Cyber Security threats and mitigations in the Healthcare Sector with emphasis on IoMT security and Software Defined Networking

Gunasekara M.V.G.R.S
IT21162596
AIA – IE3022
Assignment 01
3rd Year 1st Semester
it21162596@my.sliit.lk

***Abstract*— The industry that hackers attack most frequently is the healthcare sector. We address numerous threats, vulnerabilities, and IOT employed in the healthcare business in this review article, as well as risks and vulnerabilities related to the e-healthcare sector. Additionally, to lessen these risks and weaknesses in the e-healthcare ecosystem, as security safeguards and cryptographic defenses.**

Keywords— cyber security, threats in healthcare, phishing, IoT security (*keywords****)***

I. INTRODUCTION

IoT is a collection of physical objects connected to the Internet that have sensors, indications, computing power, software, and a variety of other technologies. It may then function as an intelligent things. ECG equipment, blood sugar monitors, heart rate recorders, AIDs (automatic insulin administration machines), etc. are a few examples. Compared to analog equipment and human power, these smart gadgets can operate more effectively. furthermore, this economical option [1].

Every year, there are more reports of cybercrimes and data breaches in the healthcare industry. HHS - Health and Human Services of the United States of America - has received reports of 4419 data breaches in the healthcare industry from 2009 to 2021 [2].

The average magnitude of a data breach from 2009 to 2021 is shown in Fig 1.

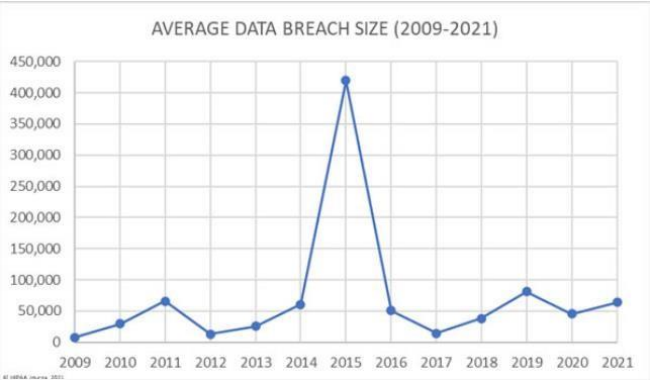

Figure 1

To provide interconnections for intelligent things, the IoT heavily relies on wireless connections and communications. Due to their flexibility requirements, wireless connections are necessary. Wireless connections are vulnerable to multiple security risks, eavesdropping, and other risks because of their open nature. Numerous data security incidents over the past 10 years have brought to light the growing danger facing all industries connected to the Internet of Things (IoT) via communication networks. While IoT data from smart objects and sensors recording health-related information may be obtained and evaluated to improve our everyday lives, communication between smart objects may reveal patient privacy information. If a patient is wearing an intelligent sensor that communicates with another device in a specific location, the link between these two devices may also be exploited for inappropriate purposes, such as tracking the patient's adaptability. Medical service providers including specialists, attendants, paramedics, and others are trusted and accepted to access and disseminate patient data as intended, but there is always a chance that the information may wind up being obtained by unauthorized parties. Continuous patient monitoring, for instance, may show when the pulse is stronger than expected or when the patient may survive a coronary event, but it may also provide other information that might make the patient feel anxious or upset. The coordination of so many disparate devices by the IoT raises unique, serious risks. More connected and brilliant structures are being built in crucial areas like healthcare. The risks associated with IoT-based core frameworks are getting worse, and any disruption or deterioration might result in expensive harm or fatal problems [1].

II. WHY TARGET HEALTHCARE? & THREATS

In the world, 90% of institutions in the healthcare industry have been compromised. [3] Additionally, the impact of inadequate security is getting worse. At the 2018 RSA Conference in the United States, hackers "killed" patients without the medical staff being aware that the operating theatre had already been commandeered. The 30-day mortality rates have increased significantly because of ambulance delays brought on by detours made to avoid the marathon. Let's say that a 4.5-minute increase in the average length of the ambulance ride caused deaths. In such circumstances, it is logical to presume that fatalities occurred because of the significant hospital ransomware-related outages that occurred in the United Kingdom. Other hospital attacks, like the one at Hollywood Presbyterian Hospital, occurred when ambulances were redirected to other facilities

because of excessive traffic, or instances identical to these also occurred at other facilities. Why focus on health care?

- They were accumulating data on patients because they were valuable resources. Hackers might then abuse them [4].

Hospitals keep a lot of patient data. The company is being targeted more frequently by hackers due to its important secret data. These businesses must safeguard patient data. With GDPR going into effect this year, hospitals must keep their data safe.

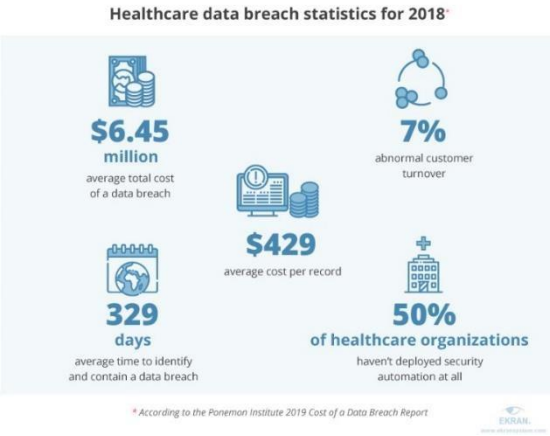

Figure 2

Payment for ransomware data recovery or fines for GDPR non-compliance is a significant and worrying concept for a healthcare organization that is already having trouble paying for basic employee requirements. Data security measures like multifactor authentication are more cost-effective than ransomware attacks. A one-time passcode, or OTP, is generated by MFA when a person signs in using a variety of bits of data. This makes it far more difficult to steal passwords and other data. Verify Figure 2.

- Medical IoT devices provide hackers with an accessible endpoint.

The benefits of modern medical technological advancements are minimal. Modern medical technology includes heart monitors, insulin pumps, and X-rays. Regarding internet security and patient data protection, these new devices provide more attack avenues. It is typical for medical devices to be used just for that purpose. They are not made to be secure. The devices may be used to attack a server even though they might not have the needed patient data. In the worst-case scenario, attackers may completely control medical equipment, preventing medical professionals from providing crucial life-saving treatment. Hackers are aware that medical devices do not save patient data. Hackers view insecure devices like laptops and PCs as easy targets. Medical organizations may have issues due to threats to medical equipment since they might provide hackers with access to other networks. components or the ability to run ransomware. Maintaining network security helps lessen the damage caused by medical device assaults.

- Remote database access by employees presents greater opportunities for hackers

In the healthcare industry, cooperation is essential to offering each patient the best alternative. People who require access to data use a variety of gadgets rather than sitting at their desktops all the time. Since not all new gadgets are secure, remote server access to them presents a challenge. Additionally, not all health professionals have cybersecurity training. Since one hacked device might expose a whole firm, infected devices must not have a network connection. For businesses with mobile workers, RBA - risk-based authentication - is one option. With the use of this technology, IT staff can establish rules that determine how risky a product is based on factors like the user, location, and more. To prevent exposing sensitive patient data to risky equipment, abnormal activity is reported [5].

- Lack of expertise in information security

Medical professionals are trained to handle a variety of scenarios, but not cyber risks. All health practitioners cannot be cybersecurity experts' best practices due to financial, material, and time constraints. Cybersecurity solutions need to be complex yet simple to use. An easy-to-use security solution is required for healthcare personnel. To focus on their work, they want the certainty that patient records are safe. Since users just need to know their own login credentials, technologies like MFA - multifactor authentication - and SSO - single sign-on - are becoming more and more popular.

- Making use of old technology

Although medical technology has advanced significantly, not all facets of healthcare have kept up. A large portion of medical equipment is out-of-date due to budgetary restrictions and an unwillingness to learn new procedures. All software should be kept current by hospitals using systems that still offer upgrades. These often include bug fixes and security updates. But eventually, programs will reach their end of life, and vendors will stop upgrading. Additional layers of security may lessen the risk of invasions where updating to more secure software is not practical or even if healthcare professionals do not want the hassle. Multifactor authentication, for example, can stop a hacker from entering other secure settings if one system is compromised. To secure patient data, healthcare organizations must act rapidly in response to emerging cyber hazards. It's crucial to plan your finances and invest in the best option for your company. Keep up with new threats as you battle to protect all of your equipment as your systems age.

There are several risks to the privacy and security of patient health information as a result of the widespread use of Web-based healthcare apps. The security of electronic patient healthcare information is significantly threatened by malicious programs and criminal actions, especially those who aim to conduct medical identity fraud and healthcare fraud. Further complicating problems is the environment created by the emergence of mobile devices, such as smartphones, where patients' wireless chats and emails from medical providers may be watched. The availability of patient

data, which may contain accurate diagnostic and treatment information and other sensitive information, is at risk due to healthcare service providers' lack of proper standards and security measures. Such problems may have a substantial impact on patients' health as well as the proper delivery of their drugs and therapies. The N3 NHS network has two additional data centers that provide identification and access monitoring for network users in addition to the twelve big data centers that provide local and national services. With the help of verified user access to the N3 network and network redundancy, the web is designed to preserve data security and integrity. To lessen data interception, certain organizational and physical security measures have been put in place. To control user conduct, these tactics include creating policies and laws.

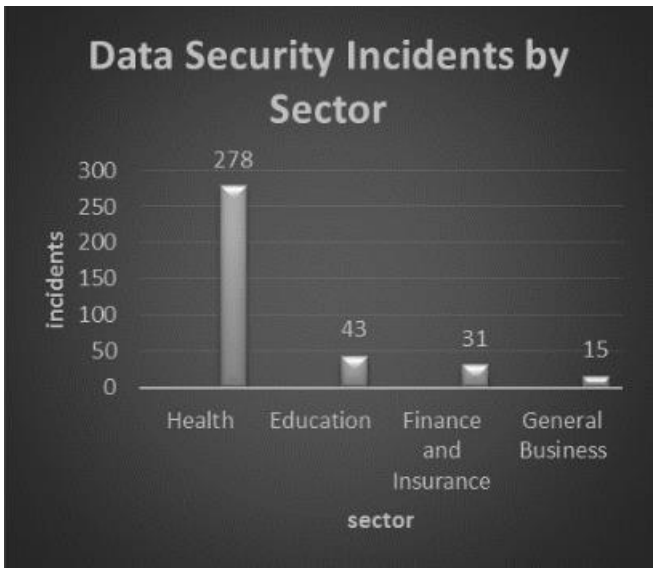

Figure 3

The Information Commissioner's Office reports that during 2013 and 2014, there were two more instances of data breaches in the healthcare industry. In the first half of 2014, 183 data breaches were reported to the information security agency, as opposed to 91 infractions during the same period in 2013. There was an increase in the number of security incidents in the healthcare industry between October 2014 and September 2015. The number of data security incidents in the healthcare sector has increased by 44% during the previous quarter. This growth's size is consistent with an overall rise in security incidents affecting sensitive data. Therefore, the percentage of total cases that belong to the health sector has not changed from the previous quarter [6].

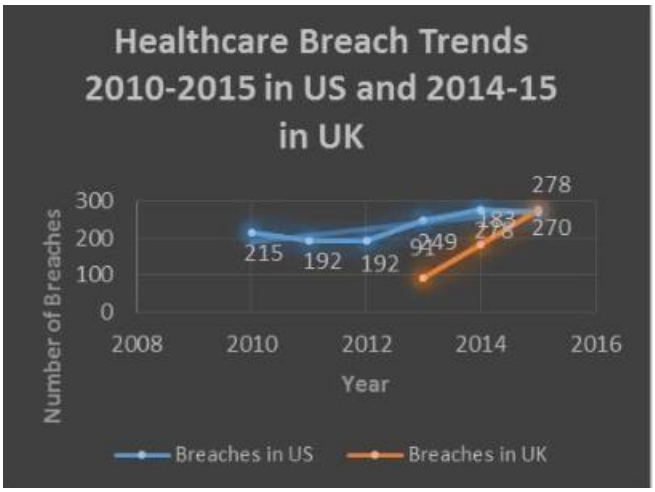

Figure 4

III. HEALTHCARE IOT SECURITY

No matter where a patient is situated, online healthcare apps connected to hospital systems enable the interchange of patient-specific data and medical information. Patient-worn sensors gather and communicate information about their vital signs to the medical systems at the institution where they are receiving treatment, including their body temperature and heart rate. An attacker may use weak authentication methods, such as those present in embedded web servers located throughout the hospital, to gain access to crucial systems. As a result, the attacker could be able to take down medical systems, acquire access to private patient information, and get past security measures to target particular patients. If a compromised sensor is linked to the patient, the consequences of a security breach might become unmanageable and possibly result in the patient's death. It follows logically from this that these devices require protection. As part of their healthcare monitoring and data analysis, hospitals may use the information gathered by Internet of Things sensing devices to assist their patients. The sensors themselves are designed to continuously collect data. Integrating IoT-based medical infrastructure with traditional IT systems and operations may lead to new risks. Due to the IoT's nebulous range of capabilities, several security vulnerabilities may arise. It's difficult to define IoT smartness, and it's unclear if the current Internet of Things (IoT) is sophisticated enough to be regarded as such. A security perspective emphasizes how challenging it is to build strong security without knowing what features the system may have or whether the process may be altered on the fly. The key concern is that evolving IoT security risks may outpace present IT security measures. The decentralized nature of the IoT, which requires patient interaction with several devices and participation in the healthcare process, is viewed as a potentially uncontrollable risk. A completely automated real-time system and human conduct seem to interact in unpredictable ways.

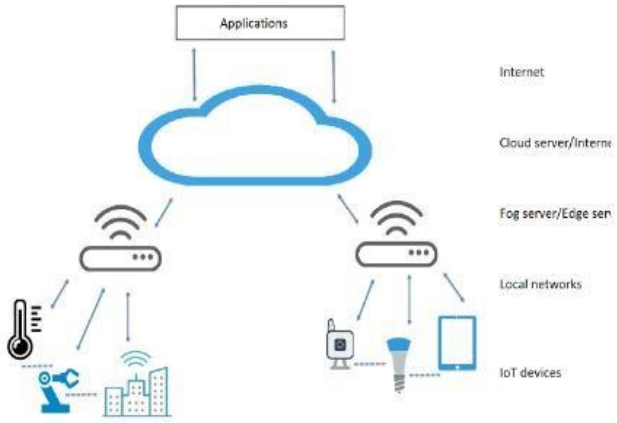

Figure 5

Healthcare will change in the next years thanks to intelligent technologies that are driven by the Internet of Things (IoT) and artificial intelligence (AI). Despite the many advantages of this integration, it is still necessary to handle the myriad security concerns that are present. Having a thorough understanding of the underlying architecture is essential since data security in the Internet of Things may be complicated. The connected networks and tiers of the Internet of Things are shown in Figure 1. Think about the potential vulnerabilities and network entry points offered by each property. This might be an "object" that communicates with consumers through input (like software that gathers data on the healthcare industry) or a sensor that gathers information about the outside world.

TABLE I. IOT ECOSYSTEM AND LAYER WEAKNESSES

Layer	Threat and Vulnerability
Acquisition	• Endpoint attack • Eavesdropping attack • Jamming • Tampering • Authenticity • Device common vulnerabilities
Network	• Data interruption • Dos and DDoS • Eavesdropping • Jamming • Tampering • Misconfiguration • Rogue access points
Integration	• Data interruption • MITM • Spoofing • Relay attacks • Lack of encryption
Analytics	• Lack of encryption • MITM
Software	• XSS • Data corruption • Data loss • Dos and DDoS • SQL injection • Lack of authentication • Lack of encryption • Buffer overflow • Remote code execution • Phishing • Heap overflow

The pertinent literature has listed device-specific vulnerabilities. However, security researchers frequently ignore them. Similar to this, a major problem is the growing use of weak passwords and common Wi-Fi and router credentials. According to OWASP research, the most frequent IoT device vulnerability is weak or hardcoded passwords. On Internet of Things devices, users frequently forget to change their passwords or don't follow standard practices for establishing safe passwords. Even if the Internet of Things promotes socio-economic development and physical well-being, security issues are equally as important as its benefits [7].

IV. SECURITY VULNERABILITIES IN THE HEALTHCARE INDUSTRY

Apps for healthcare are incredibly important services. Compared to other information and apps, healthcare data must be protected, which makes it more important and difficult to keep secure. Medical applications may face several risks, which differ in their sources and scope. The majority of these security issues are brought up in the report. These security risks include Man-in-the-Middle attacks, impersonation, message tampering, and eavesdropping assaults.

- ❖ Eavesdropping

  Hackers can eavesdrop on network traffic by seeing it as it passes via PCs, servers, routers, switches, portable devices, and IoT IoT devices. Network sniffing is another word for eavesdropping. This occurs when malicious actors attempt to get unauthorized access to data moving between two or more devices by using weak or unsecured connections. The prevalence of eavesdropping is particularly high with wireless technologies. This type of assault is referred to as a "man in the middle" attack.

- Impersonation attacks

  This kind of phishing and impersonation assault is a true scam when an invader poses as a real person to demand money or sensitive information from a company. These attacks typically come from individuals who are aiming for high-level targets like CEOs, directors, etc. These bad guys are out to steal money, leak information, or break into a company's network by providing login information or disclosing secret information.

- MITM (Man in the Middle Attack)

  When an attacker tampers with a continuous data transfer or conversation, it is known as a man-in-the-middle attack. Figure 6 depicts the attackers as both legal parties after they put themselves in the "between" of the message. This enables the attacker to intercept data and information from either side while also giving both legitimate parties access to malicious websites or other material in a way that cannot always be discovered until it is too soon. This form of assault is comparable to the telephone game when one person's remarks are passed from person to person until they have altered by the moment they reach the final victim. A man-in-the-middle attack involves the intermediate person attempting to influence the communication without the knowledge of either of the two actual participants to steal personal information or do other harm [8].

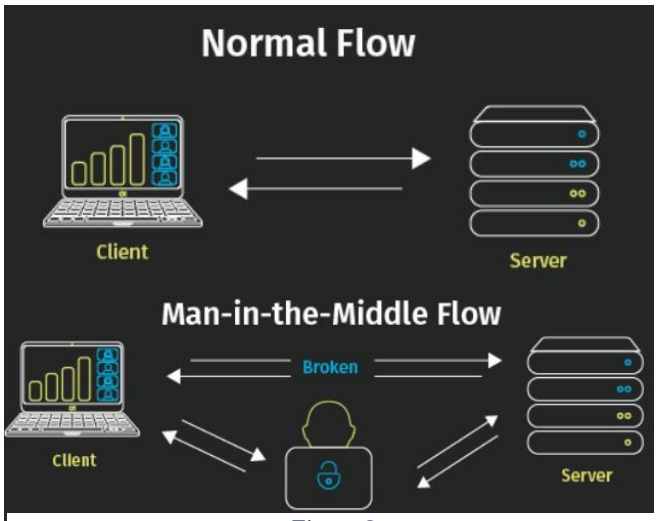

Figure 6

- Jamming

  A hacker intentionally delivers radio interference to a wireless network to launch a jamming attack. As a result, it lowers the frequency ratio at the receiver side and interferes with wireless communication that is already in place.

- Spoofing

  The term "spoofing" refers to the practice of a cybercriminal impersonating a reliable entity or device to trick you into doing something that will be damaging to you and beneficial to the attacker. Any time a cybercriminal disguises their identity as something else, they spoof. Spoofing may be used using a variety of communication routes and calls for different levels of technological skill. When fraudsters mentally mislead potential targets by capitalizing on human flaws like worry, greed, or a lack of technological expertise, spoofing attacks typically include a social engineering element.

- XSS

  An instance of injection is a cross-site scripting (XSS) attack, in which a malicious program is injected into often reliable and harmless websites. Cross-site scripting is when a hacker sends a malicious script to a different end user, frequently through a client-based program, using an internet application. Every online program that incorporates user input into its output without verifying or encrypting it contains holes that make these actions possible. An attacker could send a harmful program to an unwitting user via XSS. The end user's browser appears to be unable to recognize that the program should no longer be believed and will continue to execute the script. The malicious program may obtain the session cookies and authentication information since it thinks the script came from a reliable source.

- Buffer overflow

  By overwriting a program's buffer (memory), hackers can take advantage of buffer overflow vulnerabilities. Changing the application's execution path might cause data to be lost or sensitive information to be made public. For instance, a hacker may add more code, giving the program fresh instructions, and thereby get access to the target machine. Let's assume that attackers are aware of the RAM layout of a program. They could purposely inject data that the buffers are unable to hold and use their script to rewrite executable file parts. To exploit payloads and take over the system, a hacker can, for example, change a pointer [9].

- DOS & DDOS

  A distributed denial of service (DDOS) assault, also known as a denial of service (DoS) attack, involves flooding the target or the area around it with an excessive amount of Internet traffic to disrupt regular traffic to a particular server, service, or system.

  DDoS attacks become effective by using a variety of compromised computer networks as a source of harmful traffic. Computers and other linked assets, such as Internet of Things (IoT) devices, may be exploited by machines [10].

V. LITERATURE REVIEW

Numerous studies have emphasized the challenges because of how quickly technology is developing. to offer solutions and methods to address issues as well. Numerous research studies are advised to assure data security and privacy in IoT applications, particularly in healthcare applications, since technology has invaded many areas of humanity [11]. Proposed Architecture for Medical System Security There have been two security measures recommended. The coexistence proof format for commodities with various tags and a verification schema for IoT-based healthcare systems. Their communication was strong and safe because of their schema. To ensure success, they used their strategy. Researchers developed a centralized data storage system that collected information from several sensing devices. This study tries to safeguard system security, confidentiality, and privacy. They used two different cryptography programs. the fusion of functional and attribute-based encryption techniques. Framework proposed architecture Using Wireless Body Area Networks (WBAN), a cloud-based architecture for secure healthcare applications was created. To secure inter-sensor communication, they used a multi-biometric key generation approach. They connected the EHR that was maintained centrally on the cloud for the healthcare sector. Their strategy created a secure cloud-based architecture that guarded patient data privacy and communication operations. a method for ensuring complete security for the Internet of Things in the healthcare sector. The suggested architecture incorporates end-user authentication and authorization, as shown. End-to-end encryption follows. Finally, a smart gateway connecting cloud services and sensors. To simulate their proposed schema, they produced hardware and software. The cost of communication is reduced by this study. Additionally, they found that this model is 97% faster than the other schemas they examined.

A method to protect existing IoT-based medical systems employing body sensor networks was developed by the author. This study addressed the security issues that body sensor network systems raised and created a remedy for them. When compared to earlier techniques, they shortened the execution time by 42%. The writers provided a description [12].

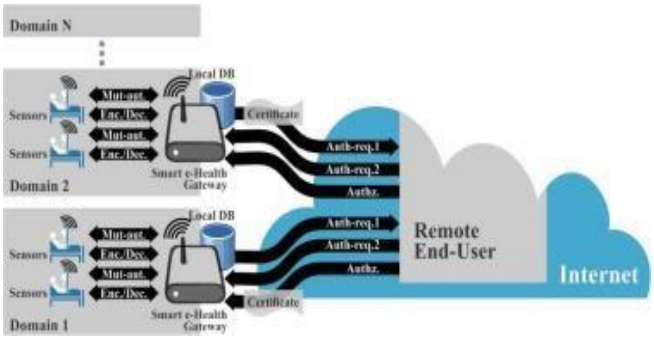

Figure 7

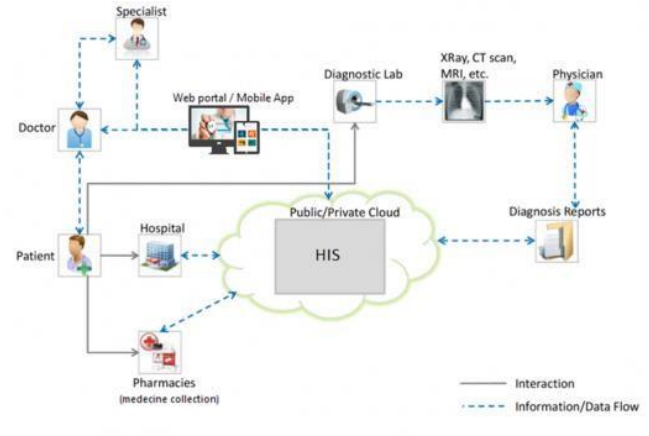

Figure 8

An easy-to-use attribute-based encryption (ABE) solution was proposed to protect data interchange, device connection, and stored data in the IoT framework. The traditional (ABE) IoT schema was formerly quite inclusive. To protect and secure the privacy of the data, they used an encryption algorithm (ECC). They evaluated the communications and processing costs of their schema using matrices. The findings show that the recommended schema is less expensive and quicker than the current schema, even though it has severe restrictions.

VI. SECURITY COUNTERMEASURES

To combat security risks, a variety of security techniques are used. Different types of threats are addressed using a variety of ways. To protect the stored data from numerous threats, some choices include cryptography, identification, and authorization. This article focuses on cryptographic methods for protecting data from various security threats, albeit not all of the partners were included. A flexible architecture like the Internet of Things calls for the use of cryptography and authentication techniques in specific situations to protect data.

Conventional cybersecurity controls are employed as a foundation for newly developed ways since they cannot be applied directly to Internet-of-the-thick application types. This research will explore some of the most used symmetric encryption methods. DES, 3DES, Bluefish, and AES are some of these methods.

- Data encryption – DES

  Data Encryption Standard: IBM developed the DES algorithm in 1977. Using this method, a fixed-length stream of plaintext bits may be encrypted. This plaintext is then transformed into cipher-text that is the same size. Each block has a length of 64 bits, with 56 bits used for the algorithm's key size and the final 8 bits going to the checking party. This method is described as a rather sluggish cryptographic algorithm [13].

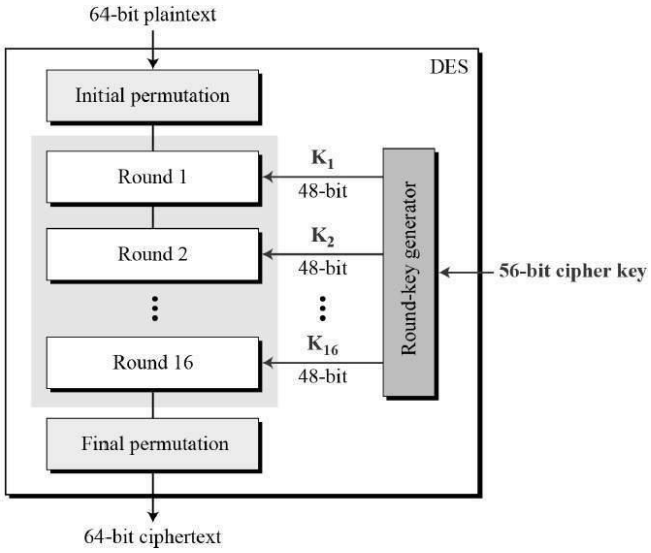

Figure 9

- Blowfish

  In 1993, this method was developed. It uses a key length of 32 to 448 bits and a block length of 64 bits. It was created to ostensibly take the role of the DES algorithm. To be faster and considerably more secure, it uses a variable key size. That algorithm is open-source and available to everyone in the public. Compared to DES and 3DES, it is said to operate more quickly and reliably.

- Triple data encryption – 3DES

  As an improvement to DES, the 3DES Standard was introduced in 1998. This technique ran the DES three times. The block size is similarly 64 bits, with 56 bits being the essential length. This approach beats DES in speed, but it is also seen to be a slow algorithm because it needs to run DES three times. It has better efficiency than DES.

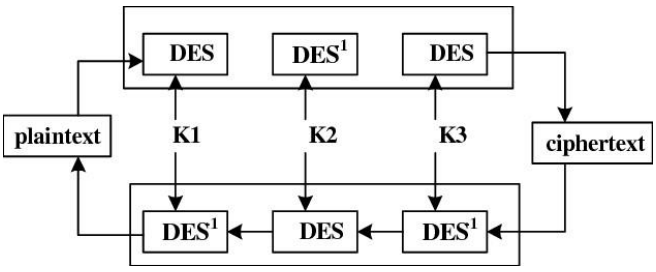

Figure 10

- Advanced encryption standard – AES

  The United States government adopted the Advanced Encryption Standard (AES), a symmetric block cipher, to protect sensitive data. Globally, hardware and software encrypt sensitive data using the Advanced Encryption Standard. It is essential to the preservation of electronic information and the security of government information. The National Institute of Standards and Technology began work on AES in 1997 after recognizing the need for a successor for a Des data encryption standard that was starting to be vulnerable to attackers using brute force [14].

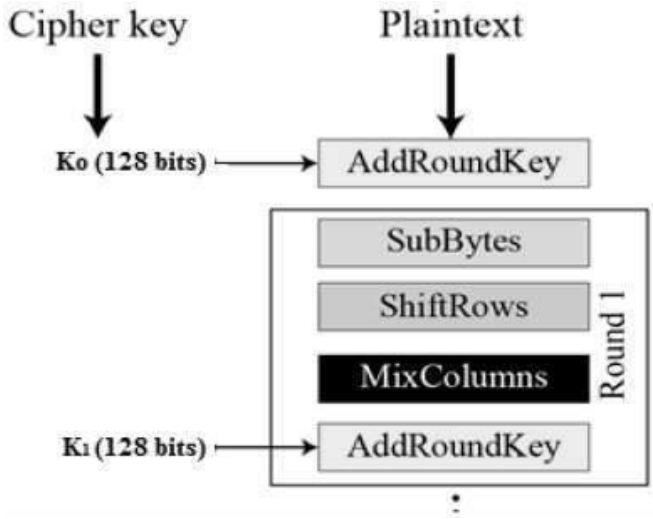

Figure 11

Intelligent medical places a high focus on information security, therefore greater efforts may be made to increase the level of security for medical database networks.

a) Deployment of security professionals

   To constantly monitor, update, and safeguard the networked devices, there must be enough internet security experts working in medical and smart medical facilities. The It gap in the context of smart healthcare will be closed by this. To deal with problems, the clinics need to be staffed with skilled personnel and have efficient incident response strategies.

b) Inventory maintenance

   A complete inventory of every item connected to the network is required for the Internet of Things (IoT). Their operations, together with the bandwidth and interconnections, must be routinely watched over. It is necessary to construct and keep up a vulnerability database with the most current vulnerability reports relevant to the connection's used items. Use the appropriate updates that their providers have provided for upgrading related equipment.

c) Compliance

   Before being used, IoT equipment must pass tests to ensure that it complies with safety standards and other pertinent health product standards [13]. It is important to confirm that the devices can install security upgrades. The legislative conditions and limitations must be followed while gathering and disseminating data.

d) Secure update

Any contact formed with unauthorized IPs must be treated as undesirable traffic, and only authorized IPs should be allowed to provide the update. Only certain ports must be used for connectivity during security patch updates, and those ports must be permanently blocked following the update. Connectivity must only be made using the permitted IPs in the list.

e) Product security

It is necessary to use material from similar manufacturers to expand the network as far as is practical. To lessen the risk of supply chain assaults, the producer must strive to include as few third-party items as possible in their architecture. Before installing a device into the system, the default password must be changed. In a healthcare setting, it is typically preferable to deploy specialized application-focused devices rather than generic IoT devices from third parties.

f) Network segmentation

Micro-segmentation may keep out all unauthorized disclosures from outside the network to the critical equipment. So that the breakdown of one item won't necessarily impact how the network runs, it must be made sure that network materials is adaptable in its connections.

g) Data integrity

Only the authorized individual should have access to the data stored on the storage medium; the public should not. The device must only gather the information that is required, and it must be confirmed that it does not record any superfluous data. It is necessary to maintain regular data backups to lessen any unforeseeable attacks [15].

VII. FUTURE RESEARCH

Numerous studies have been conducted on "Cyber Security Threats and Protections in the Medical Sector," but much more research needs to be done.

VIII. CONCLUSION

Numerous advantages of smart healthcare include speedier diagnosis, wiser choice-making, and proactive treatment. Such networks must include internet security as a core component. However, most E-healthcare systems are exposed to assaults because of several issues. This essay assesses the traits present in both computer security issues and intelligent health system features. The proactive steps that may be performed to enhance the integrity of e-healthcare systems are also highlighted. The suggested preventative measures can be applied as best practices for creating safe Smart Healthcare. This study examined a range of security issues in the healthcare sector. And it covered many of the countermeasures for these kinds of assaults. In literature, cryptography is viewed as the most effective and crucial defense. This article also covered a few of the most used encryption methods.

IX. REFERENCES

[1] A. J. a. O. A. N.S. Abouzakhar, "Internet of Things Security: A Review of Risk and Threats to Healthcare Sector," 2017.

[2] "Healthcare was Most Attacked Industry in 2015," 2015.

[3] E. Perakslis, "Cybersecurity in Healthcare," *New England Journal of Medicine*, pp. 395-397, 2014.

[4] S. Muzammal, "Counter measuring conceivable security threats on smart healthcare devices".

[5] "9 Reasons Healthcare is the Biggest Target for Cyberattacks," *https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/* , 2022.

[6] "Data protection," *https://www.itpro.co.uk/data-protection-0* , 2022.

[7] D. Miessler, "Preparing to Release the OWASP IoT Top 10," *https://danielmiessler.com/blog/preparing-to-releasethe-owasp-iot-top-10-2018/* , 2018.

[8] "Man in the Middle Attack," *https://www.veracode.com/security/manmiddle-attack* , 2022.

[9] "Buffer Overflow," *https://www.imperva.com/learn/applicationsecurity/buffer-overflow/* , 2022.

[10] "Waht is a DDoS attack?," *https://www.cloudflare.com/engb/learning/ddos/what-is-a-ddos-attack/* , 2022.

[11] S. Moosavi, "End to End security schema for mobility enabled healthcare IoT," *Future Generation Computer System*, pp. 108-124, 2016.

[12] A. A. H. A. a. N. H. F.A. Khan, "A Cloud-based Healthcare Framework for Security and Patients," *Data Privacy Using Wireless Body Area Networks*, pp. 511-517, 2014.

[13] "Data Encryption Standard," *https://www.tutorialspoint.com/cryptography/data_enc ryption_standard.htm* , 2022.

[14] GeeksforGeeks, "Advanced Encryption Standard," *https://www.geeksforgeeks.org/advanced-encryptionstandard-aes/* , 2022.

[15] K. G. a. V. R. R. Marshal, "Proactive measures to mitigate cyber security challenges in IoT based smart healthcare networks," 2021.

X.AUTHOR PROFILE

Gunasekara M.V.G.R.S.
Cyber Security Researcher
Undergraduate at SLIIT