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

Gallage E.D.S – IT21385414
Faculty of Computing (Specializing in Cyber Security)
Sri Lanka Institute of Information Technology (SLIIT) Malabe, Sri Lanka.

***Abstract*— The healthcare sector's reliance on digital technologies and the Internet of Medical Things (IoMT) has led to improved patient care and operational efficiencies. However, this has also created significant cybersecurity challenges. This research review examines cyber security threats in the IoMT ecosystem, including ransomware attacks, data breaches, and potential device compromise. The review identifies emerging trends, gaps in knowledge, and pressing issues in healthcare cybersecurity. It evaluates current mitigation strategies, including encryption and threat intelligence sharing, to protect patient data integrity and privacy.**

Keywords—IOT, cyber-security, healthcare, threats, Medical Device.

I. INTRODUCTION

Patient care, medical research, and operational efficiency have all been revolutionized in recent years by the adoption of digital technologies in the healthcare industry. This transformation has been significantly facilitated by the development of the Internet of Medical Things (IoMT), which allows connected medical devices and systems to improve diagnosis, treatment, and healthcare administration. However, as the healthcare sector relies more and more on connected technologies, it must contend with an increase in cyberthreats that aim to compromise the availability, confidentiality, and integrity of sensitive patient data.

This study explores the complex landscape of cybersecurity risks that affect the healthcare industry, highlighting the difficulties brought on by the Internet of Medical Things. The attack surface grows as medical devices become smarter and more connected, opening new ways for malicious actors to exploit flaws. Successful cyberattacks in the healthcare industry have far-reaching effects that go beyond financial loss, affecting patient safety, privacy violations, and the continuity of vital services.

The main goal of this study is to thoroughly examine the cybersecurity risks that the healthcare sector faces, with a focus on IoMT in particular. We seek to define effective mitigation strategies and best practises that can strengthen the resilience of healthcare systems against cyber threats by comprehending the changing threat landscape. To help healthcare organizations, policymakers, and cybersecurity experts navigate the intricate intersection of healthcare and cybersecurity, this research goes beyond theoretical considerations.

This review paper aims to contribute valuable insights that empower stakeholders to actively protect patient well-being, uphold data privacy, and ensure the continued trustworthiness of healthcare systems in an era of rapid digital transformation as we navigate the complex web of technological advancements and potential vulnerabilities in the healthcare sector.

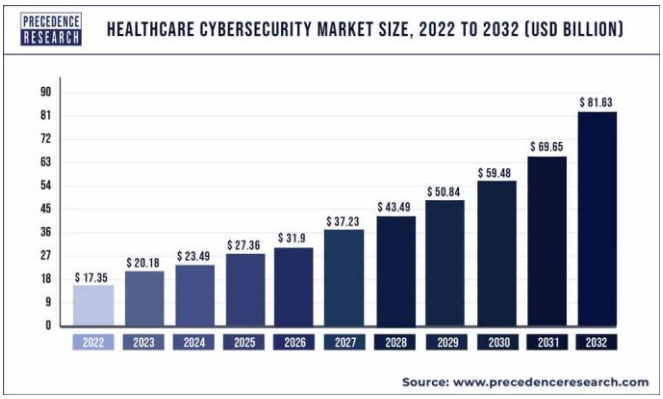

Figure 1: Healthcare cyber security market size

II. RESEARCH OBJECTIVES

The review paper document details the cybersecurity risks to the healthcare industry as well as countermeasures. Nowadays, cyber-attacks pose a threat to enterprises all over the world. Therefore, enterprises face a variety of difficulties because of cyber-attacks. They must therefore use threat and attack mitigation techniques to ensure their safety. This review paper discusses ways to stop cyber-attacks, incidents that occurred because of cyber-attacks, and how businesses were able to recover from cyber-attacks by utilizing a variety of mitigation techniques. Additionally, it describes the various types of assaults, talks about how they happen, and explains why people commit cyber-attacks.

III. Review of the Literature

A. *Why Target Healthcare? and the Threats*

Medical professionals and patient data have become incredibly valuable targets for cybercriminals as more healthcare providers and medical professionals adopt digitization in almost all aspects of their daily tasks and as more health records convert to electronic health records (EHRs). Ransomware attacks against medical institutions are on the rise. [1] Internet attacks are a growing threat to businesses, endangering routine operations and compromising patient data. Healthcare professionals frequently work long, demanding shifts and don't have the time or resources to learn about the risks associated with using the internet. A comprehensive overhaul of online security would likely cause too much disruption for many organizations to even consider.

- Healthcare personnel lack online risk education. [2]

Medical professionals lack the expertise needed to identify and counteract online threats. It is simply not possible for every member of the healthcare staff to be fluent in cybersecurity best practices due to budget, resource, and time constraints. [2] Although cybersecurity solutions are complicated, their user interface must be straightforward. A rapid and simple-to-access secure network is necessary for medical staff. Additionally, they require the assurance that patient data is secure. Solutions like MFA and SSO are becoming more and more popular because they use a secure one-time code to add extra security layers without requiring the user to know anything besides their login credentials.

- Using outdated technologies

Although medical technology has made incredible strides in recent years, not all facets of the healthcare sector have kept up. Medical technology is frequently becoming out of date due to tight budgets and reluctance to learn new systems. [2]
The most recent version of every piece of software should always be installed in hospitals using methods that still permit system updates.
Bug fixes are frequently included in these to keep systems largely secure. However, the vendors will stop providing updates when the software reaches its end of life. It is still possible to lower the risk of cyber-attacks by adding more layers of security in situations where switching to more secure software is not an option or where medical staff doesn't want to deal with the hassle. If one system is compromised, an MFA solution can limit an attacker's lateral movement through the network because they won't be able to log in to other protected systems.

- Medical devices are an easy entry point for attackers. [2]

The benefits of modern medical technology advancements are few. A few examples of modern medical technology are X-rays, insulin pumps, and heart monitors. These new devices provide more attack vectors in terms of internet security and the privacy of patient information. Medical equipment is frequently used exclusively for that purpose. They are not designed to be safe. Even if the devices don't have the required patient data, they might still be used to attack a server. In the worst case, attackers may completely take control of medical equipment, preventing medical personnel from providing vital life-saving care. The fact that patient data is not stored on medical devices is known to hackers.

- For attackers, confidential patient information is extremely valuable. [2]

Security experts claim that hackers are increasingly focusing on the $3 trillion U.S. healthcare sector because it still relies on many outdated computer systems without the most recent security features. [3]
The ability to sell huge amounts of personal data for profit is making the healthcare sector a much more attractive target for attackers as they find new ways to profit, according to Dave Kennedy, CEO of TrustedSEC LLC and an expert on healthcare security. Hospitals have poor security, making it simple for these hackers to obtain a lot of personal information for medical fraud. [3]
Cyber security experts describe the black market for stolen patient data in detail.
The data that can be purchased includes names, birth dates, policy numbers, diagnosis codes, and billing information. Experts who investigated into cyber-attacks on healthcare organizations claim that fraudsters use this data to make fake identifications to buy resalable medical supplies or medications or they combine a patient number with a fake provider number to submit false insurance claims.

- Staff must access data remotely, increasing attack opportunities. [2]

In the healthcare sector, teamwork is essential as departments cooperate to offer each patient the best solution. People who need to access information are frequently working remotely from various devices rather than sitting at their desks. [2]
Remotely connecting to a network from new devices is risky because not all of them will be secure. Additionally, healthcare staff frequently lacks knowledge of even the most basic cyber security best practices. Compromise devices must never be permitted access to the network because just one compromised device can expose an entire organization to risk.
RBA (risk-based authentication) is one option for companies with mobile workforces. This solution simplifies risk analysis by enabling IT staff to set up rules that base a device's risk on factors like the user, their location, and more. Any unusual activity is then recorded to ensure that malicious software cannot access confidential patient information.

- Maintaining security is challenging due to the vast number of devices used in hospitals.

Nowadays healthcare organizations oversee a vast network of connected medical devices as well as enormous amounts of patient data. The thousands of medical devices connected to their network that pose a threat to attackers can be managed by larger organizations. [2]

IT professionals are tasked with protecting an entire hardware network against intrusions because healthcare staff is frequently too busy to stay informed about the most recent device threats. Medical device hacks and data breaches can affect the entire network due to a single compromised device. Healthcare professionals must be able to operate their own devices to some extent. This will free up IT experts to deal with trickier network security and IT problems. A self-service portal is offered by some MFA solutions, allowing users to reset security PINs and other items on their own. This helps lighten the load on the support desk.

B. Healthcare IOT Security

IoT in healthcare has become a growing significant market, especially in recent years as healthcare developments have taken center stage. According to research, the global healthcare IoT market is anticipated to reach $534.3 billion by 2025, suggesting that this trajectory is likely to continue. Unfortunately, despite its many advantages, expanding IoT also increases risks and security attacks by giving cybercriminals a larger attack surface to target. [4]

In 2021, the healthcare industry experienced a marked increase in IoT attacks. The market's increased adoption of IoT doesn't seem to be slowing down this trend. Therefore, it's essential to be constantly aware of the risks associated with technological advancement and to take the necessary precautions to avoid them.

C. Security Vulnerabilities in the Healthcare Industry and Preventive Measures

As the healthcare sector pushes for technological advancements, security issues are becoming more problematic. Among these difficulties are preventing patient data breaches and addressing new dangers related to connected medical devices. A dynamic but risky environment is produced by the enormous amount of health information that is digitally stored and using Internet of Things (IoT) devices. Risks like ransomware attacks, which can compromise patient data and disrupt crucial systems, are a recurring worry. Vulnerabilities are also a result of human error, such as falling for phishing scams.

Several cybersecurity-related problems plague the healthcare sector. These problems range from distributed denial of service (DDoS) attacks that impair hospitals' ability to provide patient care to malware that compromises the security of systems and the privacy of patients. [5]

A. Ransomware

Malware known as ransomware encrypts a victim's files and requests payment to decrypt them. The delivery of care could be severely disrupted by this attack, which could also compromise sensitive patient data and result in enormous financial losses. [6]

Critical processes in the healthcare sector are slowed down or rendered completely inoperable when this happens. Hospitals are then forced to revert to using pen and paper, which slows down the healing process and ultimately consumes funds that might have been used for hospital modernization. [7]

When compared to other industries, the health sector has experienced tremendous growth due to ransomware. This ransomware has a significant impact on this industry. 66% of health service organizations experienced one of these attacks in the previous year. Quantitatively, these risks have increased significantly. This is malicious software that accesses an organization's electronic files. This causes the service process to lag. On almost 60% of the machines in an organization, these attacks typically take place. The majority of this is produced by opening emails.

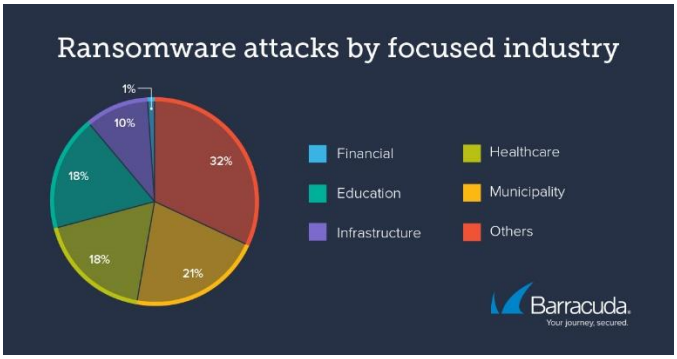

Figure 1: Ransomware attacks by focused industry

Ransomware typically spreads to victims' computers in one of three ways:

- Through malicious links in phishing emails.
- Malicious attachments that users click.
- By seeing a malicious advertisement (malvertising).

Biggest Healthcare Industry Ransomware attacks,

- Medibank

9.7 million customers' personal information, including information on 1.8 million international customers and prominent Australian politicians Prime Minister Anthony Albanese and cybersecurity minister Clare O'Neil, were stolen by Russian-based hackers thought to be affiliated with the infamous REvil ransomware gang. Patient

names, dates of birth, social security numbers, and, in some cases, medical records were among the data stolen. The cyberterrorists demanded a $10M ransom, but Medibank refused to comply, claiming, "We believe there is only a limited chance paying a ransom would ensure the return of our customers' data and prevent it from being published." [8]

- Regal Medical Group

This medical practice in Southern California was the target of a ransomware attack in December 2022, and patients were informed in early 2023. According to the group, "the categories of impacted personal information may include, among other things: your name, address, date of birth, diagnosis and treatment, laboratory test results, prescription data, radiology reports, Medicare ID number, health plan member number, and phone number (for some, but not all, potentially impacted individuals)." [8]

Preventive Measure against Ransomware Attacks.

1. Comprehensive Employee Training:

   The first line of defense against cyber threats is frequently the workforce. To inform staff of the dangers of ransomware, phishing emails, suspicious attachments, and social engineering strategies, hold regular training sessions. Give them the tools they need to quickly spot and report potential security breaches. Create a culture of cybersecurity awareness throughout the business to encourage a pro-active approach. [9]

2. Access Controls and Privileged Account Management. [9]

   Limit user permissions and the potential impact of a ransomware attack by implementing strict access controls. Use multi-factor authentication and strong, individual passwords for each account to increase security. To lessen the risk of unauthorized access, review and update user privileges on a regular basis based on job roles.

3. Network Segmentation. [9]

   By isolating sensitive data and crucial systems, network infrastructure segmentation prevents ransomware from spreading laterally. Establish strict access controls and firewalls between each zone of the network and divide it into separate areas. By limiting the spread of ransomware across the entire network, this segmentation lessens the effect of a ransomware infection.

4. Regular Penetration Tests and Vulnerability Assessments. [9]

   Conduct regular penetration tests and vulnerability assessments to identify weak points in the network and software infrastructure. Thanks to this proactive approach, healthcare organizations can address vulnerabilities before threat actors can take advantage of them. Engage ethical hackers to simulate actual attack scenarios so that security measures can be evaluated for effectiveness.

5. Incident Response Plan. [9]

   Make sure the incident response plan is precise and outlines what to do in the event of a ransomware attack. Establish communication channels, specify a step-by-step containment, mitigation, and recovery process, and clearly define the roles and responsibilities of the key personnel. Regularly test and revise the incident response plan to account for evolving threats and organizational changes.

6. Continue to gain knowledge and collaborate. [9]

   To stay current on the latest ransomware trends and security measures, actively participate in online communities and information-sharing platforms. Cooperate with other healthcare organizations and subject-matter specialists to exchange knowledge, ideas, and the most effective ways to stop and contain ransomware attacks.

B. DDoS Attacks

The group primarily uses DDoS attacks, which can send tens of thousands of connection requests and packets per minute to the target server or website, slowing down or even shutting down vulnerable systems. Kill Net's DDoS attacks typically do not result in significant damage, but they can cause service interruptions that last for several hours or even days. [10]

DDoS attacks are a common tactic, technique, and procedure (TTP) used by hackers and cybercriminals to overwhelm a network to the point of unitability. Healthcare professionals who need network access to provide proper patient care or Internet access to send and receive emails, prescriptions, records, and other information may find this to be a significant problem. Although some DDoS attacks are opportunistic or even unintentional, many of them target victims for a social, political, ideological, or financial cause connected to a situation that enrages the cyber threat actors.

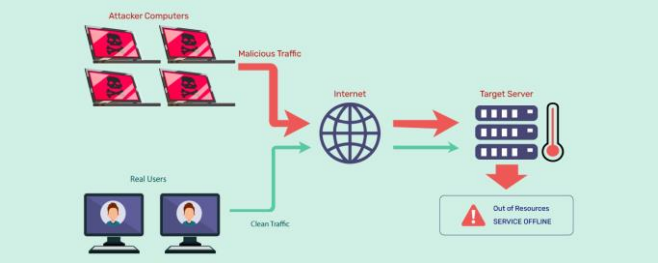

Figure 2: DDoS attack steps

Preventive Measures Against DDoS Attacks.

1. Network monitoring. [10]
An organization can use network monitoring to look for suspicious activity in data packets and notify security experts when such activity is discovered.

2. DDoS response plans. [10]
Having a dedicated DDoS response plan is another crucial step to preserving the effective operation of healthcare systems and infrastructure.

3. Web Application Firewalls. [10]
Web Application Firewalls (WAFs) can be set up in healthcare systems that use web applications and configured with the proper inbound and outbound network policies.

4. Data backups. [10]
To guarantee zero downtime, healthcare systems should back up their data (to thwart ransomware attacks) and use cloud services to restore data.

5. 5. Ethical hackers' knowledge. [10]
Improve the security posture of your infrastructure by working with security experts like Packet Labs to conduct thorough penetration testing.

C. Data breaches

One of the most expensive types of data breaches is a hack into a healthcare system. Even though the average cost of a data breach was $4.45 million across all industries, the average cost of a healthcare data breach was the highest of all, coming in at $10.93 million. Over the last three years, there has been a significant 53.3% increase in the cost of healthcare. [11]

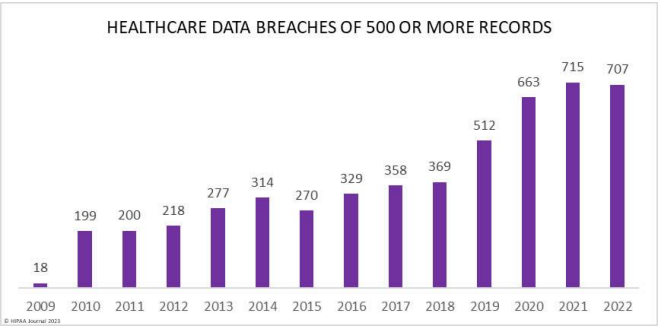

Figure 3: Healthcare Data Breaches Record

In the healthcare sector, breaches happen frequently. Data leaks can occur for several reasons, including malware that steals credentials, insiders who unintentionally or intentionally disclose patient information, and lost laptops or other devices.

Cybercriminals target medical databases for financial gain, with over 15 million health records compromised due to data breaches, making Personal Health Information (PHI) more valuable than credit card numbers or PII..

Preventive Measures Against Data Breaches,

Having proper network security and application security is crucial for preventing compromises in the first place. Encryption is the most effective way to stop unauthorized access to patient data once someone has gained access to healthcare systems.
It is essential that third parties and vendors who have access to healthcare networks or databases use encryption during both the storage and transmission of data, as well as take the necessary security measures with regard to patient information. Training on proper PHI usage and handling is advised to reduce data breaches caused by employee error, such as a lost device or unintentional disclosure.

1. Conduct an annual security risk analysis. [12]

   At the very least, healthcare organizations ought to conduct a yearly HIPAA security risk analysis. This is comparable to the wellness checkup that doctors advise their patients to get. Considering that the HIPAA Security Rule already requires periodic risk analysis, think of this as killing two birds with one stone. This analysis will help you find weaknesses and potential areas for improvement to prevent a healthcare data breach.

2. Monitor devices and records. [12]

   A component of continuing education for staff members is to remind them never to leave electronic devices or paper records unattended. Making sure that every employee has received training on how to properly log on and off computers, particularly for shared devices, is the other element.

3. 3. Control regarding access to patient data. [12]
Users should only have access to patient health information that is relevant to their position. By controlling user permissions and restricting access, a healthcare data breach must be prevented.

4. Restrict use of personal devices. [12]
The IT team is entirely in charge of making sure that your internal network and devices are secure. Create a "bring your own device" policy that is

clear about what gadgets, including laptops, tablets, and smartphones, are permitted for both internal and external use. Can I bring this equipment provided by the company home with me? Will you allow connections to your internal network from privately owned devices? The application and enforcement of this policy can help to stop healthcare data breaches.

5. Update IT infrastructure. [12]
Change is the only constant in the fields of technology and data security. To keep equipment secure, replace or upgrade outdated hardware that can no longer receive security patches.

D. Man in the Middle Attack- MITM

Man-in-the-middle attacks happen when a threat actor gets on a user's or a device's communication with an application or another device. Here, they will either listen in on the conversation to gather information or pretend to be one of the other parties. The threat actor can seize control of the transmitted data and hijack sensitive information from this vantage point. A man-in-the-middle attack in the healthcare industry might lead to theft of prescriptions for opioids, for instance, or even the manipulation of pacemakers and other medical devices.

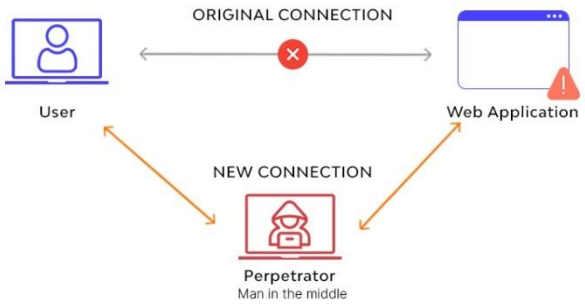

Figure 4: Man in the Middle Attack

Around 17 network-connected devices are used by each hospital bed in the average hospital. According to estimates, the global IoT healthcare market will grow at a compound annual growth rate of 25.9%, from $73.5 billion in 2021 to $190 billion in 2028. IoT devices may lack all available mitigation strategies, such as encryption protocols, making them more susceptible to man-in-the-middle attacks. 15%–20% of medical IoT devices surveyed ran Windows 7 or an earlier version, putting them at least ten years behind current security standards. [13]

Prevent Man-in-the-Middle Attack

Man-in-the-middle attack mitigation is challenging due to the stealthy nature of this kind of cyber-attack. Threat actors can enter and exit a network undetected. Man-in-the-middle prevention focuses on preventing the threat actor from ever connecting to your network. This is achieved by combining security tools, changing people's behavior, and working with a security provider who takes a comprehensive approach to safeguarding devices, networks, and data. [13]

1. Virtual Private Network (VPN). [14]
VPNs encrypt online traffic to prevent hackers from reading or changing messages.

2. Network intrusion detection system (NIDS). [14]

To track traffic to and from all devices on the network, NIDS are positioned at key nodes across the network. It analyses the traffic that is being sent over the whole subnet and compares it to a database of known attacks. An alert can be issued to a cybersecurity expert as soon as an attack is discovered, or unusual behavior is discovered.

3. Firewall. [14]
Unauthorized access can be prevented with a powerful firewall.

4. Two-factor authentication. [14]
Using two-factor authentication, which demands a second form of identification in addition to your password, is an excellent technique to stop email hijacking.

5. 5. Make use of secure DNS servers . [14]
Verify the security of the DNS servers (DNS cache) use.

E. Phishing

Sending malicious emails and waiting for a company employee to open a harmful attachment or click on a malicious link is the most effective technique to hack a company. Because of this, phishing is still one of the most hazardous attack methods.

PHI access or ransomware delivery are the two common goals of phishing attacks against the healthcare sector. PHI is now a highly sought-after item on the underground market because it can be used to fabricate identities, get free medical care, and commit insurance fraud. Hackers may demand high ransom payments once ransomware has been installed on a healthcare organization's network to unlock the encrypted files. [15]

Prevent Phishing Attack.

1. Minimize the Amount of Information Available. [16]
Healthcare organizations should be careful not to provide personnel directories or other contact information on their public websites in order to prevent falling prey to these vacuum cleaner-style phishing tactics. Spear-phishing attempts, which are

more sophisticated spam campaigns, can also be fueled by online publishing directories and organizational charts. In these assaults, phishers prioritize quality over quantity by looking for specific targets and meticulously crafting email campaigns that use the names of important administrators or other crucial information to lend them credibility. [16]
The organization's public profile is minimized, and the possibility of a successful phishing attack is decreased by reducing the quantity of publicly accessible data.

2. Prepare Your Staff for Cyberattacks. [16]
Employees who click links or reply to messages are used as the weak link in the security chain by phishers. [16]

Any campaign to prevent these attacks must include employee education and awareness as a key component. This will enable employees to identify suspicious messages and respond appropriately. To add credibility and urgency, these educational campaigns ought to use actual instances of phishing attacks that the organization has encountered.

3. Remove all suspect content [16]
By stopping phishing attempts from ever reaching their intended targets, technical solutions can help halt them. [16]

The most effective phishing filters should be in place to prevent incoming emails for healthcare organizations that manage their own email systems. This also applies to the usage of phishing blacklists, which quarantine incoming messages from reliable spam sources. By throwing these messages to the digital trash, the chance of a worker accidentally clicking a harmful link is removed.

4. Deploy Multifactor Authentication. [16]
Healthcare organizations that haven't already adopted multifactor authentication to protect user accounts should do so right immediately. Frequently, this is done by requiring users to log in using a registered device. As a result, phishing credentials are essentially useless and there is less chance that attackers will continue to target the organization.

IV. FUTURE RESEARCH

Healthcare blockchain technology and healthcare quantum computing are two emerging technologies that are transforming the healthcare industry. Blockchain technology improves processing efficiency, business opportunity generation, data security, and transparency by enabling the study and sharing of healthcare data while ensuring privacy and security. It involves a systematic process from patient usage data collection to the provision of appropriate opioid medication. Registration contracts (SC) manage patients' medical data through a distributed, global registry, ensuring patient satisfaction and preserving the exchange of health information.

Quantum computing uses quantum states to perform calculations, with applications in drug development, clinical trials in computer simulations, sequencing and analyzing DNA, and designing secure medical data platforms. Quantum computers can perform more complex calculations, faster sequencing, and encryption systems, making it possible to analyze the full genome and integrate genetic data into health records.

Despite its potential, quantum computing is still considered science fiction and requires implementation using quantum physics, which only a select few are familiar with. Despite its potential, quantum computing is still in its research phase and has great promise for the healthcare industry.

V. CONCLUSION

The review paper's focus was on Internet of Medical Things cybersecurity threats and mitigation in the healthcare sector. In this review paper, I sought to identify the threats facing the healthcare industry, which places a strong emphasis on the Internet of Medical Things, as well as the best new technologies that should be applied in the industry going forward. I also sought to determine how to mitigate those threats.

ACKNOWLEDGEMENT

Mr. Kanishka Yapa, the professor in charge of the Applied Information Assurance module, has helped and advice to me since the beginning of the project by holding lecture sessions and practical sessions. Also, a big thank you to everyone that helped me a lot with locating the right materials and coming up with new ideas to make the project a success.

REFERENCES

Bibliography

[1] N. Ali, "Why do threat actors target healthcare providers," thesecuritycompany, 2 February 02 February 2023. [Online]. Available: https://thesecuritycompany.com/the-insider/healthcare-why-cyber-awareness-and-training-is-vital/. [Accessed 5 October 2023].

[2] Unkown, "9 reasons why healthcare is the biggest target for cyberattacks," swivelsecure, [Online]. Available: https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/. [Accessed 5 October 2023].

[3] J. F. Caroline Humer, "Your medical record is worth more to hackers than your credit card," REUTERS, 24 Septhember 2014. [Online]. Available: https://www.reuters.com/article/us-cybersecurity-

hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUKKCN0HJ21I20140924/. [Accessed 5 October 2023].

[4] G. S. Cohen, "8 Essentials for Healthcare IoT Security," FirstPoint, 17 April 2023. [Online]. Available: https://www.firstpoint-mg.com/blog/8-essentials-for-healthcare-iot-security/. [Accessed 5 October 2023].

[5] Unknown, "Cyber Attacks: In the Healthcare Sector," Center for Internet Security, [Online]. Available: https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector. [Accessed 5 October 2023].

[6] Unknown, "7 BIGGEST CYBER SECURITY ISSUES IN HEALTHCARE," Ralabs, 12 January 2023. [Online]. Available: https://ralabs.org/biggest-cyber-security-issues-in-healthcare/. [Accessed 5 October 2023].

[7] Unknown, "Ransomware: In the Healthcare Sector," Center for Internet Security, [Online]. Available: https://www.cisecurity.org/insights/blog/ransomware-in-the-healthcare-sector. [Accessed 5 October 2023].

[8] Unknown, "The Top 15 Healthcare Industry Cyber Attacks of the Past Decade," Arctic Wolf, 22 August August 22, 2023. [Online]. Available: https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/. [Accessed 5 October 2023].

[9] D. Porter, "Safeguarding the Healthcare Industry: Effective Measures to Prevent Ransomware Attacks," CyberGuard Compliance,Cloud Security Alliance, 25 September 2023. [Online]. Available: https://cloudsecurityalliance.org/blog/2023/09/25/safeguarding-the-healthcare-industry-effective-measures-to-prevent-ransomware-attacks/. [Accessed 5 October 2023].

[10] Unknown, "The Ongoing Threat of DDoS Attacks on the Healthcare Sector," Packetlabs, 14 August 2023. [Online]. Available: https://www.packetlabs.net/posts/ddos-attacks-on-the-healthcare-sector/. [Accessed 5 October 2023].

[11] M. Greenlee, "Cost of a data breach 2023: Healthcare industry impacts," SecurityIntelligenece, 16 August August 16, 2023. [Online]. Available: https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/. [Accessed 5 October 2023].

[12] Unknown, "10 Ways to Prevent a Healthcare Data Breach," Applied Medical Systems, [Online]. Available: https://appliedmedicalsystems.com/10-ways-prevent-healthcare-data-breach/. [Accessed 5 October 2023].

[13] S. Poremba, "How to prevent man-in-the-middle attacks in healthcare," verizon.com, [Online]. Available: https://www.verizon.com/business/resources/articles/s/how-to-prevent-man-in-the-middle-attacks-in-healthcare/. [Accessed 5 October 2023].

[14] A. T. Tunggal, "What Is a Man-in-the-Middle Attack? Prevention Tips and Guide," UpGuard, 02 May 2023. [Online]. Available: https://www.upguard.com/blog/man-in-the-middle-attack. [Accessed 5 October 2023].

[15] Unknown, "Protect Healthcare Data from Phishing," THE HIPPA JOURNAL, [Online]. Available: https://www.hipaajournal.com/protect-healthcare-data-from-phishing/. [Accessed 5 October 2023].

[16] M. chapple, "Phishing Attacks in Healthcare: 4 Proven Ways to Prevent a Breach," HealthTech, 1 October 2020. [Online]. Available: https://healthtechmagazine.net/article/2020/10/phishing-attacks-healthcare-4-proven-ways-prevent-breach. [Accessed 5 October 2023].

VIII. AUTHOR PROFILE

Gallage E.D.S
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)