A Review of Penetration Testing Methodologies for Securing Healthcare IoT and IoMT Systems

Chandira Deshan Aluthge

Undergraduate Student, Cyber Security

Sri Lanka Institute of Information Technology

Horana , Sri Lanka

Chandiradeshan12@gmail.com

***Abstract*—**The proliferation and speed of deployments like IoT are helping healthcare, using the IIoT to augment patient care as well as increase operational efficiency. Unfortunately, this new technology has posed cybersecurity risks as smart buildings use IoT or the internet to connect various devices and control their operation thus security is critical. Finally, this paper presents an extensive synthesis of penetration testing methodologies to ensure secure assessment and defense for Healthcare IoT and IoMT systems. The paper uses an extensive review of current literature to define strengths and flaws in existing methods, highlighting the need for customised security strategies accounting for the particular risks specific to healthcare environments. The review also discusses the shortcoming of current research and potential future for emerging more hardened and effective frameworks that may test penetration testing with respect to risk aversion medical data protection, as well maintenance integrity healthcare processes.

Keywords—· Penetration Testing,Healthcare IoT,IoMT (Internet of Medical Things),Cybersecurity,Cyber Threats,Vulnerability Assessment,Risk Management,Future Research,System Security

I. INTRODUCTION

The paper will examine different penetration testing methodologies designed to identify and mitigate vulnerabilities in Healthcare IoT and IoMT systems And it will be further studied about the people, organizations and service providers affected by it To evaluate how well these methodologies address the unique security challenges posed by Healthcare IoT/IoMT systems and to propose areas for future research and improvement. The importance of the topic "A Review of Penetration Testing Methodologies for Securing Healthcare IoT and IoMT Systems" lies with the increasing use and emerging threat of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices in healthcare. Cyber-attacks targeting these devices. This is why this topic is important .

II. RESEARCH OBJECTIVE

Research aim for your study on "A Review of Penetration Testing Methodologies to Secure IoT and IoMT Systems in Healthcare" can be crafted as follows:

Research Objective:

Abstract This paper aims to explore the currently available literature on penetration testing techniques for securing Healthcare IoT (Internet of Things) or IoMT (Internet Medical Things) systems. The aim is to discover by evaluating and synthesis of the current approaches how effective are they in tackling cybersecurity challenges within healthcare. Finally, this review investigates where these approaches can support security applications for IoT and IoMT wearable devices in healthcare institutions but also identifies challenges or potential issues with the literature that warrant further research directions.

III. REVIEW OF THE LITERATURE

.

A. What is penetration testing?

Penetration testing, sometimes called pen testing, is the process by which a cyber-security expert searches for and tries to exploit vulnerabilities in a computer system. Finding any weak points in a system's protections that an attacker could exploit is the goal of this assault scenario[1].

B. What is IoMT?

IoMT security is a cybersecurity protection technique and set of measures that guards against cyberattacks that target medical devices that are connected to the internet. Internet of Medical Things (IoMT) security can be viewed as a cybersecurity plan and defense mechanism that guards against potential cyberattacks against IoMT devices that are linked to

a healthcare network. Medical IoT Security is another name for IoMT security[2].

Examples of IoMT include the following:

- Using remote patient monitoring (RPM) for people with chronic diseases and long-term conditions.
- Tracking patient medication orders.
- Tracking the location of patients admitted to hospitals.
- Collecting data from patients' wearable mobile health devices.
- Connecting ambulances en route to medical facilities to healthcare professionals [3].

C. What is IoT ?

The Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025[4].

you likely use IoT devices every day. The list below outlines a few IoT devices that you may be familiar with:

- Smart home devices
- Wearable technologies
- Personal medical devices
- Autonomous vehicles[4]

D. Why is penetration testing important for Healthcare IoT and IoMT Systems

Healthcare Device Pentesting, sometimes referred to as Healthcare Device Penetration Testing, is an organized approach to evaluating the security of medical equipment by simulating cyberattacks. These assessments look for weaknesses and vulnerabilities in medical imaging equipment, pacemakers, insulin pumps, and other devices that could be used by adversaries.

Through strict adherence to security guidelines and regulations, security testing aims to strengthen the entire cybersecurity posture of medical equipment. Security experts conduct controlled and ethical hacking operations to test the device's resistance to potential cyber threats, such as illegal access, data breaches, and manipulation of medical capabilities.

Maintaining patient safety, protecting private medical information, and averting potentially fatal situations brought on by compromised equipment are the ultimate goals. In order to combat the growing threat of cybercrime in the healthcare industry and promote the advancement of secure and reliable medical technology, medical device security testing services are essential.

In the healthcare sector, where a security compromise could have disastrous effects, penetration testing is crucial and its significance cannot be emphasized. By mimicking the mindset of a potential attacker, penetration testing frameworks for medical devices assist companies in staying one step ahead of cybercriminals[5].

E. IoMT Security Challenges

Weak security is one of the primary problems with IoT in healthcare. IoMT devices are particularly susceptible to compromise because the majority of them were not created with security in mind. Better security is required by IoMT because, in contrast to other industries, a security breech in a healthcare network could directly result in the loss of life[5].

Some of the key security challenges in healthcare related to connected medical devices include:

- Breach of Information
- DDoS Exploits
- Phishing Attacks
- Man-in-the-Middle Attacks

1. Breach of Information

The number of data breaches in the healthcare sector is disproportionately high when compared to other industries. In the healthcare industry, there were 1.76 data breaches on average every day in 2020. Despite the strict requirements set by HIPAA to prevent unauthorized access to health data and other sensitive information, many healthcare institutions do not follow its security protocols. Cybercriminals might use these cybersecurity flaws to get access, endangering patient confidentiality even in the face of measures to prevent such breaches, such as HIPAA penetration testing frameworks[5].

2. DDoS Exploits

A distributed denial-of-service attack is when a server is targeted with a large number of false connection requests, which overwhelm the server and bring it down. This assault

involves the coercive recruitment of several endpoints and Internet of Things devices into a botnet through malware infection. DDoS attacks have the advantage of being able to disrupt networks in the same way without compromising them, which makes them easier to use on a much wider scale. They have chosen the ransom model due to the potential speed and devastation that these strikes might entail. A healthcare facility may potentially be targeted by DDoS attacks, which would end only if a ransom was paid[5].

3. Phishing Attacks

Phishing is the technique of inserting dangerous links into seemingly harmless emails. According to vulnerability assessment for healthcare devices, email phishing is the most prevalent sort of phishing. Phishing emails can appear quite convincing, and they frequently make use of a well-known medical condition to encourage link clicks. Some advanced threat actors write phishing emails as answers in an existing email thread to increase authenticity and reduce suspicion. When a link in an email scam is clicked, users are sent to a bogus web page that looks like the login screen for known internal software. Once these credentials are supplied, fraudsters utilize them almost immediately to obtain access to healthcare systems[5]

4. Attacks by "Man-in-the-Middle"

An attacker launches a "man-in-the-middle" attack when they manage to eavesdrop on communication between two parties. This can happen if the medical equipment is not set up correctly or if the attacker has physical access to the device. Man-in-the-middle (MITM) attacks have the potential to cause service disruptions and data breaches. Among the most dangerous cyberthreats associated with public and private Wi-Fi networks are MITM attacks. In 2016, a Man-in-the-Middle attack on a US hospital led to the loss of patient information[5].

F. People affected by healthcare cyberattacks so far

Millions of people are affected by healthcare cyber-attacks. Looking at the year 2023, it will be more than one hundred million.

- Attacks aren't necessarily more frequent than they have been in recent years. However, according to John Riggi, national advisor for cybersecurity for the American Hospital Association, the attacks have caused greater harm and impacted a larger number of people.

“I think this year we are going to break all records in terms of the number of individuals impacted,” Riggi tells Chief Healthcare Executive[6].

According to federal data on health data breaches, Riggi estimates that cyberattacks targeting healthcare institutions have impacted about 106 million people. To put things in perspective, the number of people impacted this year has more than doubled from the approximately 44 million affected by health information breaches in 2022.Stated differently, this year roughly one in three Americans had experienced some sort of health data leak[6].

- On May 12, 2017, thieves employing the WannaCry ransomware attacked the National Health Service of the United Kingdom. In order to prevent a remote takeover, these ransomware attacks took advantage of a flaw in PCs running an outdated version of Windows that wasn't patched. The spyware requested $300 in Bitcoin payment and encrypted the host machines' contents. The victims were informed by the crooks that all encrypted files will be erased in seven days and that the $300 payment would double after three days. The incident caused disruptions to healthcare services throughout the United Kingdom. Roughly 19,000 appointments, including radiological sessions, outpatient appointments, and elective admissions, were canceled by the NHS. Emergency ambulances had to be rerouted to hospitals that were not affected.The WannaCry attack is the most costly and extensive in NHS history to date. The NHS spent roughly £72 million on technology to recover data and strengthen the security of the current infrastructure, but lost about £20 million as a result of canceled appointments[7].

- The first instance where a patient's mortality was directly connected to a cyberattack is discussed in a 2020 BBC article.Prior to a ransomware attack disabling the systems supporting their medical gadgets, a patient at Düsseldorf University Hospital was due to receive crucial treatment.The hospital was obliged to move their patient to a different hospital, which was located thirty kilometers (19 miles) away, due to their suddenly restricted capacity to offer proper care. Tragically, the patient passed away during the transfer.German prosecutors launched a homicide investigation as a result of the incident to find out if the threat actors may be prosecuted for negligent homicide. If proven true, this might establish a standard for such occurrences in the future[7].

- In 2020, the global shutdown caused by the COVID-19 epidemic allowed cybercriminals to successfully launch many ransomware attacks against healthcare organizations throughout the globe. During that time, more than 500 healthcare organizations reported experiencing a data breach or cyberattack, with UHS being among the main victims.Critical infrastructure supporting more than 400 locations both inside and outside the US was impacted by the attack. In order to

control the exposure and eliminate the ransomware from the impacted machines, this necessitated a shutdown. Ambulances were diverted and patients in need of surgery were moved to other neighboring facilities by the affected hospitals. Both the length of the patient's recuperation and the chance of death rose as a result. UHS reported a $67 million loss as a result of the attack following the disaster. The majority of the losses are incurred by the company as a result of its temporary incapacity to operate at full capacity and the extra expense of employing specialists to repair its systems and put cybersecurity measures in place[7].

- A data breach occurred at Premera Blue Cross, a health insurer, in the spring of 2014, however it wasn't discovered until March 2015. About 10.4 million clients were impacted, according to the firm, when the breach was found and damages were calculated. The information that was obtained included names, physical addresses, dates of birth, email addresses, bank account information, Social Security numbers, and clinical data from health plans.Cybercriminals used a phishing email to deceive an employee into installing malware on a work computer, which allowed for the cybersecurity disaster.At the time, the Premera Blue Cross breach was the greatest, and it resulted in the second-highest HIPAA settlement. The company was mandated to pay $6.85 million to resolve a class-action lawsuit in 2020[7].

G.Who are these stakeholders?

Healthcare systems are groups of institutions, organizations, and resources that collaborate to provide populations with healthcare. They must oversee people, finances, insurance, and human and material resources in addition to directly serving clients. Additionally, they teach communities how to prevent illness and lead healthy lives. Healthcare systems serve a variety of purposes, are highly complicated, and have numerous duties.This means that establishing and preserving connections with a wide range of internal and external stakeholders is necessary for carrying out initiatives in this industry, let alone managing a hospital or other similar facility.These stakeholders are who? How are we going to recognize them? What are the difficulties in maintaining connections with them, and why is it necessary to provide them careful attention?All the people and organizations impacted by a healthcare facility or project are considered stakeholders in the field of healthcare. Every stakeholder has a different set of interests, and some are able to significantly affect how a project turns out[8].

The healthcare sector is generally considered to have four main stakeholder groups:

- Patients
- Service providers
- Decision-makers
- Payers

These four groups are connected and influence each other[8].

1. Patients

Patients are the sector's most important stakeholder, both in terms of numbers and value. Patients are the primary reason healthcare systems exist. Services and projects must therefore take account of their needs, interests, opinions and so on. As taxpayers and voters, patience also have influence[8].

2. Service suppliers

These are the professionals (individuals or institutions) who provide health care to patients. They also train medical and paramedical personnel[8].

3. Decision-makers

They are responsible for overseeing all aspects of healthcare, including issues such as eligibility, financing and quality. Depending on the type of public healthcare system, these authorities may vary slightly. For example, in the province of Quebec, Canada, the main decision-makers are the Minister of Health and Social Services, the National Director of Public Health, and the Regional Directors of Public Health[8].

4. Payers

This group includes insurance companies, public health organizations and individuals who assume financial responsibility for healthcare services. Payers influence health policies, service pricing, and reimbursement rates[8].

- *Internal and external stakeholders*

Stakeholders can be divided based on whether or not they belong to the organization in question. If they are part of the organization, they are considered internal stakeholders; if they are not, they are external stakeholders.

I. Internal stakeholders

Beyond decision-makers, payers, and medical staff, internal stakeholders may also include facility board members, volunteers, and donors.

II. External stakeholders

In addition to patients, external stakeholders include private insurance companies, as well as pharmaceutical and medical equipment companies[8].

IV. Future research

- **AI and Machine Learning Integration:** To improve predictive analytics, customize patient care, and automate decision-making processes, the Internet of Medical Things (IoMT) will significantly rely on artificial intelligence (AI) and machine learning (ML). AI will make it possible for cutting-edge medical devices to have predictive maintenance, real-time health monitoring, and more accurate diagnosis[9].

- **Improved wearables and implantables:** The upcoming generation of wearables and implantables will provide even more functionality, extended battery life, and increased precision. These gadgets will track intricate biomarkers in addition to basic vital signs and give patients and healthcare professionals real-time feedback[9].

- **Enhanced patient involvement:** Gamification, user-friendly interfaces, and real-time feedback systems are some of the ways that future IoMT solutions can improve patient participation. Patients will be given the confidence to actively manage their health and follow treatment regimens as a result[9].

- **Automated healthcare facilities:** IoMT will make healthcare facilities more effective and automated. Reduction of operational expenses and enhancement of service delivery can be achieved through automated inventory management, predictive repair of medical equipment, and optimized workflows[9].

- **Big data analytics:** Using sophisticated big data analytics, the enormous volumes of data produced by IoMT devices will be utilized. Further advancements in healthcare will be fueled by the insightful information this will provide about illness patterns, treatment outcomes, and population health trends[9].

- Ethical considerations: A growing number of discussions will center on patient permission, data privacy, and fair access to IoMT technologies as they pertain to the moral ramifications of broad adoption of IoMT. It will be essential to guarantee that IoMT benefits all populations, particularly underprivileged ones[9].

- **Cross-industry collaboration:** As IoMT progresses, there will be more exchanges between technology firms, insurance companies, healthcare providers, and regulatory agencies. These collaborations will promote innovation, enhance interoperability, and guarantee the security, efficacy, and widespread adoption of IoMT solutions[9].

V. Conclusion

With the integration of IoT and IoMT systems, the healthcare industry is witnessing a revolutionary change that presents previously unheard-of chances to improve patient care, streamline operations, and improve overall health outcomes. But these developments also bring with them serious cybersecurity risks that might have disastrous effects if left unchecked. The importance of penetration testing in safeguarding Healthcare IoT and IoMT systems has been brought to light by this review.

Methodologies for penetration testing offer a methodical way to find and fix vulnerabilities that cybercriminals might exploit. Personalized penetration testing techniques are necessary in the healthcare industry due to the vital nature of medical devices and the sensitive nature of patient data. The current approaches provide a strong basis, but they also highlight shortcomings in addressing the particular requirements of IoT and IoMT systems in the healthcare industry, such as the absence of real-time monitoring features and the scant attention paid to regulatory compliance.

Subsequent investigations ought to concentrate on creating more resilient and all-encompassing penetration testing frameworks tailored especially for the healthcare industry. This involves improving real-time monitoring, incorporating compliance checks with laws like HIPAA, and integrating AI and machine learning for predictive threat identification. Furthermore, as IoT and IoMT technologies develop further, it will become increasingly important to do continuing study and modify security procedures in order to remain ahead of new risks.

In conclusion, even though healthcare IoT and IoMT system security has advanced significantly, penetration testing techniques still require constant innovation and development. By doing this, it will be possible for healthcare providers to fully take advantage of IoT and IoMT technologies while maintaining patient safety, data privacy, and the operational integrity of the industry.

ACKNOWLEDGMENT

I would like to express my gratitude to all those who have supported and guided me throughout this paper's journey. Special thanks go to Mr. Kanishka Yapa, the lecturer in charge of the Applied Information Assurance module at Sri Lanka Institute of Information Technology (SLIIT), for offering me the opportunity to work on this review paper and for your valuable guidance. I also extend my thanks to the authors and publishers whose research and references have been instrumental in shaping this paper. Your hard work and contributions have been indispensable in making this paper a reality

REFERENCES

[1] Cloudflare, “What Is Penetration Testing? What Is Pen Testing? | Cloudflare,” Cloudflare, 2022. Available: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

[1]“What is IoMT Security?,” Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-iomt-security

[3]“What is IoMT (Internet of Medical Things) or healthcare IoT? - Definition from WhatIs.com,” IoT Agenda. https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things

[4]J. Schulze, “What is the Internet of Things (IoT)? With Examples,” Coursera, Jun. 16, 2023. https://www.coursera.org/articles/internet-of-things

[5]C. Sahoo, “Healthcare Device Pentesting | Medical Device Security Testing,” Qualysec | Penetration Testing Services and Solutions, Dec. 21, 2023. https://qualysec.com/healthcare-device-pentesting/#:~:text=4.- (accessed Sep. 11, 2024).

[6]R. Southwick, “Healthcare cyberattacks have affected more than 100 million people in 2023,” OncLive, Dec. 18, 2023. https://www.chiefhealthcareexecutive.com/view/health-data-cyberattacks-have-affected-more-than-100-million-people-in-2023

[7]D. Strickland, “The Impact of Cyberattacks on Healthcare,” CurrentWare, Apr. 06, 2022. https://www.currentware.com/blog/the-impact-of-cyberattacks-on-healthcare/

[8]C. Crowe, “Identifying Stakeholders in the Healthcare Sector,” Boréalis, Nov. 16, 2023. https://www.boreal-is.com/blog/stakeholders-in-healthcare/

[9]A. Buendia, “Internet of Medical Things (IoMT): the future of MedTech | Scilife,” Scilife.io, Jun. 12, 2024. https://www.scilife.io/blog/internet-of-medical-things-medtech#:~:text=Automated%20healthcare%20facilities%3A%20IoMT%20will (accessed Sep. 11, 2024).

AUTHOR PROFIL

- Chandira Deshan Aluthge
- Born in Horana, Sri Lanka,
- 04/10/2001
- Pursuing a Bachelor of Science (B.Sc.) in Cyber Security at Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka (Expected Graduation: 2026)