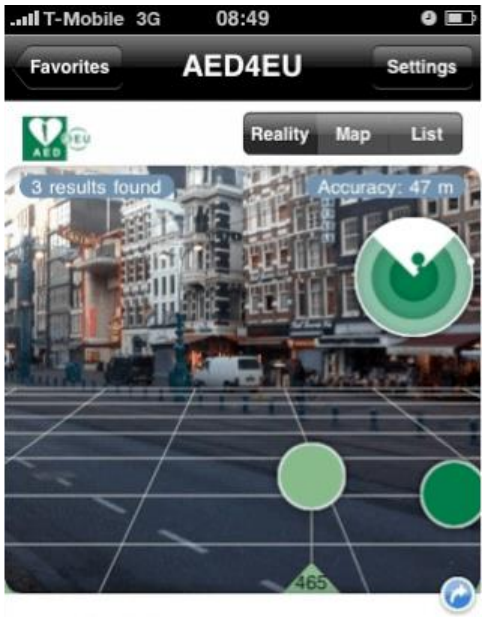

Fig. 4. – AR technology in real world

D. Vulnerabilities in Health Sector

1) Employees in Health Sector

Employees in the healthcare industry are the people who can access patients' health records with the least effort. While most of the staff members respect the rules of their organization, still there is a chance for an employee to break the rules and steal sensitive information from the system. Attackers can use this sensitive information for identity theft. Other than that they also can blackmail the patients [14]. There are a few purposes to stealing sensitive information by acting as a legitimate employee. One method is to steal users' credit card information and perform fraudulent purchases. And the other method is to steal demographic information and other social security information in order to commit variety of crimes [15].

2) Malware and Social Engineering attempts

Well organized malwares which have the ability to install inside the computers can compromise the entire system. Biggest challenge of malwares are they act like legitimate links to click or trusted files from trusted entities to open and install. Therefore it is essential to train the staff about malwares and phishing attempts [14]. Another type of phishing is to act like emails come from trusted entities. Once users open the attachments attached to the email, malwares will automatically execute inside the computer which have the ability to create and leave backdoors in victims computers [16].

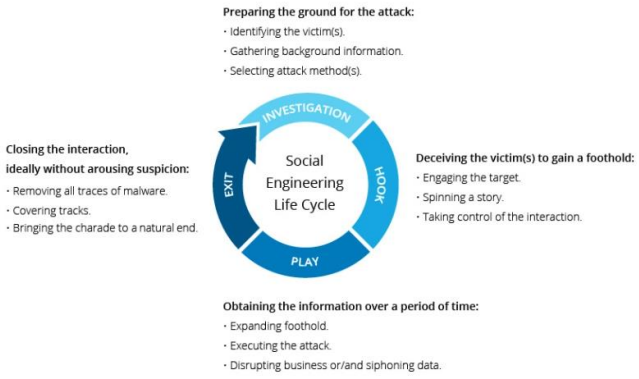

Fig. 5. – Social engineering life cycle

3) Vendors

Healthcare providers deal with vendors without evaluating the associated threat. For an example, if a hospital appoints a cleaning company, its employees should have right to use computers. There is all information related to patients, and there may be financial information of the hospital in computer network. Therefore, the information which are stored in the computers should not be viewed by the normal employees. There may be difficulties in locking all kind of access to the data since cleaning and maintenance are essential to providing a healthy work environment. [14].

4) Mobile Devices

Most healthcare services allow mobile users to logins to their system without checking any security standard of the device which is used to access the system. Since the staff communication devices are not included in organization's network security plan, this puts their networks vulnerable to malware and hackers. This problem is deepened once staff disposes of the equipment in an upgrade — network information or passwords might still be available, creating a natural access point for criminals. Unless the organization decides strict standards or forbids user devices altogether, there is not much that companies can do. In much the same way, lost or stolen devices correspond to an immense risk. Any mobile device used to access a service's network turn out to be a responsibility as soon as it is lost or stolen. If the device is taken by a criminal, he has the access to network using old or stored login data in that device. Once the network is accessed by a criminal it is difficult to distinguish their presence or reseal the breach. The security of online medical devices is frequently missing, creating them straightforward objects for hackers. There was a time that instruments such as infusion pumps just supplied data to the doctor and patient engaged. However, as the Internet of Medical Things (IoMT) continues to develop, these tools are created to distribute the information to outside sources and otherwise relate with the world beyond the doctor's office. This data could be intercepted or manipulated, generating a host of issues. Furthermore, hackers could obtain access to control most items associated to the network, together with how the machines function [14].

5) Unauthorized Access

Computers or any kind of end devices that are in publicly open places can easily be accessed by attackers or unauthorized parties. If that device contains any kind of sensitive information, they can easily steal them and sell them to 3rd parties or blackmail patients. Therefore, authorized people should make sure to keep the end devices that contain sensitive information about patients and other information in a secure location. [14].

6) Inadequate disposal of old hardware

Most of the people believe that once they've deleted any information, no longer have to worry about anyone accessing that information. But still there is a chance for someone to to recover that information. People used to dispose old hard drives and other hardware improperly. But attackers can recover that kind of improperly disposed hardware and recover the data in it. Employees should know the fact that anything they save inside a hardware is vulnerable. [14].

E. Threats in Health Sector

1) Denial of Service attacks

A denial of service (DoS) attack is a type of attack which can shut down a machine or an entire network. Basically, DoS attacks make targeted machines or networks inaccessible to their legitimate users. DoS attacks reach this target by sending requests, traffic, or information that can lead to trigger a crash rapidly to the targeted machine or network. Although there is a number of varieties of DoS attacks, the main goal of this kind of attack is to make machines and networks inaccessible to legitimate users [17].

There are a few kinds of DoS attacks including:

- Buffer overflow attacks - This is the most common type of DoS attack. Buffer overflow attacks send more traffic than the developers have built the system to handle.
- ICMP flood - This is also known as the ping of death attack. In this attack, attackers will send spoofed packets that ping every computer in that network. That will amplify the traffic [18].
- SYN flood - In this attack, attackers will send a request to connect to a server, but it will never complete the connecting process which is known as the handshake process. This will lead to filling all the ports with syn requests and legitimate users will not be able to connect.

2) Man-in-the-Middle attacks

Man in the Middle attacks is another common type of cybersecurity attack which can happen not only in the healthcare industry but in every industry which uses a network to communicate. Basically, Man in the middle attack can happen during any kind of communication session over the internet. Attackers will intercept the communication between two users or clients and the server communication in order to observe the information sharing. MIMT attacks are mainly used to steal login credentials and personal information. In the healthcare sector, attackers can intercept the communication between the healthcare experts and the patients and steal the data at the transmission process [19].

There are few variations of MitM attacks.

- **Wi-Fi eavesdropping** - Attackers can maintain a Wi-Fi connection with a fake name and victims connect to that Wi-Fi connection. Right after the victim connects to the Wi-Fi, attackers can monitor all the activities of the victim, and also, they can steal the personal information of the victim including credit card information.
- **Email Hijacking** - Attackers can steal someone's email address and send malicious instructions to a user. Victim users tend to follow malicious instructions and provide their personal information and money. Most of the time these kinds of emails are acting as emails coming from banking institutions.
- **Steal Cookies** - Since most websites rely on cookies, these kinds of attacks are easy to perform. Attackers steal cookies from the user's browser which contain the user's username, password, and other credentials.

3) Malware attacks

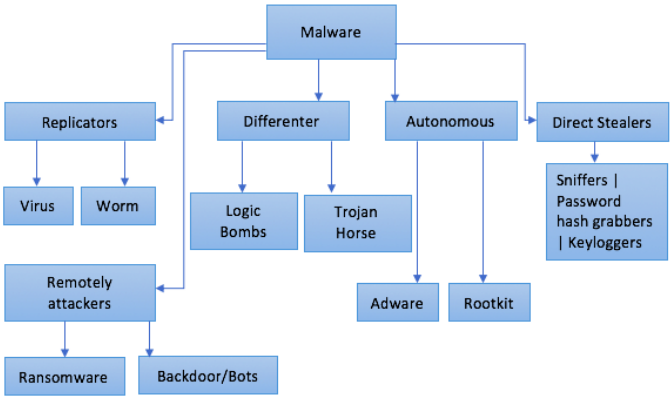

Fig. 5. – Types of malwares

Malware attacks are another common category in the cyber security attack domain. It can be considered a popular yet most dangerous attack type. Malware is a shorten form of malicious software. It contains variants of malicious software including ransomware, adware and spyware. Usually malware software consists of a code developed by cyber attackers which has the ability to damage a targeted system or to gain the unauthorized access to a network. Malwares are normally behave as a file or a link which requires the victim to open. When the particular victim open the link or the file, automatically the malware will initiate to execute inside the network [16].

Types of malwares

- Adware
- Annoyware
- Botnet
- Crimeware
- Dropper
- Hijacker
- Keylogger
- Miner
- Ransomware

4) Phishing attacks

Phishing attacks usually act as messages coming from a trusted entity. Most of the times phishing attacks are delivered through emails. Phishing attack plays a major role in social engineering attacks. The targets of this kind of attack are users' sensitive data like credit card details and login credentials. Users should be aware of phishing attacks in order to protect themselves from them. Since phishing attacks do have not a specific method to process [20].

5) Physical attacks

Physical attacks can happen due to the lack of physical security. Attackers can tamper with the devices and data inside the devices physically. Tampering with one bit of data will be affected the entire system. Therefore, authorities should ensure that attackers cannot reach the physical healthcare devices easily to destroy or tamper with them.

There are major layers of IoT and there are specific threats which can be affected to particular layers [21].

Layer	Possible threats
Cloud	- DDoS attacks - Buffer overflow attacks - Impersonations - Remote code execution
Core	- Data interruption

	- Man-in-the-middle attacks - Impersonation - Data exchange issues - Spoofing - Modification of data at rest and in transit - Relay attack - Jamming
Edge	- Connection flooding - Data interruption - DoS - Eavesdropping - Impersonation - Jamming - Packer Manipulation - Physical Attacks
Things	- Authenticity - Device end point attacks - Counterfeiting attacks - Eavesdropping - Hardware interruption - Jamming - Resource exhaustion - Privacy - Spyware - Repudiation - OS vulnerabilities

F. Real world scenarios

1) UVM health network attack

The University of Vermont Health Network shut down its IT system after identifying a cyberattack that happened on the 28th of October 2020. They did not disclose the details about the attack but they mention that attack infected 5,000 end devices including computers that were connected to their network. That outage lasted more than 40 days and they had to temporarily move 300 workers who were unable to do their regular job tasks since the hardware outage. As mentioned by the UVM medical center president and COO Stephen Leffler on 8th of December, UVM health system is losing more than $1 million per day in their revenue and will cost $63 million to resolve the problem [22].

2) Ryuk ransomware attack

On the 26th of October 2020, 6 hospitals in the United States has been attacked over 24 hours of period by the Ryuk ransomware, a variant of Hermes ransomware that can be considered one of the most dangerous ransomware. Klamath Falls, Ore-based sky lakes medical center, and a few other hospitals reported that they had an IT outage due to this ransomware in that time period. Apart from that Sky Lakes medical center had to purchase 2,000 new computers as a result of this attack. After this attack happened, unaffected healthcare systems across the United States took preventive measures immediately [23] [22].

3) Nebraska medicine system attack

Nebraska medicine system in Omaha reported there was a network outage that happened due to a security incident on 20th September 2020. Also, they reported that they have been reverted to paper records during this outage which lasted several days. Apart from that this attack also affected the EHRs and computer systems in North Platte [22].

There are some popular data breaches happened in healthcare sector previous year (2021). Organization and the number of affected people is in the chart below [8].

Organization	Date reported	Number of people affected
Florida Healthy Kids Corporation	29/1/2021	3,500,000
20/20 Eye Care Network, Inc.	24/5/2021	3,253,822
Forefront Dermatology	8/7/2021	2,413,553
NEC Networks, LLC	5/5/2021	1,656,569
Eskenazi Health	1/10/2021	1,515,918
The Kroger Co.	19/2/2021	1,474,284
St. Joseph's/Candler Health System, Inc.	10/8/2021	1,400,000
University Medical Center Southern Nevada	13/8/2021	1,300,000
American Anesthesiology, Inc.	8/1/2021	1,269,074
Professional Business Systems, Inc.	1/7/2021	1,210,688

G. How to protect data in Healthcare Sector

Protecting data and information in the healthcare industry is not an easy task. Healthcare providers should keep the balance between protecting data and providing quality patient care. Other than that, they should also meet the strict

healthcare-related rules and regulations which are stated by HIPAA and other institutions such as the EU's General Data Protection Regulation (GDPR) [24]. Protected health information which is known as PHI is among an individual's most sensitive private data. There are some best practices used by the healthcare providers in order to protect their patients' healthcare records which are stored in endpoints as well as in the cloud and keep the safety of that data while they are in transit, at rest as well in use. Some of these prevention methods require sophisticated approach to secure data while some of them are more like best practices.

1) Educate Healthcare Staff members

As in all the industries, the human element remains one of the biggest threats to the health care industry as explained in the threats in the health sector chapter. But especially in the healthcare sector, one small human error can result in enormous and disastrous consequences for the entire healthcare organization. Not like the other threats, employees in the healthcare sector are not an easy entity to recover from since humans are normally doing mistakes even, they are well educated about the mistakes and effects of them. Therefore, attackers are always aiming to attack the vulnerable points made mistakenly by humans. In order to resolve this cyber security experts should always educate the healthcare staff regularly. They should inform the staff about all the attacks that can happen in their healthcare organization, all the vulnerabilities, and the effects of them [24].

2) Restrict access to data and applications

Protecting healthcare data by implementing access control tools and application is a best practice that all healthcare providers should use. Restricting access to patient information and other critical system information to only the users who require access to those data to perform their job or take decisions based on that data will reduce the data breach risk to some extent. Other than that, they should also ensure that only authorized users have access to protect health care records. Most of the authenticating and authorization methods are already broken by the attackers. Therefore, we should ensure that we are using the latest approaches to secure access controls. Multi-factor authentication is one of the best approaches to maintaining the access control systems which require users to use more than one validation method in order to validate their identity [24].
Such as,

- Information is known only to a particular user like pin number or password.
- Object or a thing owned by only authorized users such as an ID card.
- Something unique to the authorized users such as biometrics. (Face ID, Fingerprint)

3) Use data usage control methods

As mentioned in the threats in the healthcare sector chapter, there can be people who are acting as the employees in a particular organization and get access to all the sensitive information and modify them in order to make the system vulnerable or sell those data to a 3rd party. In order to prevent that kind of situations, health care organizations can use data control methods to block specific actions involving sensitive data which can be made by the different kinds of users such as uploading health care records of patients anywhere, sending emails to out of the organization. copying healthcare information to external drives. There is more than one method to control data usage. Organizations either can block all the actions which are involving sensitive data or can distribute different kinds of rule sets based on the user type. The second method is more sophisticated but still, it is the most accurate data usage control method [24].

4) Monitor logging and usage records

Monitoring all the logging records and accessing records can be considered as a best practice to use not only in the healthcare industry but in any kind of organization. Enabling authorized parties to monitor users' actions such as that particular user is accessing what kind of information when that user logs in to the system, from where that user logged in. Monitoring and documenting all the user records can be beneficiary in multiple ways. When an incident occurs usually that organization is conducting an investigation in order to get a clear idea about what happened and who is responsible for that incident. Monitoring logging records of users makes that process easier [24].

5) Encrypt data

Encryption is one of the most accurate methods to secure data in healthcare organizations. According to the rules and regulations provided by the HIPAA, it is not mandatory to use encryption methods to secure patients' health information but it also provides some recommendations for encrypting data. But as a responsible healthcare organization, it is a best practice to encrypt all the data in transit as well as the data at rest. By encrypting the data in the healthcare industry even if the attackers get access to sensitive information it will require additional effort to decrypt those data which is impossible most of the time. Encryption methods and which kind of data should encrypt can be vary on the type of data [24].

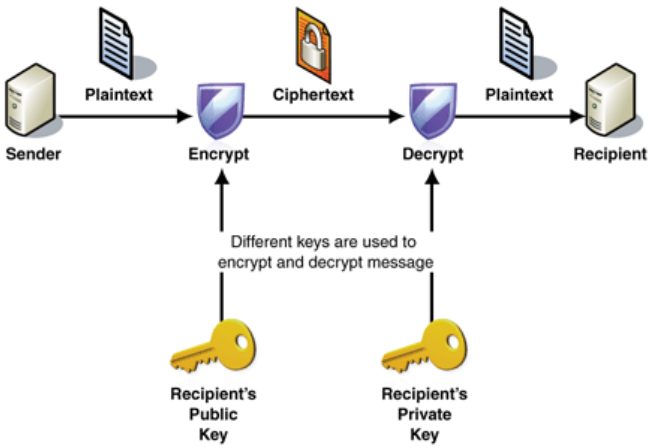

Fig. 6. – Encryption and Decryption process

6) Secure mobile devices

With the trend of using IoT technologies for everything, the usage of mobile devices for industrial purposes is also significantly increasing. when mobile devices initiate to play a major role in the healthcare industry, it creates more chances for attackers to attack the industry since it is considerably easy to attack mobile devices [24]. To prevent that kind of chances security measures for the mobile devices can be taken by the authorities. Including the methods mentioned below,

- Manage all the connected devices to the organization including the settings and configurations.
- Inform and enforce mobile device users to use strong passwords and always use biometrics if possible.
- Enable the ability to lock devices remotely.
- Monitor all the resources received by the mobile devices.
- Enable the ability to encrypt the data in mobile devices remotely.
- Use authenticating tools.
- Enforce users to keep their mobile devices up to date.

IV. FUTURE RESEARCH

Internet of Things are rapidly spreading throughout the globe. It is connecting with several other technologies and making human life easier Since Internet of Things is still a new concept, there are few flaws and doubtful points in several aspects including technology, legal as well as economic When consider about the challenges in term of security and accessibility, cloud computing which is a major technology used in IoT has few limitations when it comes to data and cost rates. There are some reported flaws in IoT user interfaces as well. As the consumers' feedbacks, IoT applications must be more user friendly and instructions to use should me more specific and clearer. Users might get confused when using IoT applications since the whole IoT concept is still new to the users. When we consider about the IoT network, LAN networks are use often which requires high cost to set up. And there are chances for the LAN administrators to access patients' data and use it for bad purposes. Other than that, at the time of data being transmitted through the network, data can be lost as discussed in the threat chapter. There should be proper backup system for IoT which is not addressed or researched yet. There are thousands of IoT wearable devices in the market at this moment. But all those devices are having a limited power supply. There should be a solution for that low power problem as well in the future. When we think about the sensor side of IoT, still there are no devices that can check the accuracy of the data that are being retrieved from human bodies via sensors. Above all there are number of stake holders who are hold their hands with various of IoT technologies. Still there is no research that have been conducted under the topic healthcare IoT from the perspective of the stakeholders. There should be more research about healthcare IoT including above issues. If these issues get sorted in the future IoT in healthcare will make a revolution in healthcare industry.

V. CONCLUSION

This reviewed paper looked into a variety of new devices which added in healthcare sector ,new security threats that exist in the healthcare industry. It also examined some of the security solutions for such threats. IoT-enabled healthcare, as well as its infrastructure, is vulnerable to a number of major security risks and malevolent activities. IoT-based health infrastructures could be used to launch new types of cyber-attacks, resulting in not only significant financial losses but also human tragedies. If so it will be so dangerous. Therefore, we just need to take necessary countermeasure to prevent from these types of attacks. In near future these devices and technologies will be improved much more .So it will make our lives much easier. But unfortunately, the cyber-attacks to these systems will be also increase. If we can identify the threats and vulnerabilities in these systems quickly and take necessary countermeasures quickly there won't be any problem. This research gives the reader a clear idea about the Cyber Security threats and mitigations in the Healthcare Sector.

VI. AUTHOR PROFILE

Pasindu Bandara Aththanayaka is 3 rd year undergraduate student at Sri Lanka Institute of Information Technology (SLIIT) who is currently pursuing his BSc (Hons) in Information Technology Specializing in Cyber Security.

VII. ACKNOWLEDGEMENT

I would like to express my deepest thanks to Mr. Kanishka Yapa, Lecturer in charge of the Applied Information Assurance (IE3022) module for giving me this great opportunity to conduct research on such an emerging and novel topic. And the support you gave throughout this time is highly appreciated. This research would not have been possible without your support and guidance.

VIII. REFERENCES

[1] Zou, N., Liang, S., & He, D., "Issues and challenges of user and data interaction in healthcare-related IoT," 2020.

[2] A. A. Economides, "User perceptions of Internet of Things (IoT) systems," Springer, Cham, 2018.

[3] Arcadius, T.C., Gao, B., Tian, G., Yan, Y.:, "Structural health monitoring framework based on internet of things: a survey," IEEE, 2017.

[4] Dimitrov, D.V., "Medical internet of things and big data in healthcare," 2016.

[5] ChaoLia, XiangpeiHua, LiliZhangb, "The IoT-based heart disease monitoring system for pervasive healthcare service," ScienceDirect, 2017.

[6] JunQi, PoYang, GeyongMin, OliverAmft, FengDong, LidaXue, "Advanced internet of things for personalised healthcare systems: A survey," ScienceDirect, 2017.

[7] FarmanAli, S.M. RiazulIslam, DaehanKwak, PervezKhan, NiamatUllah, Sang-joYoo, K.S.Kwak, "Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare," ScienceDirect, 2018.

[8] K. Jercich, "The biggest healthcare data breaches of 2021," 2021. [Online]. Available: https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021. [Accessed 1 April 2022].

[9] "How SDN is Powering Next-Gen Healthcare Tech Innovation," 2 March 2020. [Online]. Available: https://business.comcast.com/community/browse-all/details/sdn-powering-the-next-generation-of-healthcare-networks#:~:text=Indeed%2C%20software%2Ddefined%20networking%20(,and%20simplifying%20compliance%2C%20among%20other. [Accessed 1 April 2022].

[10] G. Healthcare, "Radio-frequency identification technology in healthcare," 20 June 2017. [Online]. Available: https://www.medicaldevice-network.com/comment/commentradio-frequency-identification-technology-in-healthcare-5848545/#:~:text=RFID%20helps%20to%20mitigate%20drug,of%20administering%20the%20wrong%20medications.. [Accessed 7 April 2022].

[11] S. Oueida, Y. Kotb, M. Aloqaily, Y. Jararweh, T. Baker, "An edge computing based smart healthcare framework for resource management," 2018.

[12] A. Dhilawala, "9 Key Benefits of Cloud Computing in Healthcare," [Online]. Available: https://www.galendata.com/9-benefits-cloud-computing-healthcare/#:~:text=What%20is%20cloud%20computing%20in,data%20on%20a%20personal%20computer..

[13] T. M. Futurist, "Augmented Reality In Healthcare: 9 Examples," 2 November 2021. [Online]. Available: https://medicalfuturist.com/augmented-reality-in-healthcare-will-be-revolutionary/. [Accessed 1 April 2022].

[14] "Security Threats in HealthCare Systems," [Online]. Available: https://consoltech.com/blog/security-threats-healthcare-systems/.

[15] "Insider Threats: In the Healthcare Sector," [Online]. Available: https://www.cisecurity.org/insights/blog/insider-threats-in-the-healthcare-sector. [Accessed 1 April 2022].

[16] "Malware Attacks: Definition and Best Practices," [Online]. Available: https://www.rapid7.com/fundamentals/malware-attacks/#:~:text=A%20malware%20attack%20is%20a,command%20and%20control%2C%20and%20more.. [Accessed 1 April 2022].

[17] Rashmi V. Deshmukha, Kailas K. Devadkarb, "Understanding DDoS Attack & Its Effect In Cloud Environment," 2015.

[18] "Ping flood (ICMP flood)," [Online]. Available: https://www.imperva.com/learn/ddos/ping-icmp-flood/#:~:text=Ping%20flood%2C%20also%20known%20as,requests%2C%20also%20known%20as%20pings..

[19] C. Team, "What are Man-in-the-Middle (MITM) Attacks?," [Online]. Available: https://resources.cylera.com/what-are-man-in-the-middle-mitm-attacks. [Accessed 1 April 2022].

[20] "What Is Phishing?," [Online]. Available: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. [Accessed 1 April 2022].

[21] Áine MacDermott, Phillip Kendrick, Ibrahim Idowu, Mal Ashall, Qi Shi, "Securing Things in the Healthcare Internet of Things".

[22] L. Dyrda, "The 5 most significant cyberattacks in healthcare for 2020," 14 December 2020. [Online]. Available: https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html. [Accessed 1 April 2022].

[23] "What is RYUK Ransomware?," [Online]. Available: https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html.

[24] N. Lord, "Healthcare Cybersecurity: Tips for Securing Private Health Data," 17 September 2020. [Online]. Available: https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data. [Accessed 1 April 2022].