Cyber Security threats and mitigations in the Healthcare Sector with emphasis on Internet of Medical Things

MUNASINGHA R.S.I – IT20643904

Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe 10115,
Sri Lanka
It20643904@my.sliit.lk

***Abstract*— Cyber threats and cyber attacks have become a major concern for organizations of all sizes. Cyber security is a topic which most healthcare organizations find difficult to understand. The healthcare sector is complex and sensitive regarding data privacy, patient confidentiality, patient records, and patient identity verification. This makes the sector an ideal target for cyber criminals who prey on weak cybersecurity practices to steal personal information or misuse the data to commit frauds or identity theft. In addition, the widespread use of internet has made it easier for cyber criminals to spread malware or phishing links via email attachments to lure unsuspecting users into downloading malicious software which can then be used as a source of further cyberattacks. The growing use of internet-enabled devices in hospitals and other medical facilities has made these places more vulnerable than ever before. It is imperative that healthcare organizations adopt best practices to protect their critical information from cyber threats and attacks in order not only minimize the impact but also prevent them completely in future. Let's explore how cyber security threats pose a serious threat to healthcare organizations with emphasis on Internet of Medical Things (IoMT).**

***Keywords*— IoMT; IoT; E-health; Security; Privacy; Health Cyber Security Threats; Secure Healthcare Systems; Health Data Breaches;**

I. INTRODUCTION

Cyber security is one of the fastest-growing industries in the world. It is projected to generate $6 trillion in value by 2021. With the growing access to information and communication, cyber security has become a lot more complex than it originally was thought be. Healthcare sector has been listed as one of the top targeted sectors in terms of cybersecurity[1] because of its huge value and its core components, such as protected health information (PHI), clinical trial systems, electronic medical records (EMR), electronic health system (EHS), electronic health record organization (EHRO), and patient portals. The healthcare sector is also considered an "endpoint" for cyber threats because of its high exposure to malicious actors, users, and operating systems using it for legitimate purposes like accessing PHI, uploading or downloading malicious files or software code, or connecting to network resources.

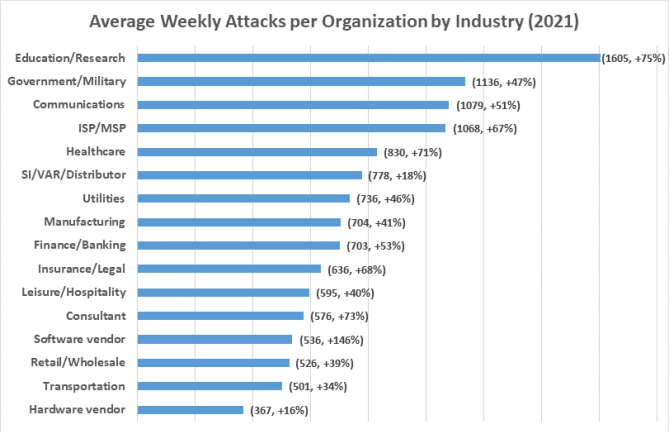

Fig. 1. Average weekly attacks per Organization

II. WHAT ARE THE CYBER SECURITY THREATS IN HEALTHCARE?

Hospitals, doctors' offices and other healthcare institutions face a number of cyber security threats and mitigations in the healthcare sector. The most common threats in the healthcare sector include: - Bias, Error and Vulnerability in Healthcare Systems - Biased systems, human error and weak security controls are responsible for many cyber security threats in healthcare. Biased systems are those that have discriminatory assumptions built into them[2]. These assumptions lead to unintentional, or even intentional, failures in the system. Examples of biased systems in healthcare include electronic health records, or EHRs. In order to avoid inaccurate, incomplete and/or biased data, many healthcare systems use a "black box" approach[3], where data is fed into a computer program and then the computer program generates an output. Because the computer program will almost always be biased, the output is typically unreliable. In an effort to reduce bias, many EHR systems use a number of techniques. For example,

if a doctor enters a diagnosis into the computer program, the computer program will automatically assume that the doctor also has the data that is associated with that diagnosis. Because the assumptions that the computer program is making as it reads the data are not being transparently communicated out to the data, the data will be biased. As a result, the computer program will generate an output that is inaccurate. - Hijacking of Medical Devices and Sensors - Examples of hijacking of medical devices and sensors include when hackers use a device's signal to send false data. At the same time, hackers may also attempt to take control of a device by, for example, sending fake signals that trigger false readings. - Theft of Medical Information (IMI) - Hacking into medical devices can give hackers access to patients' medical records[4].

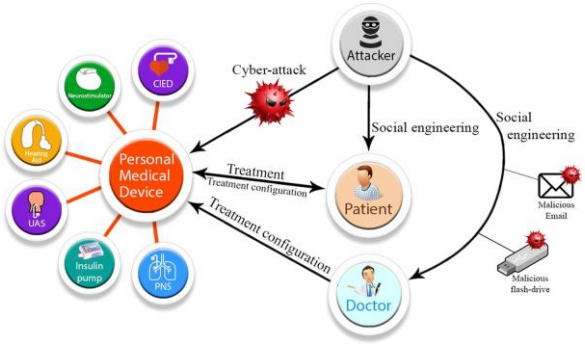

Figure 2 [5]

Medical devices and software, such as hospital systems and medical devices, are often not properly protected by encryption. As soon as medical devices connect to the internet, they become targets for hackers. - Denial of Service (DoS) Attacks - Healthcare systems are often not designed to withstand DDoS attacks, which can cause systems to become unstable and unable to function[6].

III. Bias, Error and Vulnerability in Healthcare Systems

Biased systems, human error and weak security controls are responsible for many cyber security threats in healthcare. Biased systems are those that have discriminatory assumptions built into them. These assumptions lead to unintentional, or even intentional, failures in the system. Examples of biased systems in healthcare include electronic health records, or EHRs. In order to avoid inaccurate, incomplete and/or biased data, many healthcare systems use a "black box" approach, where data is fed into a computer program and then the computer program generates an output. Because the computer program will almost always be biased, the output is typically unreliable. In an effort to reduce bias, many EHR systems use a number of techniques. For example, if a doctor enters a diagnosis into the computer program, the computer program will automatically assume that the doctor also has the data that is associated with that diagnosis. Because the assumptions that the computer program is making as it reads the data are not being transparently communicated out to the data, the data will be biased. As a result, the computer program will generate an output that is inaccurate[7].

IV. Most Common Cyber Security Threats in Healthcare

The healthcare sector is extremely susceptible to cyber attacks due to the enormous volume of sensitive information stored in its systems, such as doctors' records, patient records and hospital infrastructure systems. The Internet of Medical Things (IMT) and its role in cyber security threats is also of significant interest. The IMT is the growing collection of electronic medical devices (e-MDs), such as medical devices and wearables, connected to healthcare networks. This creates numerous security risks when hackers attempt to use IMT devices to gain access to these networks and the information stored on them. If hackers are able to gain access to IMT devices, then they can also potentially use these to create malware, conduct data breaches and create DoS (Diversion of Service) and DDoS (Distributed Denial of Service) attacks[8].

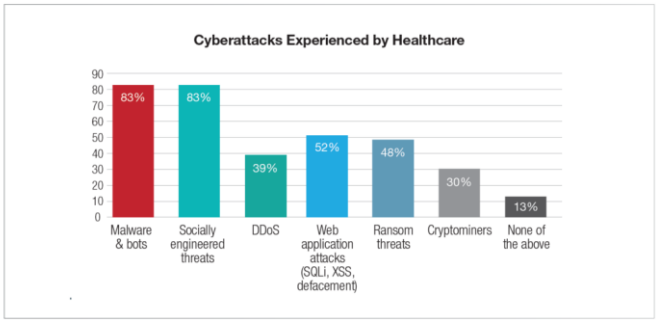

Figure 3[13]

A. *Data breaches*

A data breach is the unauthorized access of organization's data. This may occur through a cyber attack, a data entry error or through a software flaw. The result of a data breach is usually a significant loss of business and trust. In addition, a data breach may cause a number of reputational issues for organization and, if the identity of the data is compromised, may even face criminal charges. A data breach can cause a number of issues in the healthcare sector, including a decreased appeal as a medical treatment option, lowered provider/hospital trust scores, potential fines from regulatory authorities and potential lawsuits from patients. Therefore, it is essential for healthcare organizations to prevent data breaches through strong cyber security implementations and practices[9].

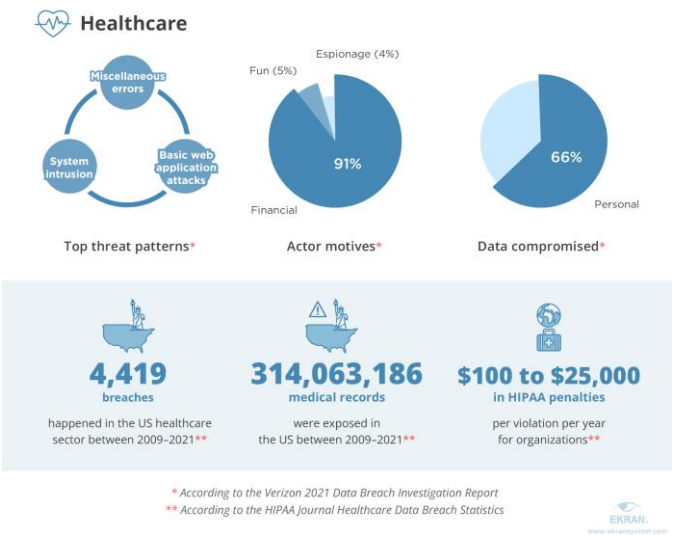

Figure 4 [9]

B. *Hijacking of Medical Devices and Sensors*

Examples of hijacking of medical devices and sensors include when hackers use a device's signal to send false data. At the same time, hackers may also attempt to take control of a device by, for example, sending fake signals that trigger false readings[10].

C. *Theft of Medical Information (IMI)*

Hacking into medical devices can give hackers access to patients' medical records. Medical devices and software, such as hospital systems and medical devices, are often not properly protected by encryption. As soon as medical devices connect to the internet, they become targets for hackers[11].

D. *Malware attacks*

A malware attack is when a hacker uses malware to infiltrate your systems. The malware may be downloaded on a device, such as a computer, phone or medical device. Once installed, the malware has the capability to send data back to the hacker and/or have other malicious activities performed on the infected device. The most common types of malware in the healthcare sector include viruses, ransomware and spyware. Viruses are programs that replicate themselves and then attempt to infect other devices. They can also cause data loss, data corruption and/or functional issues in the devices they infect. Ransomware is a type of malware that encrypts data on a device. This is done so that until the user pays a ransom, they cannot access the data. The hackers who are behind these attacks are usually after financial gain, such as a ransom for unlocking the data[12].

E. *DDoS Attacks*

A DDoS attack is an attempt to saturate a targeted server's bandwidth capacity by sending an abnormally large amount of traffic to the targeted server. As the targeted server is not designed to handle this amount of traffic, it is forced to slow down and stop receiving data from other sources. This can have serious consequences for a healthcare organization, as it can significantly disrupt critical business operations and negatively impact the quality of patient care. Since a significant number of health care organizations run on cloud-based functions, such as EHR systems, patient-facing websites and data entry applications, a DDoS attack can have a major impact on these businesses. To protect against DDoS attacks, organizations can implement DDoS protection solutions, such as an Internet Security System (ISS). The ISS is a device that sits between the targeted server and the ISP's network. It has the capability to identify and defend against DDoS attacks by either blocking the attack or filtering it so that it does not cause any disruption to the targeted server[12].

F. *Darkweb and ransomware threats*

The darkweb is a network of websites, such as the Tor Network, that are located on the Darknet. Darknet is a subnetwork of the Internet, which is typically not mapped or monitored by Internet search engines like Google, Bing and Yahoo. Darknet is one of the most common places where criminals operate. In fact, the darkweb is known for being one of the most dangerous places in the digital landscape. Darknet is a breeding ground for both cyber threats and cyber criminals. Darknet is often used to distribute ransomware, which is a type of malware that blocks access to your data. This type of malware has become increasingly common in the healthcare sector, as hackers use it to hold organizations' data hostage until a ransom is paid.

V. LITERATURE REVIEW

With technology advancing at such a rapid rate, several studies have identified the difficulties this has caused. In addition to providing solutions and techniques to these problems, we must conduct more studies in order to guarantee the security and privacy of IoT applications, particularly in healthcare applications. Technology has permeated many aspects of life, so many studies are required to ensure proper data security and privacy in IoT applications, particularly in healthcare applications. Sensor data is then end-to-end encrypted. A gateway between sensors and the cloud is also suggested. They created hardware and software that emulated their suggestion. This study reduces communication costs, as well as discovering that this design is 97% faster than others they tested. They also found that this design is 97% faster than others.

[16]'s author devised a method for securing current IoT-based medical devices using body sensor networks. This study addressed the security risks raised by body sensor networks systems and devised a way to address these issues. When compared to earlier approaches, they shortened execution time by 42%. The authors presented an identification Architecture

for medical system security [16]. Two security measures have been proposed. The identification schema for IoT-based medical systems and the coexistence proof schema for multi-tagged goods. Their communication paradigm allowed for strong and secure communication. They used their strategy to ensure success. In [17], researchers developed a centralized data storage system that collected data from multiple sensing devices.

This research is an attempt to assure system security, privacy, and confidentiality. They used two different cryptographic systems. A hybrid of attribute-based and functional encryption methods. Framework architecture proposed [26] A cloud-based architecture for safe healthcare applications utilizing Wireless Body Area Networks was created in [17]. (WBAN). To secure inter-sensor communication, they used a multi-biometric key generation approach. They also linked the EHR, which is housed centrally on the health sector cloud. Their approach resulted in the creation of a secure cloud-based architecture that safeguarded communication operations as well as patient data security and privacy. [18]

In the IoT framework, a lightweight attribute-based encryption (ABE) system is proposed to secure stored data, device communication, and data sharing. Traditional (ABE) was a general IoT schema. For data privacy and security, they used a cryptographic algorithm (ECC). They employed matrices to calculate the transmission and processing costs of their schema. Although the proposed schema has many drawbacks, the findings show that it is less expensive and faster than the current design.

VI. SECURITY COUNTERMESURES

To address security risks, numerous security measures are used. Various solutions are employed to address various types of threats. Cryptography, identification, and authorization are some of the possibilities for protecting data from various threats. This document focuses on Cryptography algorithms for protecting data from several forms of security concerns, but not all of the companions were included. Because the Internet of Things is a flexible architecture, cryptography and authentication techniques are required in some cases for data protection.

Traditional cybersecurity controls, on the other hand, cannot be used directly for Internet-of-the-thick applications, and they are used as a foundation for newly developed ways. This study will go through some of the most used symmetric encryption algorithms. DES, 3DES, Blowfish, and AES are examples of these approaches.

1) Data encryption standard – DES:

Data encryption standard (DES) is a family of symmetric-key block ciphers developed by IBM. DES is considered the grandfather of all modern block ciphers and is the basis for most commercial block ciphers. DES was made public in 1977[14].

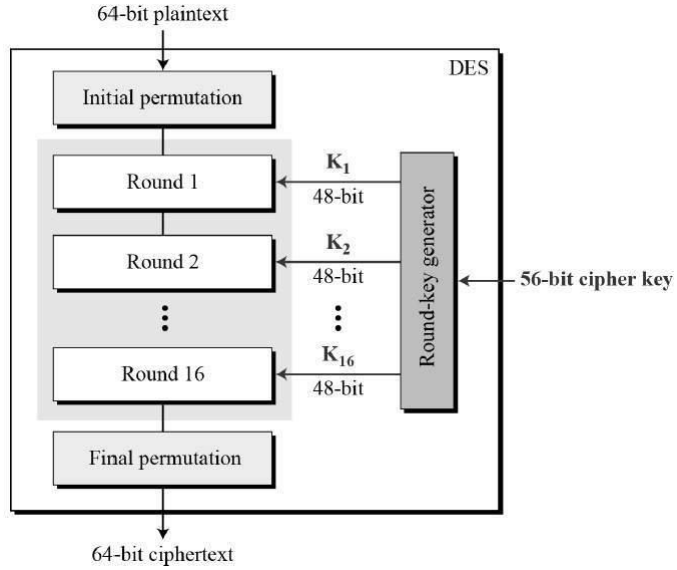

Figure 5. DES Structure

2) Blowfish:

Blowfish is a cipher algorithm, invented by Bruce Schneier in 1993, and is one of the algorithms used to protect many SSL connections. Schneier designed Blowfish to prevent brute force attacks. Blowfish is a little more computationally expensive than some other ciphers, but it's considered to be more secure.

3) *Triple data encryption – 3DES:*

As an improvement to DES, 3DES Standard was introduced in 1998. This approach ran the DES three times. It also uses the same block size, 64 bits, with 56 bits reserved for critical length. This approach is faster than DES, but it is also thought to be a slow algorithm because it needs running DES three times. It outperforms DES in terms of efficiency.

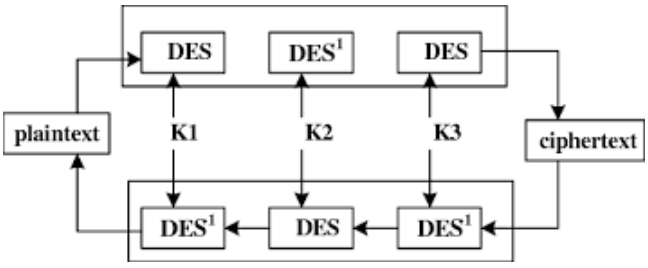

Figure 6. 3DES Diagram

4) Advanced encryption standard – AES:

Advanced Encryption Standard (AES) is a symmetric-key block cipher. It was published in 2001 by NIST and is the de facto encryption standard used today. Thanks to its strong encryption, AES is often used to secure sensitive data,

including credit card transactions, personal health information, and government communications. AES is AES is so-called due to its Advanced Encryption Standard[15].

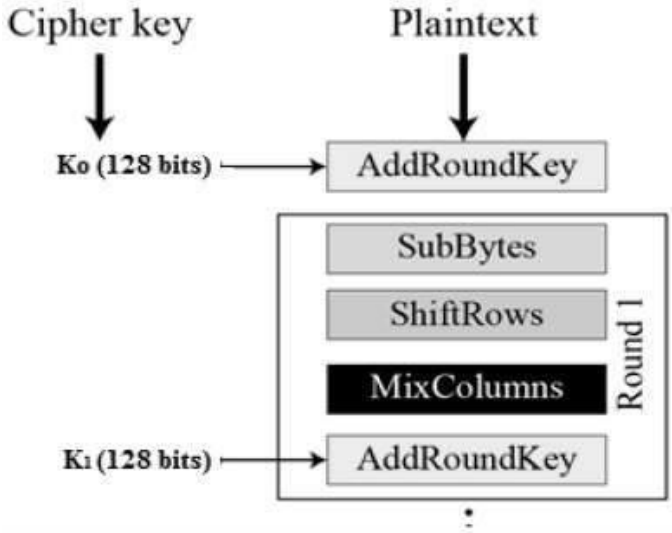

Figure 7. Advanced encryption standard

Because information security is a significant concern in Intelligent Healthcare, further proactive efforts to increase the level of security of Healthcare Information networks may be implemented.

A. Deployment of security professionals

A sufficient number of internet security professionals must be installed in medical and Intelligent Healthcare systems to regularly monitor, update, and safeguard the network-connected devices. In an Intelligent Healthcare context, this will attempt to reduce the It divide. To resolve concerns, the clinics must be equipped with experienced teams and proper incident response strategies[20].

B. Inventory maintenance

The Internet of Things (IoT) must include inventories of all network-connected objects. Their operations, including bandwidth and connectivity, must be checked on a frequent basis. A vulnerability database must be created and maintained with the most recent vulnerability reports pertaining to the commodities utilized in the connection. Related equipment must be upgraded using the patches provided by their manufacturers[20].

C. Compliance

Before deployment, IoT equipment must be tested to ensure compliance with safety rules such as ISO/IEC 82304, ISO/IEC 62304, and other applicable health goods standards [13]. The devices' ability to perform security upgrades should be verified. The collection and dissemination of data must adhere to the statutory conditions and restrictions[20].

D. Secure update

The update should only be allowed from approved IP addresses, and any communication with unauthorized IP addresses should be treated as undesired traffic. Connectivity efforts for security patches must be made only through designated ports and must be closed permanently following the update. Only approved specified IPs may be used for connectivity[20].

E. Product security

The network must be constructed as much as feasible using devices from the same manufacturer. To reduce the risk of supply chain assaults, the maker should attempt to use as few third-party items as possible in their architecture. Before installing the devices into the system, the default password must be changed. In most cases, it is preferable to deploy application-specific devices in a healthcare setting rather than third-party generic IoT devices[20].

F. Network segmentation

Micro-segmentation can protect critical equipment from unwanted disclosure outside of the network. It must be ensured that network equipment is flexiblely connected, so that the failure of one appliance does not affect the overall operation of the network[20].

G. Data Integrity

The data recorded on storage media should be accessible only to the verified user, and no data should be accessible to the general public. The device must collect just the essential information, and it must be validated that it does not collect any superfluous data [21]. To limit any unusual attack, information must be backed up on a regular basis[20].

H. Security audit

Third-party audits of the system must be performed on a regular basis, and network vulnerabilities must be investigated. The new gadgets must replace those that cannot be updated.

VII. FUTURE RESEARCH

The Internet of Things is quickly growing over the world. It is linking with other technologies and making human life simpler. Because the Internet of Things is still a new idea, there are several defects and questions in numerous areas such as technology, law, and economics. When it comes to data and cost rates, cloud computing, which is a significant technology utilized in IoT, has a few restrictions when it comes to security and accessibility. There have also been some identified issues in IoT user interfaces. According to customer feedback, IoT apps must be more user pleasant, and usage instructions must be more explicit and clear. Users may be

perplexed when utilizing IoT apps since the entire IoT idea is still new to them. When it comes to IoT networks, LAN networks are frequently used, but they are expensive to set up. Furthermore, there is a risk that LAN administrators will gain access to patients' data and misuse it. Aside from that, as stated in the danger chapter, data might be lost while being transferred via the network. There should be a robust backup mechanism for IoT, which has not yet been addressed or explored. There are now hundreds of IoT wearable gadgets on the market. However, all of those gadgets have a limited power supply. In the future, there should be a solution to the low power issue as well. When it comes to the sensor side of IoT, there are currently no technologies that can validate the accuracy of data obtained from human bodies via sensors. Above all, there are a lot of stakeholders that are working with various IoT technologies. There is yet to be any study undertaken on the topic of healthcare IoT from the standpoint of stakeholders. More study on healthcare IoT, including the aforementioned problems, should be conducted. If these concerns are resolved, IoT in healthcare will revolutionize the healthcare business.

VIII. CONCLUSIONS

Healthcare organizations face a range of threats when it comes to cyber security, including bias in the system, hacking of medical devices, stolen medical information, and denial of service attacks. Organizations must protect themselves from these threats by implementing strong cyber security policies and practices. Healthcare organizations must also protect themselves against cyber threats by conducting regular risk assessments and implementing appropriate safeguards. These steps will help healthcare organizations prevent cyber threats and mitigate the effects if they occur. These threats and mitigations can be especially challenging for healthcare organizations that rely on technology to deliver patient care and manage patient records. To address these challenges, healthcare organizations should focus their efforts on the following: - Implementing strong policies and procedures for cybersecurity - Conducting regular risk assessments to identify and mitigate threats - Implementing appropriate safeguards to protect critical healthcare assets - Ensuring that all employees are trained on policies and procedures and know how to report cyber security threats.

ACKNOWLEDGMENT

Mr. Kanishka Yapa, the lecturer in charge of the Applied Information Assurance module, has helped and advised me since the beginning of the project by holding lecture and practical sessions. Also, a big thank you to everyone who assisted me much in acquiring the appropriate materials and coming up with fresh ideas to ensure the project's success.

REFERENCES

[1] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/
[2] https://health-policy-systems.biomedcentral.com/articles/10.1186/1478-4505-8-35
[3] https://jamanetwork.com/journals/jama/article-abstract/386184
[4] https://www.aamc.org/news-insights/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices
[5] https://www.sciencedirect.com/science/article/pii/S1532046419301522
[6] https://healthitsecurity.com/features/the-threat-of-distributed-denial-of-service-attacks-in-healthcare
[7] https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-14-36
[8] https://contentsecurity.com.au/cyber-security-concerns-in-healthcare/
[9] https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches
[10] https://duo.com/decipher/hacking-medical-devices-to-hijack-secure-facilities
[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6179506/
[12] https://www.cisecurity.org/insights/blog/ransomware-in-the-healthcare-sector
[13] https://blog.radware.com/security/2020/08/security-challenges-for-healthcare-providers/
[14] https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm
[15] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
[16] P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," IEEE Transactions on Industrial Electronics
[17] J.-L. Hou and K.-H. Yeh, "Novel Authentication Schemes for IoT Based Healthcare Systems," International Journal of Distributed Sensor Networks
[18] D. Sharma and D. Jinwala, "Functional Encryption in IoT E-Health Care System
[19] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks"
[20] R. Marshal, K. Gobinath, and V. V. Rao, "Proactive measures to mitigate cyber security challenges in IoT based smart healthcare networks"
[21] M. Elhoseny et al., "Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions"

IX. AUTHOR PROFILE

Munasingha R.S.I
3rd year 1st semester
Undergraduate in B.Sc.(Hons) in Information Technology specializing in Cyber security.
Sri Lanka Institute of Information Technology (Malabe, Sri Lanka)