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

IT22562074 | JAYARATHNA K.P.G.C.M | Mobile – 070-1463982| Y3.S1.WD.CS.01.02

***Abstract*—The rapid adoption of IoT and IoMT devices within the healthcare industry has changed how patient care, processes, and data are managed. Nevertheless, the use of these interconnectable devices poses their own set of problems, especially where cybersecurity is concerned, since a weakness in any of these systems can result in information theft, abuse, or even interruptions. The objective of this review is to detail security penetration testing awareness concentrations within healthcare IoT and IoMT domains. The paper tackles the existing literature on penetration profiling techniques and categorizes them around issues such as black-box testing, white-box testing and grey-box testing effective in bridging the penetrative gaps in the health system. The study also highlights issues affecting the adoption of conventional penetration testing in healthcare IoT systems including power consumption of medical devices and compliance issues. The results show that penetration testing is one of the strategies that can be used to improve cybersecurity in health systems, although there is a widening gap in the availability of tools and approaches that will be productive in the highly dynamic and resource limited environment of IoTs and IoMTs.Finally, the paper suggests directions for future research, focusing on the development of automated testing tools, AI integration, and improved vulnerability detection mechanisms in healthcare networks. Finally, the paper suggests directions for future research, focusing on the development of automated testing tools, AI integration, and improved vulnerability detection mechanisms in healthcare networks.**

Keywords—Penetration Testing, Healthcare IoT Security, IoMT (Internet of Medical Things), Cybersecurity, Vulnerability Assessment, Network Penetration Testing, Firmware Security, Data Privacy, Device Takeover, Regulatory Compliance (HIPAA/GDPR)

I. INTRODUCTION

Thanks to the emerging discoveries as well as the integration of Internet of Things (IoT) and Internet of Medical Things (IoMT), the health sector has undergone some revolutions. The traditional methods of patient monitoring, data gathering, and care providing have been enhanced by a variety of IoT and IoMT devices, from fitness monitors to insulin pumps and implantable defibrillators. The presence of such technologies allows for remote assessment, continued surveillance, and unrestricted exchange of information and so increases efficiency in the provision of healthcare services. Except that with these developments comes the possibility of adopting connected devices, and it also comes with great risks, most importantly cybersecurity. There is something quite apparent with healthcare IoT and IoMT devices that makes them very much prone to attack. Most existing IoT devices operate on reduced computing ability, older unpatched software, and less robust security standards. Such weaknesses leave very critical systems vulnerable to various cyber legal issues such as information leakage, violation of health care confidentiality, and manipulation of professional medical equipment. The trend of increasing use of such devices by health care facilities and provision of services to the patients using these devices makes it imperative for the IoT and IoMT systems to be secured from patients and other vulnerable information breaches.

Penetration testing as a measure of a general defense mechanism in cyberspace has been instrumental in managing risk in the areas of Healthcare IoT and IoMT systems and hence should be employed. Through ethical hacking, penetration exploitation testing reveals gaps in the security performance of the entire network, end devices, their operating systems and apps, and their communication software and protocols baptized as attack surface cleansing offering more solutions to organizations that strive to comprehend their vulnerabilities' threats. Due to critical health care services, protection of these devices is not just a technological issue, it is also a legal obligation under HIPAA and GDPR. [1] [2]

This literature aims to investigate different IoT and IoMT device Penetration Testing approaches in healthcare settings. The purpose of such investigation is to evaluate the appropriateness of such methodologies from the perspective of healthcare system protection as well as to seek out the gaps that the healthcare system presents as unique features to be addressed in future studies. However, there is a need to comprehend and manage the security risk posed by the Internet of things (IoT) and Internet of Medical Things (IoMT) systems to health care services as more IoT-enabled devices are adopted in health care organizations. [3]

II. RESEARCH STATEMENT/OBJECTIVES

This report explores the penetration testing strategies that have been employed against the penetration testing strategies protection of the healthcare internet of things (IoT) and internet of medical things (IoMT) systems. These systems have become susceptible and vulnerable to cyber threats jeopardizing patient security and the confidentiality of information with the growth of interconnected devices in healthcare environments. Penetration testing is a method used to evaluate the security of a system, prior to the use of the identified weakness by an attacker. This review brings together current research on other research studies which have been conducted regarding a variety of testing techniques and their effectiveness in healthcare settings. With the use of various methods employed in different studies, the present article assesses these techniques considering addressing the

security specificities encountered in healthcare IoT/IOMT and the respective systems respectively.

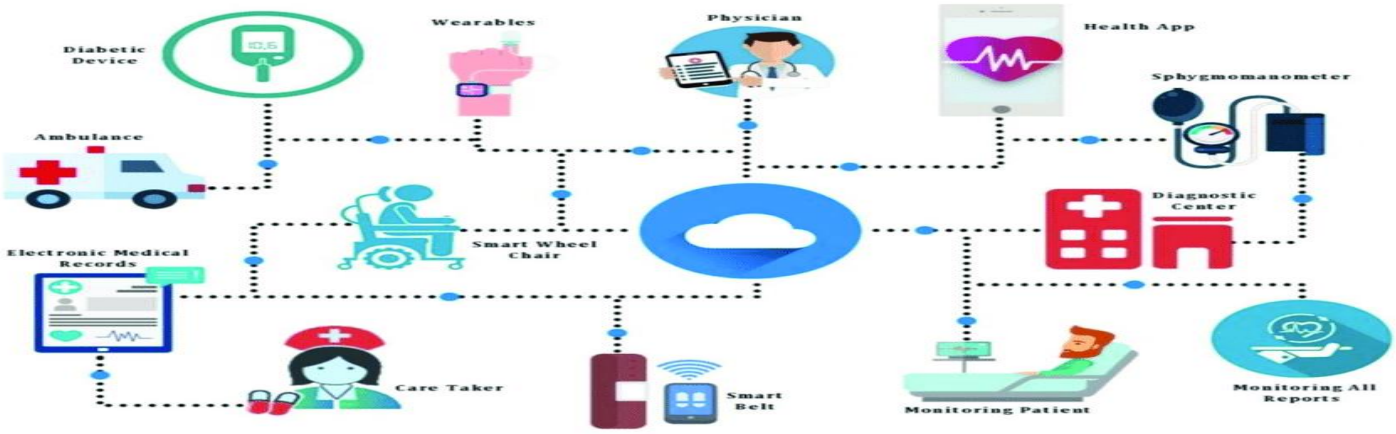

FIGURE 1: Infrastructure of Internet of Medical Things (IoMT).

A. Research Questions

RQ1: What is the prevalent penetration testing methods applied to healthcare IoT and IoMT devices, and into which classes are they grouped?

RQ2: How likely are these methods to succeed in detecting any forms of vulnerabilities in system aspects such as data leakage and external intrusion access vulnerabilities in healthcare systems?

RQ3: What is the penetration testing efficacy in performing its functions when incorporated in the healthcare IoT IoMT setup?

RQ4: What are the research gaps identified, and what are future testing tools within the healthcare IoT and IoMT systems that will be developed to meet their requirements?

B. Research Objectives

Based on the above research questions, the following objectives have been formed

Objective 1: To pinpoint and classify the primary penetration testing methods of black, white, and grey box currently used for evaluation of the health related IoT and IoMT devices' security aspects

Objective 2: To assess the extent to which these penetration testing methods can be useful in detecting vulnerabilities related to healthcare systems such as data leakage, outsider unauthorized access, and computer virus infiltrations.

Objective 3: To understand the uniqueness of penetrating healthcare IoT and IoMT systems focusing more on their resource limits, diversity of devices and regulations.

Objective 4: To fill in the missing areas of the current literature and suggest what else may follow and include the construction of effective, advanced, targeted testing tools and frameworks which fit well into the IoT IoMT system in healthcare which is fast, and resource limited.

III. REVIEW OF THE LITERATURE

Due to the growing use of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices in the field, medical services and the quality of care that the patients receive have greatly improved. At the same time, this evolution is accompanied by high-level cybersecurity challenges and risks that are concerns chiefly because of the expansive exposure that the IoT devices have.
This portion of the paper provides an overview of the current state of penetration testing penetration testing existing literature on healthcare IoT and IoMT systems, with a division by testing approaches, tools and challenges.

A. penetration testing Methodologies

Penetration testing, often known as ethical hacking practice is the practice of assessing the security posture of computer systems through simulated cyber-attacks on the computer systems before they are carried out by the bad guys. There are certain methodologies that tend to be associated with even this particular domain, and they are typically referred to as black – box, white – box and grey – box testing, which is mainly concerned with the testing of a particular system. [1] [2]

- **Black-Box Testing**:
  The black-box penetration tester does not have any prior information regarding the functioning of the internal workings of a system. Research, for example Smith et al. (2021), demonstrates that there is considerable utility in the carrying out of some aspects of the black box testing in the healthcare sector where access to some internal system data may be restricted due to privacy issues. Applying black-box testing is appropriate when evaluating public service applications of healthcare systems, including patient portals and telemedicine services that are prone to imitation by outsiders. [3]

Challenges:
Narrowed Scope: Bullseye testing is only able to underscore defects that can be spotted externally, and thus it is more useful within a wider context than black box testing.

Costly: There is need for extra resources and time, as the whole process would require a lot of investigative work which would be laborious.

- **White-Box Testing**:
  On the contrary to the previous technique to test the system, white box testing allows the tester to have full control and knowledge of the system's internal structure which includes source code, network architecture and databases. Johnson and Lee 2020 opined that it was plausible to use empirical evidence that supports the notion the weaknesses of the White Box Testing approach is best suited for complicated healthcare IoT systems Nowadays, detailed knowledge of device firmware and communication protocols has become a necessity in order to identify such duplicated errors in this category of medical systems. [3]

Challenges:
Finesse: It demands in-depth understanding and skills which may require help from the resources of the markets.

Risk of Overlooking Some Problems: Even if one has all potential resources in the execution of a project, some problems will take place neglect, and this is where its boundaries fall short to go further.

- **Grey-Box Testing**:
  Grey-box testing is a combination of both white box testing and black box testing since some degree of system knowledge is possessed by the tester. [8] [3] This approach is particularly applicable to IoMT devices, where only partial details such as device stats and known security policies may be present. McCarthy et al. (2022) observe that the middle-path of grey-box testing is beneficial as it minimizes the disadvantages of the other taken two, black-box and white-box, by letting one know some context sufficient to seek for security. [8]

Challenges:
Inconsistency: The existing information procedures being a subset of the correct information procedures may lead to failure in properly defending the system.

Complete Control: Obtaining adequate information for the testing purpose may be compromising.

Due to the more practical inclusion of the IoT and IoMT devices into healthcare systems, security of such systems by internal or external penetration testing is important. Because these devices are integrated with other healthcare devices and the internet, penetration testing helps bring vulnerabilities that are likely able to compromise a patient's information.

- **External and Internal Network Testing**:
  Network penetration testing is further divided into external penetration testing and internal penetration testing. In external penetration testing, the security assessment of systems available to the public over the internet is performed, discovering weaknesses in healthcare-internet solutions, such as patient and remote user authentication systems. Internal penetration testing seeks to explore the risks that these networks might be exposed to once they have been established, concentrating on how viruses or an infiltrator that already possesses some level of access can use the network to cause further harm

- **External and Internal Device Testing**:
  Since IoT and IoMT devices are also standalone devices, they stand the risk of being challenged by physical attack. Penetration testing of this nature assesses the degree of security against external attack that is embedded into such devices, so that the ability to gain access to the device does not permit control of the device or access to information on the device. [8] [1]

- **Software Testing**:
  Penetration testing equally applies to the software and firmware used in IoT and IoMT devices. Software testing helps to identify if there are any vulnerabilities in the code of the device, and whether the firmware and other operational software are useful in shielding the device from any eventual attacks. Given the fact that many of the healthcare IoT/IoMT devices support the use of special firmware, programming a device or using unsupported applications may pose a grave threat to security.

Penetration testing of the devices employed in healthcare IoT and IoMT environments proves useful to prevent the exposure of sensitive data over such interlinked devices. Methodologies such as black box, white box and grey box testing techniques are employed to consider the various levels of testing for accessing the weakness as well as testing that covers the entire network and devices levels for effective security results.

OWASP IoT Top 10 has developed a list of the top 10 security issues for IoT systems. These include weak or hardcoded passwords, insecure interfaces and lack of encryption. This framework helps penetration testers focus on the most critical vulnerabilities in IoT systems. [9]

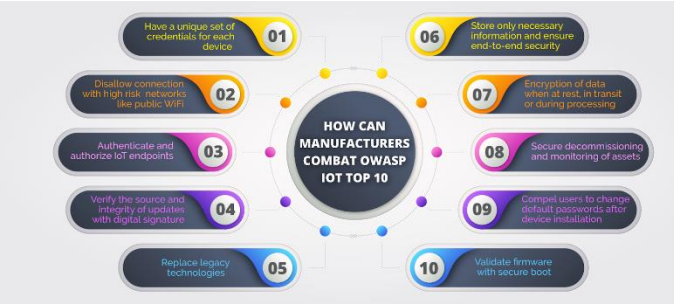

FIGURE 2: OWASP IoT Top 10

B. Challenges in Securing Healthcare IoT/IoMT Systems

- **Device Constraints**
  There is little processing power, memory and battery back up in IoT and IoMT devices and therefore resorting to normal cyber security methods is futile. Research by Davis et al. (2019) a smart pumping module with intelligent insulin management system can be dedicated to process illnesses without relevant security computing thus increasing the chances of attacks. Penetration testing in these situations requires noninvasive operational tools that do not interfere with how a device operates.

- **Network Complexity**
  The healthcare networks are usually so complicated that there are several IoT and IoMT devices that link with each other as well as other external systems like computers and clouds. This also means that there are numerous vulnerabilities that can be exploited for a cyber-attack. Network segmentation and isolation remain critical reducing the attack surface, however, carrying out penetration testing in such crumbled environments could be quite a challenge, according to Green and Patel (2021). Inter-systems intrusions may sometimes crossline the norms of patient interactions and even breach the patients' data protection laws.

- **Regulatory Constraints**
  Healthcare provisions are complex since there are laws governing them, which govern the liberties and internal management of the patients. There are laws such as HIPAA (Health Insurance Portability and Accountability Act) in the USA and GDPR (General Data Protection Regulation) in Europe that concern patient privacy and data security in healthcare systems. [5] Some research like Zhang and Hernandez (2020) unearths that there are limitations which such regulations have to participate in penetration testing which can be undertaken without breaching any compliance measures. Such a scenario will lead to surfaces which majorly underscore non-invasive technologies for security assessments.

C. Penetration Testing Tools for IoT and IoMT Systems

Understandably, many mechanisms and methods have been established aimed at penetration testing IoT and IoMT systems, with each approach being better or worse in various aspects. However, several studies have tested these tools in healthcare environments with emphasis on their usability and efficiency.

- **Nmap**: Nmap is a tool that is quite popular in network mapping and scanner utilities. As noted by Taylor and Brown (2021), Nmap is good for initial reconnaissance purposes in healthcare IoT environments as it helps map out open ports and network services.

- **Metasploit**: Metasploit has become a common platform used to write and run exploitation codes against a pre-defined target. Metasploit main disadvantage is its low level of modification and inclusion of new devices during the test – according to Garcia et al (2020) – unlike Metasploit that has wide variety of usage analyzing Plague life systems or modularity that can be used on the connected health IoT environments which includes devices like smart devices and patient monitoring systems such as smart, deep-seated pacers. Metasploit is helpful particularly in post-exploitation scenarios. [3] It is useful when an attacker has exploited a device or network vulnerability, and has control of the device or network, and it is necessary to simulate possible actions of the user. [13]

- **Burp Suite:** Burp Suite is a very popular web application testing tool, but it can also be used in patient portal healthcare systems, and even in systems that include cloud-based electronic health records application. [7] According to Martinez and Kumar (2022) studies, Burp Suite is capable of finding the way to those common but critical web vulnerabilities within healthcare applications including the SQL injection and cross-site scripting.

Other Emerging Penetration Testing Tools for IoT and IoMT Systems

- **Wireshark**: Enumerating the communication protocols supported by IoMT and monitoring devices/interrogating the monitoring web analyzer network using Wireshark. Wireshark is a widely adopted protocol analysis tool with an application of monitoring and inspecting processes of IoT/IoMT devices and other networked systems. In the healthcare industry, Wireshark is used to capture and analyze ongoing communications between medical equipment and hospital systems to look for security weaknesses. It can be used when handling any forms of spying, subtle traffic modifications or unencoded data sent, a useful tool for thermal IoT system management. [11]

- **Maltego:** Maltego is a multipurpose software which is very efficient in the task of data mining, data collection, & also depicts relationships between people, systems, and domains graphically.

Metasploit is a tool conventionally utilized to attack the weaknesses of systems while it is impossible – however, in any penetration test, this tool facilitates in the preparation process, where all the information about the object is being collected. Maltego is useful in the case of healthcare IoT & IoMT systems like most researchers, Sorensen explains that Maltego helps find devices, services and network infrastructures that can be vulnerabilities

- **Hydra**: Conventional brute-force attack tools used for cracking passwords, for example Hydra. It is very good in checking systems that have only poor geolocation wi-fi security which is a common problem in IFT or igena codes and Igena-like devices. Since many IoT/IoMT devices box out strong or complex folder restricts passwords making Hydra useful in checking such devices to grow brute force attacks/codes.

The secure storage and processing of sensitive information and critical operations in Healthcare IoT and IoMT solutions require an extensive level of security in place. Tools such as Nmap, Burp Suite, ZAP, Wireshark, OSINT, Hydra, and Metasploit are useful in identifying and testing web, authentication security, and threat intelligence gathering. Likewise, network traffic balancers help maintain active protection of the patients at all time password policies, gather operational data, and reinforce additional safety measures. When used properly, these tools promote the safety of the patients, the privacy of the data, the proper functionality of the operations, and adherence to the given regulations, increasing the security of these systems in the process.

TABLE 1: Summary of Tool Applications in Healthcare IoT/IoMT Systems

Tool	Primary Function	Application in Healthcare IoT/IoMT	Strengths	Limitations
Nmap	Network scanning	When the IoM/IoMT devices in healthcare networks are mapped and discovered, they monitor the devices & services and endpoints for open ports [11].	Network reconnaissance executes Low cost.	Applicable to only vulnerabilities and exploits of specific or certain computers.
Metasploit	Exploitation framework	Walking through the surrealistic post-exploitation analysis of smart medical devices like smart definable and patient monitoring systems.	Big exploit data to assess vulnerabilities.	Support for uniquely branded ICT/IoMT is minimal.
Burp Suite	Web app security	Web application penetration testing on patient portals and cloud systems for SQL injection, XSS and other vulnerabilities. [2]	Strong towards testing vulnerabilities based on the web.	Focus on interfaces on the web; not so useful for vulnerabilities affecting any of the devices inside.
Maltego	Data mapping & OSINT	Mapping the IoT/IoMT networks and devices within the application ecosystem in healthcare; mapping these connections in terms of exposed connections between infected endpoints and the external environment.	Great at sociograms and collected data through OSINT.	Yes, for exploitation or deep TTP scanning.
Hydra	Brute-force attacks	Confirmation of weak/default passwords on healthcare IoT/IoMT devices and systems which make use of login authentication	Effective in cracking passwords over several protocols.	Only quite literal password cracking and nothing not deterioration testing.
Wireshark	Network protocol analysis	Capture & review in real time any IoT/IoMT – healthcare network communication to look for abnormal or hostile actions [14]	Passive traffic monitoring; offers insight into communication patterns and traffic.	Confined to the network domain rather than more in depth penetration testing and exploitation of networks.

D. Effectiveness of Penetration Testing in Healthcare

In the case of telemedicine hardware, several useful articles argue for penetration tests being conducted for such healthcare devices and IoT systems, while at the same time, they state the areas in which this technique cannot be useful.

Proactive Defense through Penetration Testing

Penetration testing is a method that can help find vulnerabilities in healthcare network systems, IoT systems, and IoMT devices effectively. By creating several attack scenarios such as network intrusions, infection by malicious software, data intrusion, etc., healthcare organizations can address any shortcomings in their defense systems before a real incident happens. [3]

- **Preventing Data Breaches**:
  A study conducted by Williams and Singh in 2021 demonstrated the effectiveness of regularly scheduled penetration tests in averting a potentially devastating data security breach at a commercial hospital group. Penetration testing noted that there were issues with the network layout and the IoT equipment employed for patient care and telehealth was insecure. By demonstrating these weaknesses, the hospital was able to fix flaws, introduce more effective segregation of networks and even improve the capabilities of IoT devices security reducing the attack surface area.

- **Identifying Misconfigurations and Weaknesses**:
  In healthcare settings notably, it is common that IoT and IoMT devices possess complex structures and support diverse communication channels configurations. In the context of se [1] [10]curity evaluation, it is penetration testing that is most proficient in revealing obvious security flaws such as configuration errors that may render the system susceptible to external uncleared risks. For instance, smart infusion pumps or smart ventilators usually have security breaches such as improper firewall rules, unregulated open ports, or factory-set passwords. It is through the putatively weak security configuration flaw that penetration testers facilitate the securing of the internet connected devices before any attacker exploits these weaknesses.

- **Regulatory Compliance and Risk Reduction**:
  Compliance testing helps healthcare institutions in mitigations of risks, reporting and addressing issues such as patient privacy protection under regulations such HIPAA and GDPR. [9]Testing helps especially healthcare organizations to fill those gaps fulfilling requirements of compliance and security to avert the risks of possible penalties for noncompliance. Furthermore, given that these standards assist in eliminating legal and financial exposure that may arise from data leaks where legal action and bad publicity may lead to significant expenses, effort will lessen. [10]

Limitations of Penetration Testing in Healthcare IoT Systems

Although penetration testing has merits, there are limitations that healthcare institutions need to be aware of while adopting this methodology to protect the IoT/IOMT ecosystem. Some of these drawbacks are usually due to the emerging and improving nature of these cyber threats, the nature of healthcare systems, and the limitations posed by IoT and IoMT devices.

- **Not a Comprehensive Solution**:
  Emptional definition and types of penetration testing techniques. It is quite unreasonable to suggest that this kind of test can realistically enable the resolution of threats that are generated further in the system in the future. This also brings in continuous evolution in threat responses, in particular, cyber threat penetration testing, whereby as Carter et al. (2022) present it cannot be understated that penetration testing stands without processes like continuous monitoring, patching, and quick responsiveness alongside insertion testing. But infiltration testing cannot contain such new threats as zero-day vulnerability. This means that penetration testing must be undertaken as an evolving process embedded in cohesive threat management that goes along with continuous network surveillance. [10] [7]

- **Resource Constraints of IoT Devices**:
  Additionally, in many scenarios, especially for IoT and IoMT devices, the amount of testing that can be undertaken is limited by the computational resources such as available processing power, memory size, or battery life of the devices under attack. More specific devices intended for chronically ill patients, such as pacemakers or insulin pumps, will most likely fail to undergo intensive testing for functional concerns because of safety, necessitating the use of agile and minimally intrusive techniques so as not to interfere with the working of the device.

- **Complexity of Healthcare Networks**:
  Healthcare networks tend to be large and complicated containing thousands of devices interconnected by many different protocols. [10] Testing of a single device may ignore the vulnerabilities of the entire network because such dependencies can cause other risks than those anticipated. Also, testing is made difficult by the existence of legacy systems as there are risks that would be presented that cannot be mitigated because of how important these old systems are in actual clinical care.

- **IoT-Specific Threats**:
  Normal penetration testing tools include a spectrum of weaknesses and therefore such weaknesses are

also present in testing Snort. Vulnerabilities associated with the Internet of Things covering elements such as communication port inconsistencies, firmware vulnerabilities, and various threats on the hardware are hardly catered for with the available specialty telescopes. Such soporific interdisciplinary hurdles as the traditional ones will not assist in revealing them as well the. [8]

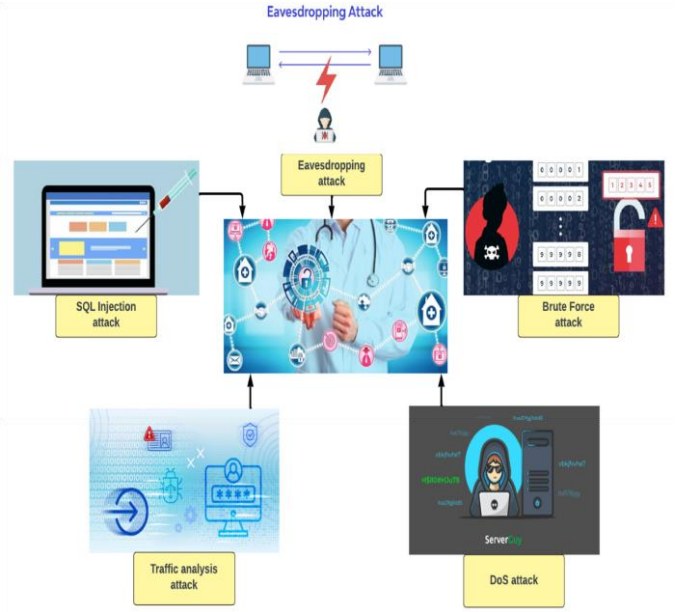

FIGURE 3: Common attacks of IoMT.

IV. Future Research

On the contrary, penetration testing has been able to provide great insights into IoT and IoMT systems. some gaps still exist that will be addressed in this paper. As new devices continue to be introduced into the health care system, so will the difficulty of securing IoT and IoMT devices. All the above features raise a need to focus future studies on development of more advanced instruments and methods that will be able to solve the problems brought by those kinds of systems.

A. Development of Automated and AI-Driven Penetration Testing Tools

The continuous advancement of the healthcare industry, especially the rise of IoT and IoMT devices makes the application of conventional penetration testing techniques largely futile as new threat surfaces emerge. Due to the emergence of limitations in the communication protocols, firmware or even the network architecture, more practical attacks tend to become more of a time-consuming manual process.

- **Automated Testing**:
  One of the most active fields in the future research has to do with the automated penetration testing tools design where networks of healthcare institutions are actively surveyed for weaknesses in a non-intrusive manner. [15] [9] [10]Such tools would conduct uninterrupted assessments and scans for vulnerabilities making it shorter to discover and fix the flaws found. This is especially true in the sector of healthcare, where IoMT devices are always in operation, rendering any form of manual testing unfeasible.

- **AI-Driven Frameworks**:
  The healthcare industry stands to benefit immensely by embracing new technologies such as artificial intelligence (AI) within penetration testing. For example, intelligent tools could learn through machine learning algorithms from previous attacks and suggest areas that are prone to new attacks and be modified to the current attacks. In the future, it is suggested, more attention should be directed towards the development of artificial intelligence systems specifically designed for the Internet of Things in healthcare, capable of detecting vulnerabilities in firmware, communication, and web interfaces. With the help of AI tools, it would also be possible to execute realistic multi-vector attacks that would provide the existent weaknesses of the system to a higher extent. [3] [15]

- **Benefits**:
  Integrating front Fibroblasts, powered by automated tools, would increase productivity and precision to such an extent, that it is possible for penetration testers to reach out to more devices within shorter time spans. Moreover, AI-assisted variant integrates constant surveillance that helps identify intrusions into the systems and enables an organization to stop the attacks from happening in the first place.

B. Exapandinf Penetration Testing for IoT and IoMT Cybersecurity in Real Time

Many devices from the Internet of Medical Things (IoMT) such as smart insulin pumps, heart monitors and pacemakers allow users to access important information in real time and are therefore indispensable for critical and immediate patient interventions. As a result of this real time nature, they have high chances of being victims of hostile and time-based e-violence where even a slight lapse or interruption could have serious implications resulting in death. [14]

- **Simulating Real-Time Attacks**:
  Further studies should identify ways in which penetration testing techniques can be developed for engaging in cyber-attacks on real time toggled IoMT devices while maintaining the normal operational functions of the devices. Most of the common penetration testing methods are intrusive and may disturb the working of a device which is not a desirable outcome. This calls for the need for a new generation of sophisticated non-intrusive approaches, which are required to help impact positively on the outcome of any security evaluations without posing a risk to any healthcare procedures.

- **Non-Invasive Testing Methods**:
  Scientists need to find and examine passive testing processes concentrated above the hardware level,

using ways like sandboxing or running virtually crafted scenarios instead of active systems. These approaches would deliver thorough evaluative studies without compromising the functionality of the active IoMT devices being evaluated. Furthermore, these devices must include an alerting component for the organizations to be informed before and not during an attack on patient care. [8] [3]

- **Benefits**:
  Simulated attacks may be conducted in a safe environment, that does not compromise device operation, thus identifying and fixing vulnerabilities without compromising on safety where life preserving apparatus have to be used on patients.

C. Security Framework for Emergency IoT/IoMT Technologies

With the emergence of next-generation technologies such as, 5G-enabled medical devices, AI-based diagnostic tools, edge computing, and other mobile devices in healthcare organizations, it may be expected that the existing security systems will also be able to cover the new issues emerging out of these technologies, which may not be the case.

- **Expanding Existing Frameworks**:
  Dorte & Goh's (2018) Provides security benchmarks based upon the OWASP IoT top 10 and MITRE ATT&CK which however pinpoints the need for penetration testing in current IoT devices and similarly confirms that those frameworks should be improved. As the 5G communication and further expanded networks and advanced methodologies such as AI, and edge-based Internet of Medical Things (IoMT) devices will be introduced, the extension to these frameworks will be necessary. For instance, a 5G enabled medical device will have some differences with latency and data transmission protocols which offer some of the attacks missing in conventional frameworks.

- **Developing New Standards**:
  In regard to the improvement of existing security policies, further studies should aim at the development of new security policies that would adequately address the needs of the healthcare IoT and IoMT devices. Such standards must be designed based upon the fact that healthcare environments are complex and heterogeneous, involving the communication of several devices utilizing different protocols and platforms. [16] [12]In a scenario whereby the medical IOMT devices are used predominantly, standards that support rapid adoption of IoMT devices and application with privacy and interoperability would be most important in protecting the devices in complex healthcare dispensation.

- **Benefits**:
  By constructing advanced designs and specialization standards, healthcare organizations will be given the guidance on the best practices for securing the emerging IoT/IoMT technologies and assist them in dealing with new threats and maintaining protection uniformly across all the devices.

D. Addressing Regulatory and Compliance Challenges

The public health system is one of the regulated systems since there are guidelines that govern privacy rules such as HIPAA, GDPR, and others, which have strict rules on how personal health information PHI is treated. These regulations, however, restrict the use of penetration testing as well since owing to some tests, privacy, and data regulations can be breached. [15]

- **Integrating Compliance into Testing:**
  In their future studies, the researchers should consider investigating the possibilities of incorporation of legal responsibilities into the methodologies of penetration testing so that any undertakings that organizations would wish to carry out in order to comprehensively secure evaluations do not break any laws. That is also one of the topics to be addressed such as building software that would automatically check compliance and notify the testers as to when some of their methods may be infringing data laws. [4] [3]

- **Regulatory Best Practices:**
  Yet, there is a lack of best practice guidelines which will assist the healthcare systems in conducting penetration tests while at the same time respecting all the measures that need to be in place to ensure compliance. It is necessary to study in what ethical ways penetration tests can be performed on live systems without breaching patient confidentiality. At the same time, it is possible to employ compliance-based testing tools that limit the types of tests to be performed based on the presence of laws.

- **Benefits:**
  This positively impacts the vulnerability testing of healthcare systems, as including regulatory compliance when considering penetration testing should not hinder security measures. legal liabilities from litigation can be reduced as there is enhanced management of cyber security.

E. Penetration Testing for Legacy IoT Systems in Healthcare

Many health care providers have been ensnared by legacy IoT and IoMT devices, which are however no longer supported by regular security updates. Such devices are probably the most exposed to cyber-attacks since they are most of the time not easy to patch or upgrade. Consequently, newer penetration testing methodologies are also required for these devices, incorporating their limitations.

- **Securing Legacy Devices**:
  In future research, there must be more penetration testing approaches worthy that do not in any way bring about disruption of the operations of the systems under evaluation. Testing techniques must be developed so as to fit within the constraints of the legacy devices and the obsolete communication protocols and firmware systems that they employ. Effective controls should be researched, compensating controls, that can assist in minimizing the exposed risk, where timely direct patching or updates are not possible. For example, legacy systems could be protected from external network attacks using techniques such as network segmentation and firewall rules.

- **Extending Device Lifespan**:
  In addition, penetration testing should also be included in a broader scope of activities aimed at sustaining the reparable serviceable period of old types of devices by figuring out how to protect them without fully replacing them. With the incorporation of low-cost innovations to the old devices, it enables healthcare organizations to continue operating on even deeply rooted medical devices without compromising their security. [8] [5]

- **Benefits:**
  Healthcare providers sustain their older devices by creating efficient testing techniques and targeted testing methods for turnover. This will allow organizations to safeguard systems while managing the threat caused by cyber-attacks against legacy systems. [3]

V. Conclusion

The deployment of IoT and IoMT devices oh the health system domain has assisted greatly in the care of patients, improving systems as well as supporting accurate diagnosis and monitoring of patients at any time. Nonetheless, such improvements come at a very high risk especially in the field of cyber security since they have prone such mission critical systems to risks like data leaks, device hijacks, and service denial among others. Because healthcare information is sensitive, and connected devices are an integral part of delivering patient care, these systems need to be secured at all costs.

This proposal`s literature review has looked at different penetration testing methodologies that have been employed in conducting different levels of security testing within the area of healthcare IoT and IoMT systems. Black-box, white-box, and grey-box testing methods that were investigated focused on determining the level of vulnerability of health information technology in relation to its network architecture and the embedded system. These methodologies, when properly utilized give health care institutions windows of opportunities to implement anti forensics measures to eliminate the risk of exposure to the targeted unauthorized personnel.

Nonetheless, it has also been noted in the review that there are equally important threats in protecting the security of healthcare IoT and IoMT systems such as resource constraints of devices, level of regulation, and nature of healthcare networks. Penetration testing is undoubtedly still one of the firm security measures, but it is appreciated that more advanced tools and frameworks need to be originated due to advancement of adversaries. Tools for efficient security control need to include automated approaches, specific approaches adaptable to healthcare settings, and non-invasive techniques.

In conclusion, while penetration tests constitute a vital protective approach towards the healthcare IoT and IoMT infrastructures, more work and time need to be spent on their development in order to meet the needs of the latest and the future scenarios. The healthcare industry cannot afford a static approach towards cyber security for protection of patients' information and safety of internet connected medical devices. Change in penetration testing methods and control measures at the health care organizations will help in reversing the cloud of cyber-attacks facing healthcare organizations and the confidence of the patients maintained.

VI. Acknowledgements

The author's deepest appreciation is extended to Mr. Kanishka Yapa for his input, comments, and support during the research. His contribution has added value to the completion of this paper. The Sri Lanka Institute of Information Technology (SLIIT) provided necessary facilities and e-learning resources which played a critical role in the review. Gratitude extends to colleagues and family members for their support and encouragement during the project.

VII. References

[1] J. D. a. R. Thompson, "Cybersecurity challenges in securing healthcare IoMT devices," *Journal of Medical Cybersecurity*, vol. vol. 12, no. no. 3, p. pp. 156–165, 2019.

[2] A. S. a. R. J. J. Doe, "A study of IoT security protocols," *EEE Internet of Things Journal*, pp. pp. 123-130,, 2022.

[3] L. e. a. Smith, "Black-Box Penetration Testing for Privacy-Conscious Healthcare IoT Systems," *Cybersecurity in Healthcare Review*, vol. vol. 7, no. no. 1, p. pp. 88–97, 2021.

[4] A. &. L. H. Johnson, "White-Box Testing in Complex Healthcare IoT Systems: Evaluating Communication Protocol Vulnerabilities," *ournal of IoT Security*, vol. vol. 14, no. no. 2, p. pp. 112–123, 2020.

[5] J. e. a. McCarthy, "Grey-Box Testing for IoMT Devices: A Hybrid Approach to Securing Medical Technology," *International Journal of Medical Device Security, vol. 13, no. 3, pp. 145–153, 2022.*, vol. vol. 13, no. no. 3, p. pp. 145–153, 2022.

[6] Q. e. a. Nguyen, "Adapting OWASP IoT Top 10 for Securing 5G-Enabled Healthcare IoT Devices," *Journal of Cybersecurity in Next-Generation Networks,* vol. vol. 8, no. no. 1, p. pp. 101–112, 2023.

[7] T. &. H. M. Zhang, "Balancing Penetration Testing and Regulatory Compliance: A Study on HIPAA and GDPR in Healthcare IoT," *Journal of Data Privacy and Security,* vol. vol. 18, no. no. 4, p. pp. 303–311, 2020.

[8] P. &. B. D. Taylor, "Nmap as a Tool for Network Discovery in Healthcare IoT: Advantages and Limitations," *Journal of Network Security,* vol. vol. 11, no. no. 2, p. 75–83, 2021.

[9] T. e. a. Garcia, "Metasploit in Healthcare IoT Systems," *Proceedings of the International Conference on Cybersecurity and Healthcare, Barcelona, Spain, ,* p. pp. 223–230, 2020.

[10] E. &. K. S. Martinez, "Testing Web-Based Healthcare Systems Using Burp Suite: A Study on SQL Injection and XSS Vulnerabilities in Patient Portals," *Journal of Web Security in Healthcare,* vol. vol. 10, no. no. 4, p. pp. 267–275, 2022.

[11] L. &. E. N. Richards, "Wireshark as a Tool for Real-Time Traffic Analysis in Healthcare IoT Networks," *Journal of Network Security and Analysis,* vol. vol. 13, no. no. 3, p. pp. 102–110, 2022.

[12] K. &. S. M. Williams, "Proactive Penetration Testing for IoT Networks in Healthcare," *International Journal of Healthcare Information Security,* vol. vol. 9, no. no. 2, p. pp. 47–55, 2021.

[13] R. &. P. D. Green, "Network Segmentation Strategies for Reducing Healthcare IoT Attack Surfaces: A Penetration Testing Perspective," *Healthcare Information Systems,* vol. vol. 22, no. no. 5, p. 199–210, 2021.

[14] K. e. a. Raman, "AI-Driven Penetration Testing for Real-Time IoMT Systems: Enhancing Security without Disrupting Patient Care,," *IEEE Transactions on Biomedical Engineering,* vol. vol. 68, no. no. 9, p. pp. 2349–2357, 2021.

[15] S. &. P. H. Kim, "Challenges in Testing IoT-Specific Security Threats: A Case Study on Healthcare IoT Devices," *Proceedings of the International Conference on IoT Security and Privacy, San Francisco, CA, USA,* p. pp. 97–104., 2022.

[16] A. P. G. Carter, "Beyond Penetration Testing: Developing a Comprehensive Cybersecurity Strategy for Healthcare IoT," *Healthcare Technology and Security Journal,* vol. vol. 15, no. no. 1, p. pp. 101–110, 2022.

AUTHOR PROFILE

JAYARATHNA K.P.G.C.M is a cybersecurity enthusiast currently pursuing a bachelor's degree at the Sri Lanka Institute of Information Technology (SLIIT). He excels in identifying vulnerabilities and putting preventative security measures in place because he concentrates on penetration testing and ethical hacking. His passion for increasing knowledge and understanding of the subject of cybersecurity is demonstrated by his active involvement in workshops and seminars, which demonstrates his commitment to security awareness and education