IT20620066 – Weththasingha M N G

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

Weththasinghe M N G
IT20620066
AIA – IE3022
Assignment 01
Third year 1st semester
It20620066@my.sliit.lk

***Abstract*— Healthcare is essential to maintaining population health and preventing disease outbreaks. By digitizing medical records, the IoT can help hospitals and healthcare providers monitor patient health more efficiently. Additionally, by providing real-time data, the IoT can help doctors make better decisions about healthcare while this industry is the most frequently targeted by hackers. Limited IT security funding, old or outdated operating systems, and little tolerance for interruption of healthcare services to patch or replace current systems are the vulnerabilities that lead to successful data breaches in the healthcare sector. Furthermore, there are thousands of medical devices in use, many of which lack security safeguards. Institutions would be required to implement both preventative and reactive security measures to reduce risk and mitigate losses. The purpose of this review paper is to evaluate cyber security threats and mitigations in the healthcare sector, with a focus on the Internet of Medical Things.**

Keywords – Cybersecurity, E-healthcare, Internet of things, Threats in Healthcare.

Introduction

E-healthcare has grown in popularity in recent years, posing several data and information security challenges. E-health is a developing field at the crossing points of medical informatics, public health, and businesses that refer to health care services and information presented or improved via the internet and other associated technologies. [1] Healthcare providers are constantly looking for new and innovative ways to improve the quality of patient care. With the increasing use of electronic health records (EHRs), health information technology (HIT) is becoming an even more important part of the healthcare landscape. EHRs are systems that allow health care providers to store, manage, and share patient data. They have revolutionized the way health care is delivered, and they are expected to play a larger role in the future Data breaches have increased dramatically since the document system was replaced with EHR while Data privacy and security are top priorities, particularly in the industry. Two types of data breaches occur which are internal breaches and external breaches. According to the 347, healthcare data breaches of five hundred or more records were reported to the Department of Health and Human Services Office for Civil Rights between January 1, 2022, and June 30, 2022.

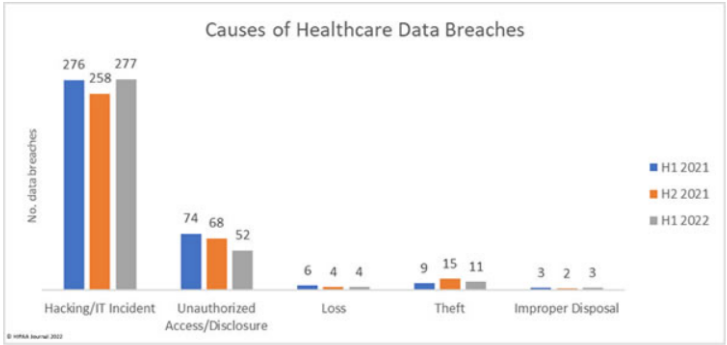


Figure 1

The chart below illustrates the locations where Protected Health Information was stored. [2] The data shows that network servers are by far the most common location of

breached data, which is remotely given the high number of cyberattacks and ransomware attacks. Most data breaches do not include electronic medical record systems. however, breaches at EHR providers have occurred this year, increasing data breaches involving EHRs.

Figure 2 Individuals affected by healthcare data breaches

Figure 2, shows the number of individuals that are affected by healthcare data breaches from 2009 to 2022 (1H) [3]. The diagram shows that the major healthcare data breaches occurred in 2015, which is the worst year so far in data breaches, with nearly 113 million records exposed. Furthermore, 2015 is regarded as the most damaging year possible due to three massive data breach attacks in the healthcare sector: Excellus, Anthem Inc, and Premera Blue Cross. Hackers stole all the patients' information during a data breach. All this information is sufficient for any individual to obtain a loan on behalf of a patient. Furthermore, these attackers sell this relevant data on the Dark Web to individuals who use it to engage in illegal activities such as drug purchases, financial schemes, or even false insurance claims.

Why do they target the healthcare sector?

According to the most recent Global Data report, 'Cybersecurity in Healthcare - Thematic Research,' increased data access opens up more opportunities for security vulnerabilities in the healthcare industry sector. As remote medicine became more popular during the COVID-19 pandemic, the Internet on medical things became increasingly connected. However, cyber security threats are more prevalent in the healthcare sector.

- Hospitals were gathering patient information because it was valuable and important for future things. On the other hand, cybercriminals can take advantage of them. Data breaches are a lucrative business for criminals. One method for hackers to profit from stolen data is to sell it in larger quantities to other criminals on the dark web. Massive amounts of stolen data records may be found in these collections. The data can then be used for criminal purposes by the buyers. Identity theft is a violent act in which the victim's private details are used to obtain benefits at the expense of the victim. Many internet services require users to provide personal information like their full name, home address, and credit card number. Criminals steal this information from online accounts to commit identity theft, such as by using the victim's credit card or applying for loans in their name. Criminals use stolen login details to gain access to accounts containing payment information, such as online shopping accounts. This is known as account takeover, and it frequently leads to identity theft. [4]

- Medical technology advancements nowadays have few drawbacks. Modern medical equipment includes X-rays, insulin pumps, and heart monitors. These new devices add new attack vectors to internet security and patient information protection. It is common for healthcare devices to serve only one purpose. They are not designed for safety. While the devices may not contain the desired patient data, they could be used to launch an attack against a server. Hackers are aware that healthcare devices do not save patient data. Hackers see insecure devices like laptops and PCs as easy targets. [5]

- Staff must access data remotely; it will increase the number of attack vectors in a particularly big way. In the healthcare industry, collaboration is essential, with units working together to provide basically the best solution for each patient in an actual major way. Those who require information are not always seated at their desk; they mostly are frequently working remotely from various devices in a

subtle way. Remotely connecting to a network from new devices definitely is risky because not all devices are secure in a particularly big way. Furthermore, even the simplest generally basic cybersecurity sort of the best procedures for all intents and purposes is frequently basically unknown to healthcare staff in a subtle way. Vulnerable devices must never gain network access, as a sort of single hacked device can subtly expose an entire organization.

Healthcare workers do not have enough time or motivation to learn about modern technologies or software security. Healthcare professionals are among the busiest and most in-demand professions in the country. Staff work long hours and under pressure, which means they do not have the resources or the time to add internet security processes to their work overload. Medical professionals lack the expertise required to acknowledge and mitigate cyberattacks.

The immeasurable quantity of devices used in hospital services makes it difficult to maintain security. In a hospital, there are lots of devices that are connected to the hospital server. The staff who do not have expert knowledge about cyberattacks cannot maintain all the devices without any issues.

Healthcare data must be accessible and shareable. Staff must have access to confidential patient data both on-site and remotely, and on multiple platforms. Because the healthcare profession is typically urgent, a team must be capable of sharing data quickly. There is no time to think about the possible security consequences of their devices.

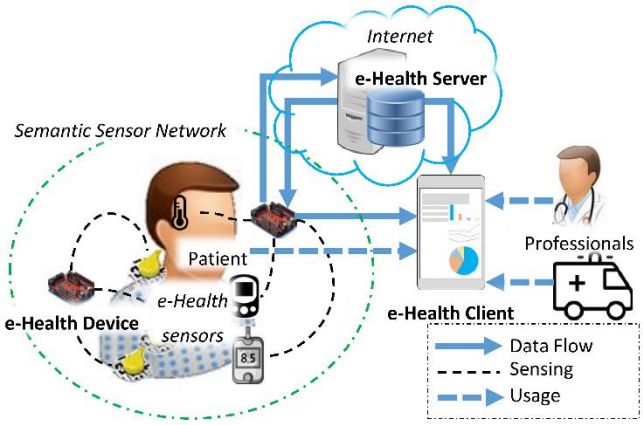
In the world, 90% of institutions in the healthcare industry have been compromised. [4] Additionally, the impact of inadequate security is getting worse. Hackers "killed" (simulated) patients at the 2018 RSA Conference in the United States of America without the doctors being aware that the operating room had already been taken over. According to IBM X-2016 Force's Cyber Security Intelligence Index, healthcare overtook the financial services sector in 2015 as the most frequently targeted industry for data-stealing cyberattacks. [6]

HEALTHCARE IOT SECURITY

Before the Internet of Things, patients could only communicate with doctors face-to-face, over the phone, or by text. There was no feasible mechanism for medical professionals or facilities to continuously evaluate patient health and offer advice. Remote monitoring in the healthcare industry is now possible thanks to the Internet of Things (IoT)-enabled devices, releasing the ability to keep patients safe and healthy and enabling doctors to provide excellent treatment. As doctor-patient interactions have gotten simpler and more effective, it has also raised patient participation and satisfaction. Additionally, [7] remote patient monitoring shortens hospital stays and avoids readmissions by keeping an eye on patients' health. IoT has a massive impact on lowering healthcare expenses and enhancing patient outcomes. Without a doubt, IoT is revolutionizing the healthcare sector by changing how devices and users interact while providing healthcare solutions.

Applications of IoT in healthcare are advantageous to patients, families, doctors, hospitals, and insurance providers. [8] An attacker may use weak authentication methods, such as those present in integrated web servers located throughout the hospital, to gain access to crucial systems. As a result, the hacker might be able to take down medical systems, get 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 breach of security could become unmanageable and even result in the patient's death. It follows logically from this that these devices require protection. As a component of their healthcare tracking and data analysis, hospitals could use the information gathered by the Internet of Things sensing devices to assist their patients. The sensors themselves are designed to continuously collect data. [9]

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 numerous devices and participation in the healthcare system, is viewed as a potentially uncontrollable risk.



A completely automated real-time system and human behavior seem to interact in unpredictable ways.

Artificial intelligence (AI) will be used more frequently in the healthcare industry as a result of the complexity and growth of data in the sector. Payers, care providers, and life sciences organizations currently use a variety of AI technologies. The main application categories include recommendations for diagnosis and treatment, patient involvement and adherence, and administrative duties. Although there are many situations in which AI can accomplish healthcare duties just as well as or better than people, implementation issues will keep the jobs of preventing the widespread automation of healthcare workers for a substantial period. [10]

SECURITY VULNERABILITIES IN THE HEALTHCARE INDUSTRY

The importance of healthcare apps is immense, and it is challenging to keep them secure. Due to the nature of the data, they collect, the applications must be well-guarded. This study aims to identify the various security threats that can affect the operations of medical apps. Some of these include impersonation, eavesdropping, and man-in-the-middle attacks.

1. Buffer overflow Attacks

A buffer overflow (or buffer overrun) happens when the amount of data generated is greater than the memory buffer's storage capacity. They frequently happen because of incorrect inputs or inadequate buffer space allocation. [11] If the transaction overwrites,

Layer		Threats and vulnerabilities
1. Market or application domain	Smart grid, connected home, smart health, or smart cities	Endpoint attack Eavesdropping attack Jamming Device Common vulnerabilities (operating system vulnerabilities, malware, weak encryption.)
2. Sensors that allow the application to perform actions	temperature sensors, humidity sensors, electric meters, smart phones	
3. Interconnection	DECT, ULE, Wi-Fi, Bluetooth, Zigbee, NFC	Data interruption Dos and DDoS Eavesdropping Jamming Tampering Misconfiguration Rogue access points
4. Integration	Geographic data, population data, Economic, GIS	Data interruption MITM – man in the middle attacks Spoofing Relay attacks
5. Analytics	Machine Learning, Predictive analytics, Data Mining	Lack of encryption MITM – man in the middle attacks
6. Application and software	Software-defined network (SDN), service-oriented architecture (SOA), collaborations, Apps, Clouds	XSS – cross-site scripting Data corruption Data loss
7. Services	energy management, health management, education, transportation	

Table 1:IoT systems and vulnerabilities [12]

executable code, it can cause the program to behave unpredictably and crash. Hackers can exploit a buffer overflow vulnerability to modify a program's memory. This can lead to a reaction that can cause the destruction of data or expose confidential information. For instance, an attacker could add more code to a program to access a target system. [13]

2. DOS & DDOS

A distributed denial of service (DDOS) attack, 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. [14]

DDoS attacks become effective by using a variety of compromised computer networks as a source of harmful traffic. PCs and other connected assets, such as Internet of Things (IoT) devices, may be among the exploited equipment.

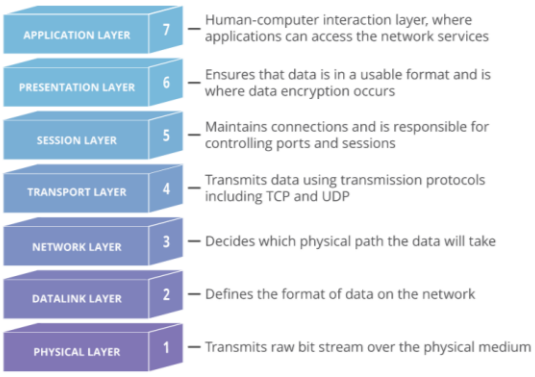


Figure 3: The OSI model is a conceptual framework used in the DDOs Model to describe network connectivity in 7 different layers.

3. XSS – Cross-site scripting.

Cybersecurity professionals refer to a certain group of online application security flaws as cross-site scripting (XSS). A program has a cross-site scripting vulnerability if an evil hacker may insert (inject) unwanted commands into valid client-side code, typically JavaScript, which is run by a browser on behalf of the online application.

In the healthcare sector, when a web application fails to properly sanitize user input, the resultant page may reflect or store the user's input (such as malware code). Code review should be done before the release of the program to best protect against the risks posed by XSS vulnerabilities. [15]

4. MITM – Man in the middle attacks

Attackers can utilize a variety of security risks to take advantage of vulnerable applications. Some of these attacks can be carried out by threat actors using automated software, while others necessitate a more active engagement on their part. An eavesdropping assault known as a "man-in-the-middle" occurs when an attacker intercepts a data transfer or communication that is already in progress. The attackers place themselves in the "middle" of the transaction and then pose as both authorized participants. This enables an attacker to send malicious links or other material to both legitimate participants in a way that may not be discovered until it is too late. The attacker is also able to intercept information and data from either party. [16]

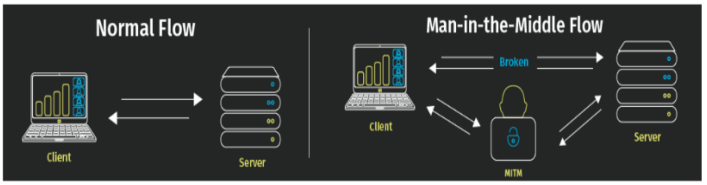


Figure 4:Difference between the normal flow and MITM flow

5. Spoofing

Attacks involving spoofing can happen in one of two ways. The first sort of assault is local spoofing, which is conducted when the victim and the attacker are on the same network. This is by far the simpler of the two kinds of spoofing attacks. The attacker can sniff network data, which allows them to find vital bits of information they need to start the attack. Blind spoofing is the second method that can be used to conduct this attack. This is a far more complex and advanced assault The attacker is not connected to the same local subnet when the assault is initiated in this way. Spoofing can be used using a variety of communication routes and calls for distinct levels of technological skill. [17]

6. Phishing

Healthcare is susceptible to phishing, like many sectors of the economy. Approximately 66% of malware was started as an email attachment, according to Verizon research. Even though it is doubtful that the WannaCry ransomware started in an email, phishing is still a common way for malware to spread. Personal information, including login passwords, is nevertheless also at risk from phishing emails and messages. In 2020 and 2021, the healthcare sector was repeatedly targeted by hackers. Even though they all use it differently, email is unquestionably the most common. If email is not protected, security breaches will happen. And that leads to the leaking of confidential data in the healthcare sector. [18]

According to a recent survey by the National Health Information Sharing and Analysis Center, fake emails are most common in the healthcare sector. However, nothing is being done to address this, with 98% of medical institutions failing to implement Domain-based Authentication Services,

Reporting & Conformance as a first step in assisting to prevent phishing (DMARC). [19]

7. Cloud computing adoption and online security

The healthcare industry is embracing cloud computing because it provides advantages including improved data access and cost-effectiveness. A CAGR of 20.5% is predicted for cloud computing utilization in the healthcare industry between now and 2020. But cloud computing has its own set of dangers. According to advisories from organizations like OWASP, data within cloud storage needs to be properly protected. Strong encryption mechanisms and appropriate and efficient authentication methods, such as second factor and risk-based, are required for the protection of data while it is at rest and while it is being transferred between web services. [20]

8. Ransomware and other Malware

Although malware is a major issue for all industries, it can affect one's life or death in the healthcare sector. The reporting and services used in healthcare are intricately intertwined. This intricate network is particularly susceptible to ransomware and other malware assaults since it shares information on our behalf to improve our health. [20]

Literature Review

Numerous studies have emphasized the challenges because of how quickly technology is developing. Moreover, it offers solutions and methods to address issues as well. Numerous research is 5advised to assure data security and privacy in IoT applications, particularly in healthcare applications, as technology has invaded many areas of life.

A method for securing current IoT-based medical systems employing body sensor networks was developed by researchers. This study addressed the security issues that body sensor network systems raised and created a remedy for them. When compared to earlier techniques, they cut the execution time by 42%. There have been two security measures recommended. The identification scheme for IoT-based medical systems and the coexistence proof scheme for goods with multiple tags. Their communication was strong and safe thanks to their schema. To ensure success, healthcare systems used their plan. [21]

A cloud-based architecture for actually secure healthcare applications utilizing Wireless Body Area Networks was created, according to the [22] Proposed framework architecture (WBAN) in a big way. To secure inter-sensor communication, they used a multi-biometric key generation approach. They connected the EHR that was generally kept centrally on the cloud for the healthcare sector. Their strategy created a secure cloud-based architecture that guarded patient data privacy and communication operations.

According to the [23] Due to the high value of Protected Health Information (PHI) on the dark web and the unlawful illegal market, data breaches are most common in the healthcare industry. These data breaches can occur for several reasons, including phishing, denial-of-service assaults, and even the human element in the system.

Security Countermeasures

.

In the healthcare sector, where nearly every aspect of the industry is being impacted by technology, to prevent security threats, a variety of security techniques are used. A flexible framework like the Internet of Things demands the use of cryptography and authentication techniques in specific situations to protect data. Consumers can now utilize mobile devices to obtain patient records, monitor their health status, organize, and manage healthcare, and perform a variety of jobs more simply thanks to the invention of new app technology and digital advancements. Diverse 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. [24]

Health and the public health sector cater to the most vulnerable population in our communities and have become one of the most targeted sectors by cyber criminals, according to a report by the National Crime Agency (NCA) released earlier this year on behalf of the World Health

Organization (WHO). [25]

Conventional cybersecurity controls are provided as a foundation for newly developed ways because they cannot be applied directly to Internet-of-the-thick application types. DES, 3DES, Bluefish, and AES are some of these methods.

1. Data Encryption Standard

The most well-known block cipher algorithm in the world is based on the DES algorithm. It was developed by IBM and designated as the American standard FIPS 46 in 1977. It is a 56-bit key, 16-round, 64-bit block cipher. [26] In DES, a round consists of a substitution (confusion) and a permutation. Using this method, a fixed-length stream of plaintext bits can be encrypted. This plaintext is then transformed into cipher text that is the same size. Even today, the DES algorithm can withstand the majority of common attacks. But owing to the tiny key size, DES is no longer advised for use.

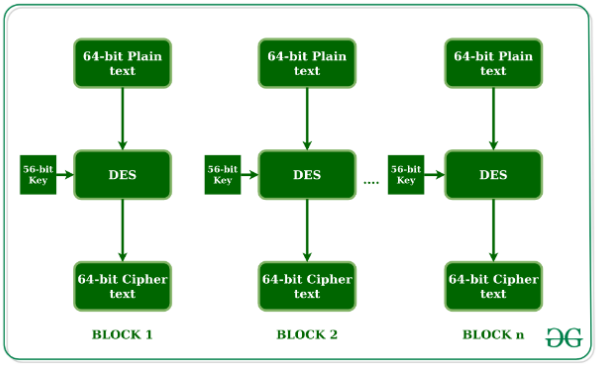


Figure 5: Data encryption standard (DES)

2. Blowfish

Bruce Schneier created the encryption method known as Blowfish in 1993 as a replacement for the DES Encryption Technique. Since no efficient cryptanalysis method has been discovered yet, it is substantially faster than DES and offers a good encryption rate. One of the first safe block ciphers, it can be used by anybody since it is not protected by any patents. [27]

Compared to DES and 3DES, it is said to operate more quickly and reliably.

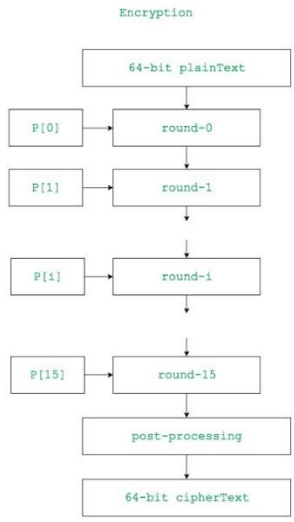


Figure 6: Blowfish Algorithm

3. Triple Data Encryption

In the Triple Data Encryption Standard (DES), each data block is subjected to three separate applications of block cipher algorithms. In Triple DES, the key size is raised to provide more security through encryption capabilities. Data is stored in blocks of sixty-four bits each. Bundle keys are three keys with a total of fifty-six bits. It is superior to DES in terms of efficiency. In terms of data encryption standards, there are three keying options:

- being independent of each other
- Keys 1 and 2 are separate.
- The three keys are all the same

Triple DES is the name of key option #3. Triple DES keys have a length of 168 bits; however, their security is just 112 bits. [28]

4. Advanced encryption standard – AES

A cryptographic technique that has received FIPS approval is described in the Advanced Encryption Standard (AES), which can be used to secure electronic data. A symmetric block cipher algorithm that can both encode (encipher) and decode (decipher) information is the AES algorithm. Data is encrypted into an unreadable format called ciphertext, which is then decrypted to restore the original plaintext form of the data. The AES algorithm can encode and decode data in blocks of 128

bits utilizing cryptographic keys with lengths of 128, 192, and 256 bits. [29]

Future Research

The healthcare industry has significantly advanced thanks to the Internet of Things (IoT), which has brought forth new dynamics like automatic insulin delivery, pressure and temper monitoring, Parkinson's disease tracking, connected inhalers and contact lenses, and more. The Internet of Medical Things (IoMT) offers fewer challenging methods that advanced patients appreciate. Patients gain from rest, intense participation, and a few private medical appointments. Carriers now have access to more precise information, better diagnostics, and more effective time management.

E-healthcare sector security is highly significant, and there are a lot of other topics to study and do research on. There are many diverse types of research available on this issue, "Cyber Security Threats and Mitigations in the Healthcare Sector." However, in my opinion, there is a lack of research that explains how cybercriminals use patient data in the underground economy and what unique defenses they can employ to mitigate it.

Not only that but also there are not many reports regarding data usage as an outside theft or inside misuse. Patient data theft for monetary gain or evil purpose is a common example of insider misuse which could not passes without consideration.

Conclusion

The review paper's focus was on the Internet of Medical Things cybersecurity vulnerabilities and prevention in the healthcare sector. In this review paper, attempted to identify the threats facing the healthcare industry, which places a strong emphasis on the Internet of Medical Things, as well as the best modern technologies that must be applied in the industry going forward. It determines how to mitigate those threats. After reading numerous research papers and appropriate websites to obtain the data needed to complete this review report. By using the best modern technologies available, such as the Internet of Medical Things, we can help to secure the healthcare industry against cyberattacks.

This review paper covered the proactive measures that might be taken to improve the security of E-healthcare systems. The preventative measures provided may be used as best practice guidelines for creating a safe Smart Healthcare system. Future studies could be done relying on this review paper to improve healthcare devices, develop modern technologies, and figure out the safest ways to use technology that already exists. 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.

REFERENCES

[1] s. alder, "1H 2022 Healthcare Data Breach Report," 2022.

[2] "HIMSS," 22 august 2022. [Online]. Available: https://www.himss.org/resources/cybersecurity-healthcare.

[3] [Online]. Available: https://www.imperva.com/learn/application-security/buffer-overflow/.

[4] "Imperva," [Online]. Available: https://www.imperva.com/learn/application-security/buffer-overflow/.

[5] H. Basnayaka, "Cyber Security threats and mitigations in the Healthcare Sector with emphasis on medical internet of things and SDN," 2022.

[6] "Security week," 2016. [Online]. Available: https://www.securityweek.com/healthcare-was-most-attacked-industry-2015-ibm.

[7] "rout ledge," 12 11 2019. [Online]. Available: https://www.routledge.com/blog/article/iot-in-healthcare-and-the-advances-in-remote-patient-monitoring. [Accessed 23 04 2022].

[8] R. Karjag and M. J. Manager, "WIPRO," [Online]. Available: https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/. [Accessed 24 09 2022].

[9] A. X. Gilies, "Tech Target," Tech Target, [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT. [Accessed 22 09 2022].

[10] T. Davenport, "The potential for artificial intelligence in healthcare," *Future health Journal,* 2019.

[11] S. M. S. ALHusayn and D. E. Alsuwat , "The Buffer

Overflow Attack and How to Solve Buffer Overflow in Recent Research," vol. 2, no. 19, 2020.

[12] "tutorial and example," 16 12 2019. [Online]. Available: https://www.tutorialandexample.com/iot-ecosystem.

[13] "Imperva," [Online]. Available: https://www.imperva.com/learn/application-security/buffer-overflow/. [Accessed 24 09 2022].

[14] "Cloud flare," [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/. [Accessed 24 09 2022].

[15] "Invicti," [Online]. Available: https://www.invicti.com/learn/cross-site-scripting-xss/. [Accessed 23 09 2022].

[16] "Veracode," [Online]. Available: https://www.veracode.com/security/man-middle-attack. [Accessed 23 09 2022].

[17] M. Gregg, Hack the Stack, 2006.

[18] "HEALTH IT SECURITY," 21 3 2021. [Online]. Available: https://healthitsecurity.com/news/the-phishing-problem-in-healthcare. [Accessed 23 09 2022].

[19] w. Priestman, and T. Anstis, "Phishing in healthcare organisations: threats, mitigation and approaches," *BMJ Health Care Inform*, 2019.

[20] S. Morrow, "INFOSEC," 8 1 2018. [Online]. Available: https://resources.infosecinstitute.com/topic/top-10-threats-healthcare-security/. [Accessed 23 09 2022].

[21] P. Gope, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics* , vol. 63, no. 11, 2016.

[22] F. A. Khan, A. ali and H. Abbas , "A cloud-based healthcare framework for security and patients data privacy using wireless body area networks," Niagara Falls, Ontario, 2014.

[23] J. Reddy and N. Elsayed, "Data Breaches in Healthcare Security Systems," ohio, 2022.

[24] S. Talukder, "Mobile Technology in Healthcare Environment:," Florida.

[25] "Cyber-Threats and Countermeasures in the Healthcare Sector," *IEEE Access*, 2018.

[26] H. Bidgoli, Encyclopedia of Information Systems, 2002.

[27] "Geeks for geeks," [Online]. Available: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/.

[28] "Tech Pedia," [Online]. Available: https://www.techopedia.com/definition/4144/triple-des. [Accessed 24 09 2022].

[29] [Online]. Available: https://www.nist.gov/publications/advanced-encryption-standard-aes. [Accessed 23 09 2022].

Weththasinghe M N G

IT20620066

Third year

Undergraduate

BSc (Hons) Cyber Security