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

Chethana Amidu Rathnayaka

*B.Sc. (Hons) Information Technology Specialized in Cyber Security,*

*SLIIT Malabe*

*Abstract*- This research investigates a comprehensive review of penetration testing techniques to protect Internet of Medical Things (IoMT) and Healthcare Internet of Things (IoT) systems. Phishing, identity theft and unauthorized access are just a few of the possible cybersecurity attacks in which IoT and IoMT integration into the healthcare sector exposes the sensitive personal data of patients and the functioning of crucial medical equipment. The research evaluates the modern penetration testing techniques, studies the extent to which healthcare vulnerabilities are prevented and remediated; and highlights the challenges of applying such techniques on IoMT. At the same time the work more than addresses research shortcomings in terms of possible future strategies for building better security systems suited exactly to the scope of IoMT. The objective is to provide relevant health care organizations with measures to avert threats or increase their ability to deal with them and improve the safety of patients and their information. Future research focuses on creating new methodologies that utilize artificial intelligence and machine learning to enhance to detect and mitigate cyber threats around the healthcare environments.

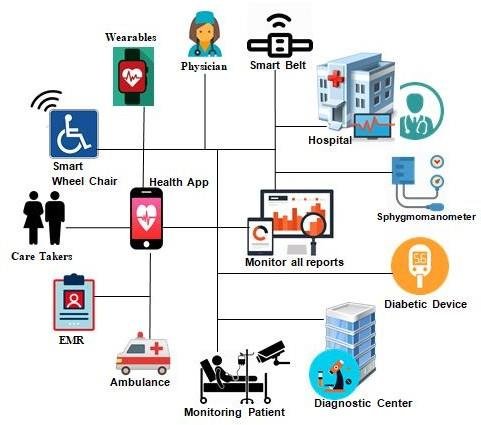
**Index Terms-** 5Gand Edge computing, AI and Machine Learning, Blockchain Technology, Healthcare IoT, IoMT (Internet of Medical things), MEd jack Attack, Quantum Cryptography, WannaCry Ransomware

1. Introduction

The Internet of Things (IoT) and the Internet of Medical Things (IoMT) Concepts in furtherance of the communication between devices and systems that better the treatment of patients and the workflow in general is quite noticeable. Healthcare systems are always integrated with special equipment and mobile apps called IoMT, which provides monitoring and data evaluation in real-time. However, this integration brings about new challenges, in particular cybersecurity threats because patient sensitive information, which these devices handle and which is fundamental for medical processes, is involved.

Cybersecurity of IoMT needs a lot of attention since a break in the security of the system can result in theft of data, wrong party access, or even interfere with ongoing emergency procedures. Patients in healthcare organizations and stakeholders within the healthcare sector are inflicted with financial, reputational, and trust issues as these threats are costly to healthcare organizations and disrupt patient care. Furthermore, the diversity in the category of IoMT devices and their computation capabilities also makes it harder to secure these systems as the device gets complicated.

The risks of cyber-attacks are exacerbated in healthcare, as they can significantly reduce patient trust, disrupt health systems, and even endanger human life. Therefore, it is crucial to prioritize cybersecurity in today’s healthcare organizations. [1] Cyberattack can lead to financial costs, damage to an organization’s reputation and even legal consequences for these healthcare organizations. Due to a breach in the medical privacy of a patient, the patient might lose trust in the service providers and may even suffer from fraudulent activities or impersonation.



**Figure 01: Internet of Medical Things**

This study will contribute to the debate by identifying current research gaps and proposing guidelines for future research aimed at developing more robust security architectures specifically designed for IoMT within the context of healthcare.

1. Research Objectives

This study focuses on investigating penetration testing methodologies, examining on current testing practices and identifying gaps on the current practices, develop and enhance penetration testing frameworks on safeguarding IoMT systems on healthcare industry. Furthermore, discovering future research directions emphasizing defective mechanisms related to healthcare cyber threats. Initially analyzing the existing methods and vulnerabilities unique to IoMT like variety of device kinds, issues with data privacy, and intricate network architectures. Understanding current practices and the gaps and limitations found in the frameworks.

The assessment also aims to offer suggestions for the creation of enhanced penetration testing frameworks that are especially suited to the requirements of IoMT systems in the healthcare industry. This involves utilizing cutting-edge technology to improve the identification of sophisticated threats, such as machine learning and artificial intelligence. Furthermore, several others highlight the necessity of explainable Ai (XAI) methods in the context of cybersecurity applications, intrusion detection, malware identification, and spam filtering [2] and considerable attention has been devoted to the interpretability, explainability, and trustworthiness of ML/DL models. [2] In order to keep up with the changing cybersecurity landscape in healthcare, the review will conclude by outlining future research topics and highlighting the necessity for more proactive defense mechanisms and adaptive security solutions. When the objectives are met this review aspires to help develop strong and pinpointed penetration testing methods which would be able to protect the health care organizations from evolving cyber threats and ensure the safety as well as the security of patients’ information.

1. Review of the literature

3.1. Definition of Healthcare IoT and IoMT Systems

The internet of medical things (IoMT) is the collection of medical devices and applications that connect to healthcare information technology systems through online computer networks. [3] These devices include remote monitoring tools, wearable sensors, smart implants and mobile applications. Recently, the IoMT has been widely applied in many areas, including smart hospitals, remote health monitoring, disease diagnosis, and infectious disease tracking, [4]operational efficiency, robotic surgery, glucose monitors for diabetes management. IoMT devices play an important role various areas in healthcare; Remote Patient monitoring: helps doctors and healthcare professionals to track essential health statics from patients remotely. This method saves time by reducing health care visits. Personalized medicine: IoMT devices, such as smart implants, remote patient monitoring devices, smart pills, and other connected devices, collect and transfer comprehensive patient data, including medication adherence and vital signs. [5]Cost Reduction: The clinical processes and information management are automated with the IoMT devices and hence economical productivity of the health care environment is improved. Surgery and Robotic Assisted Surgery: IoMT devices are mostly deployed during the surgical process where connected devices and robotic equipment help doctors in performing the procedures and provide real-time data during these medical procedures.

* 1. **Case Studies**

The increased use of IoMT has given rise to concerns in the area of cybersecurity owing to the risks associated with data loss, device interference and breach of services and there are studies done for the improvement of the healthcare industry. There are many studies and case examples which illustrate the vulnerabilities and also explored new methods of the IoMT systems.

**The MedJack Attacks:** The term “MedJack” means Medical Device Hijacking which is the most popular attack on IoMT. The most important part of a MEDJACK attack is hijacking a medical device. Until an attacker gains access, they are unable to do anything. Consequently, the malware used to infiltrate these devices has become more sophisticated and targeted. [6] It was discovered that such attacks make use of outdated software and ineffective authentication procedures on IoMT devices. The MedJack cases; As of 2015, the healthcare industry became the most attacked industry, experiencing 32.7% of all known breaches nationwide. (TrapX, 2015),[6] prompted worries about the obsolete IoMT systems provided for medical professionals to utilize, which lack security improvements, as well as the hazards of internet-enabled attacks on patient's data confidentiality.

**The WannaCry Ransomware:** The WannaCry [ransomware](https://www.sdxcentral.com/security/definitions/what-is-ransomware/) attack of May 2017 was one of the most widespread ransomware attacks, exploiting a leaked Windows software vulnerability. [7] The hackers encrypted sensitive data and demanded a ransom to release data. Microsoft were aware of this attack prior and released a path for the vulnerability but most organization did not update the path. A substantial number of IoMT devices, including MRI scanners and blood coolers, were rendered inoperable because they used older Windows operating systems compromised with the malware. Infected systems in over 150 countries resulted in a measly $100,000 payout for the attackers. [7] The attackers were a group called The Lazarus Group. This attack clearly demonstrated how embattled operational fires within IoMT systems, in the lack of cyber security measures, might jeopardize patient safety.

**Managing preeclampsia:** Preeclampsia is a severe hypertensive pregnancy disease that is usually detected after the 20th week and has a global prevalence of 5-8%. It has the potential to produce major negative health impacts for both the mother and the kid. Machine learning (ML) methods and the Internet of Things (IoT) have been successfully implemented in medical research to improve the diagnosis and prevention of complex diseases and syndromes. The goal of this work is to undertake a review of the most recent work on preeclampsia detection. [8] for the implementation of the system, A preliminary survey was conducted in 100 pregnant women with a diagnosis of preeclampsia. Each subject was provided with a device: a wearable blood pressure cuff along with a mobile app for daily use where doctors monitored their statics remotely. That leads to improvement with engagement with the patients, early detection of symptoms and reduced cost.

* 1. **Current Penetration testing techniques for IoMT**

Penetration testing, sometimes known as ethical hacking, is an important part of cybersecurity that focuses on identifying and addressing weaknesses in any digital system. In the case of the Internet of Medical Things (IoMT), which is made up of numerous linked medical devices and applications, penetration testing should consider the unique nature of these ecosystems as well as their security. The following outlines standard penetration testing tools and methodologies, their use and application to IoMT-specific vulnerabilities, and an assessment of their usefulness and weaknesses. For standard penetration testing tools for network security and network protocol analysis are Nmap and Wireshark. Vulnerability scanning and management tool to check IoMT systems vulnerabilities; OpenVas and Nessus. There are exploitation frameworks that provide tools to test vulnerabilities and to test effectiveness of the current security measures, intuition detection systems and tools to minimize the damage for critical medical devices. Metasploit Framework and Core Impact are such frameworks. [9] For IoMT devices Wireless connections are essential. If our wireless network is ’unsecured’ or ‘open’ then an intruder can easily gain access to our internal network resources as well as to the Internet, all without our consent. Aircrack-ng Suite and Kismet are such tools. Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. [9]

The increasing population and the rise in chronic diseases have increased the demand for hospital resources and monitoring technology. [11] use of IoMT devices has increased because of current pandemics like Covid-19. Although this technology brings effectiveness and cost reduction to healthcare industry several limitations are there.

**The Diversity of devices**: IoT devices are a multiplicity inside the IoT networks, ranging from full personal computer to low radio frequency identification. As a result, it is difficult to find a single security system that can accommodate even the simplest devices. [12]

**Resource constraints:** A critical issue in implementing security for the streaming health information is to offer data privacy and validation of a patient’s information over networking environment in a resource efficient manner. [13]Current computational power to implement these IoMT system is a crucial problem. n IoT lack storage capacity, power, and CPU that make the system very complicated. [14]

**Real-time and critical Operations:** Because IoMT devices are typically used in vital patient care operations, penetration testing must be conducted with extreme caution to prevent disrupting essential services. This reduces the amount of testing that can be done securely, particularly active exploitation approaches. While typical penetration testing tools and techniques can provide extremely significant insights, they must be tailored to the specific problems given by these systems. This means that in healthcare, significant attention is made in the selection of tools while custom-developing testing frameworks that disrupt patient care as little as possible while still detecting and mitigating vulnerabilities effectively.

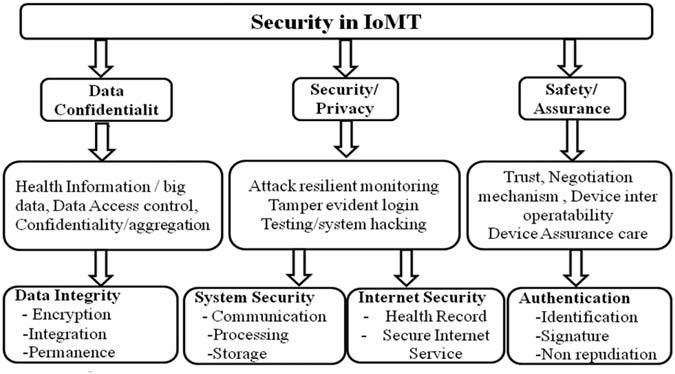
* 1. **Challenges in securing IoMT systems**

This is one of the most difficult tasks because it involves unique systems and extremely important information. IoMT devices are critical in servicing patients, but they introduce a number of dangers that must be addressed in order to protect patient safety, data quality, and the whole healthcare system. There are main challenges in securing IoMT systems.

**Data Privacy**: Data privacy remains a major concern in IoMT contexts because to the large amounts of sensitive patient information handled by these systems, such as medical records, diagnoses, and ongoing operations. Privacy is an important tension in the systemic model for IoT security because of the ubiquitous character of the environment. [15] Unauthorized access, insecure data transmissions, insecure storage methods and regulatory compliance are key challenges in securing data privacy. These leads into Man-in-the middle attacks [16], tampering and eavesdropping.

**Diverse range of Devices:** IoMT settings contain a diverse range of devices, including sensors, wearable monitors, imaging machines, and smart surgical tools. These devices are made by various vendors, run different operating systems, and communicate using various protocols. The primary concern is the Lack of Standardization. The lack of standardization is a problem for the Internet of Things (IoT) because it makes it difficult for different devices and systems to communicate and work together seamlessly. IoT devices are made by many different manufacturers and can use a wide variety of communication protocols and data formats, making it challenging to develop a unified standard that works across all devices. [17]

**Network Complexity:** IoMT devices having different levels of security and the basic security protections not being their cause a major surface for the threats. The complexity of healthcare networks and size of the interconnected devices through network creates a larger attack surface to the attackers. If your IoT ecosystem of devices grows, you give the hacker a greater surface to hit. [18] Diverse communication protocols are used in IoMT devices such as wi-fi, Bluetooth and proprietary protocols. IoT communication protocol varies according to criteria such as the transport layer Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), architecture (publisher/subscriber and client/server), security, service quality, the priority mechanism, and packet header size. [19] Securing IoMT systems require addressing faults in mentioned data privacy, Diversity of devices and their security measures and Network complexity issues adhering to variety of protocols.



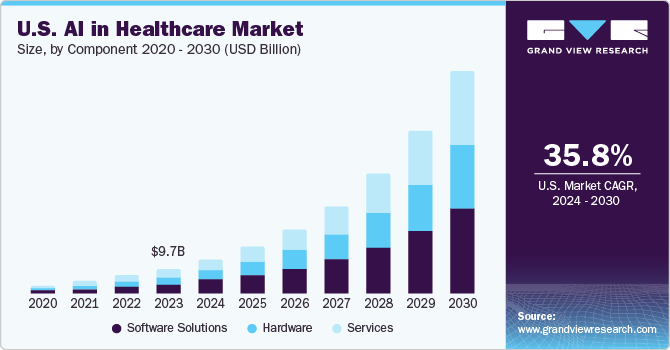
**Figure 03: security and privacy concerns**

1. **Future Research**

The rapid growth in networks of IoMT systems leads to increment of cyber threats with parrel to progresses made in developing security measures and solutions in healthcare industry. The integration of cutting-edge technologies facilitates this paradigm shift. A new age of healthcare system optimization and patient care is being ushered in. [20] This section brings out key gaps in consideration to current research, emerging trends and future research to developing new techniques for the securing of IoMT systems. There are several gaps remaining that require consideration for the future of IoMT systems.

Lack of penetration testing Frameworks: current penetration frameworks are well organized and well established for general penetration testing practices but frameworks that are specifically designed to address IoMT systems are lacking. These frameworks are essential for managing upcoming and known risks. Future research must focus on developing IoMT specific Frameworks. Lack of research on AI and ML specified security solutions: AI and ML-aided cybersecurity applications are on the rise; nevertheless, the overdevelopment of IoMT security systems based on these models is still weak. Developing artificial intelligence models that will recognize and neutralize threats aimed at IoMT systems in real-time, learning new methods of attack and also being lightweight enough to fit into IoMT devices. [21] Insufficient Focus on Data Privacy: Over the IoMT environment, medical data can be accessed by various malicious actors as it presents huge security concerns regarding confidentiality, integrity, and accuracy. [22] The system becomes vulnerable with respect to inadequate authorization or authentication of medical devices or sensors, lack of knowledge about encrypting the data, insecurity of device interface, etc. [23] Data transfer among different infrastructures needs security and privacy-preserving solutions (Rafique et al., 2019a). [24] Future study should look for creative means to ensuring data privacy, such as encryption and safe data storage. To address these gaps and challenges, focusing on emerging trends in IoMT systems and future research are essential for the advancement in security.

**Adoption of AI and Machine learning (ML):** There is increased use of AI and ML. This technology can be used to assess large volumes of data generated by IoMT devices, identifying potential security issues and responding to prevent the situation from getting worse. And AI-based models have shown their worth in pharmaceutical and healthcare industries by improving the efficiency in therapeutic drug manufacturing, real-time health monitoring, and predictive forecasting. [25]



**Figure 04: U.S. AI in healthcare market**

**Blockchain for secure data Transmission**: Blockchain technology has received attention as a means of protecting data across IoMT networks. The key reason is that it is decentralized in nature and incorporates methods to secure data such as recording data exchange in ways that cannot be manipulated. The use of a time-stamped feature of blockchain could be very useful in detecting the integrity of such data and information. Once these data are stored in a distributed ledger, the detection of an anomaly in patients’ data could be tackled efficiently. [26]

**Quantum resistant cryptography:** As quantum computers become more practical, classical encryption techniques will be rendered useless in the near future. Studies being conducted in this area are directed towards development of algorithms that are not susceptible to quantum threats in future and therefore will protect IMOT data. Quantum key distribution then generates a secure key leveraging entangled quantum states, becoming the cornerstone of encryption. Quantum encryption shields healthcare data in an impenetrable veil of secrecy, leveraging the complexities of quantum mechanics to thwart unauthorized decryption attempts. [27]

**5G and Edge computing**: With the introduction of 5G and the rise of edge computing, IoMT security has improved possibilities. 5G boosts communication between consumers and computing devices by allowing clients to get information faster and greatly reducing the time required to respond to systems. Edge computing decreases the quantity of data that must be transferred to remote centralized servers by performing computational activities near the data's source. In support of healthcare devices needing uninterrupted and reliable low-latency communications (URLLC), the cooperative utilization of 5G and MEC technologies is a way to go. [28]

 Features and improvement plan for future 5G
 **Figure 05 : Features and improvement plan for future 5G**

**Conclusion**

This review has also underscored the need to improve the penetration testing approaches for Internet of Medical Things (IoMT), as these systems tend to have their own security issues that need particular attention. On one hand, the simple IoMT sensors as well as the complex medical equipment habitually used in practice are of immense importance in enhancing the patient care and the healthcare services operational efficiency. However, their diversity, sensitivity of handled data and complexity of the networks also exposes them to significant security risks. Existing penetration testing methodologies which apply mostly to general IT and IoT systems do not adequately address vulnerabilities that are unique to IoMT. These standards have been glaringly absent in the reviews done with researchers noting that there is failure in the integration of new technologies including AI, Machine learning for timely response to threats, blockchain for secure network transmissions and 5G and edge computing for enhanced effectiveness. In order to enhance the security of IoMT, the next studies should aim at creating advanced penetration testing frameworks relevant to the IoMT environments that will encompass different operational devices and contexts within the healthcare industry. There is also a need to incorporate more advanced predictive technologies into these frameworks to reduce risk comparatively more than is currently possible. Also, contribution from the industries is equally important in order for common security policies on all the IoMT devices to be implemented.

# References

|  |  |
| --- | --- |
| [1 ] | A. Muacevic, "Clinicians’ Perspectives on Healthcare Cybersecurity and Cyber Threats," 15 octomber 2023. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10642560/#:~:text=The%20risks%20of%20cyber%2Dattacks,cybersecurity%20in%20today's%20healthcare%20organizations.. |
| [2] | A. Q. M. G. A. A.-F. A. R. J. Q. Khansa Rasheed, "computers in Biology and Medicine," ScienceDirect, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0010482522007569. |
| [3] | Ben Lutkevich, "IoT Agenda," TechTarget, march 2023. [Online]. Available: https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things. [Accessed 10 september 2024]. |
| [4] | J. W. W. Z. Chenxi Huang, "Internet of medical things: A systematic review," Neurocomputing, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231223008421. |
| [5] | c. communications, "IoMT AND PERSONALIZED MEDICINE,A Paradigm Shift in Healthcare that Tailors Treatments and Medical Devices to Individuals.," 5 april 2024. [Online]. Available: https://www.cultivate-communications.com/medical-device/iomt-personalized-medicine-shift-healthcare-tailors-treatments/. |
| [6] | S. Meggitt, "Tufts University," 12 december 2018. [Online]. Available: https://www.cs.tufts.edu/comp/116/archive/fall2018/smeggitt.pdf. |
| [7] | M. Lessing, "Sdxcentral," [Online]. Available: https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-wannacry-ransomware/. [Accessed 11 september 2024]. |
| [8] | S. S. S. S. a. K. K. Hadiyanto Hadiyanto1, "E3S web of conferences,The 8th International Conference on Energy, Environment, Epidemiology and Information System (ICENIS 2023)," 17 november 2023. [Online]. Available: https://www.e3s-conferences.org/articles/e3sconf/abs/2023/85/e3sconf\_icenis2023\_02058/e3sconf\_icenis2023\_02058.html. [Accessed 11 september 2024]. |
| [9] | S. Raj and N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool,," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020. |
| [10] | P. Pandit, "Researchgate," octomber 2021. [Online]. Available: https://www.researchgate.net/publication/354971431\_A\_Study\_of\_Security\_Tools\_for\_Wireless\_Networks. [Accessed 11 september 2024]. |
| [11] | K. Mohit, A. Kumar, S. Verma, P. Bhattacharya, D. Ghimire, S.-H. Kim and A. Hosen, "Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues.," Electronics 2023, 2023.12. |
| [12] | A.-S. Suha Ibrahim, "Security Challenges and Limitations in IoT Environments," *IJCSNS International Journal of Computer Science and Network Security,* vol. vol19, p. 7, 2019.02. |
| [13] | O. W. S. W. W. A. K. S. G. L. Sandeep Pirbhulal, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Generation Computer Systems,* vol. 95, pp. 382-391, 2019. |
| [14] | A. S. M. A. Y. N. W. K. M. Haroon, " Constraints in the IoT: the world in," 2016. |
| [15] | Y. C. †. E. N. Z. C. A. B. Arbia Riahi∗, "A Systemic Approach for IoT Security," in *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*, 2013. |
| [16] | M. V. J. L. B. Kapil M. Jain, "A Survey on Man in the Middle Attack," *IJSTE - International Journal of Science Technology & Engineering,* vol. 2, no. 9, 2016. |
| [17] | v. kunreth, "Why is lack of standardization a problem with IoT," 23 feb 2023. [Online]. Available: https://www.linkedin.com/pulse/why-lack-standardization-problem-iot-volkmar-kunerth#:~:text=The%20lack%20of%20standardization%20is,communicate%20and%20work%20together%20seamlessly.. [Accessed 11 sept 2024]. |
| [18] | C. Preisler, "moxso," 24 04 2023. [Online]. Available: https://moxso.com/blog/internet-of-things-a-larger-attack-surface. [Accessed 11 09 2024]. |
| [19] | M. A. E. Ü. Ç. K. K. A. S. Cüneyt Bayılmış, "A survey on communication protocols and performance evaluations for Internet of Things,," science Direct, 6 december 2022. [Online]. Available: (https://www.sciencedirect.com/science/article/pii/S2352864822000347). |
| [20] | W. Shafik, "IoMT Future Trends and Challenges Emerging Technologies Policy Implications and Research Questions," in *Lightweight Digital Trust Architectures in the Internet of Medical Things (IoMT)*, IGI Global, p. 23. |
| [21] | L. A. T. Fadi Muheidat, "Chapter 2 - AIoMT artificial intelligence (AI) and Internet of Medical Things (IoMT): applications, challenges, and future trends," vol. 14, pp. 33-54, 2023. |
| [22] | B. Y. Pankaj KHATIWADA, "Performance Metrics,Merits, Demerits, and Challenges," *An Overview on Security and Privacy of Data in IoMT Devices,* p. 11, 2022. |
| [23] | S. D. K. V. G. B. E.-L. A. Kaur M, "Secure and Energy Efficient-Based E-Health Care Framework for Green Internet of Things," in *IEEE Transactions on Green Communications and Networking*, 2021. |
| [24] | H. F. A. W. R. A. Q. J. Q. Raihan Ur Rasool, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML," *Journal of Network and Computer Applications,* vol. 201, 2022. |
| [25] | B. (Basel)., "national library of medicine," 12 aug 2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9330886/. |
| [26] | M. E. ,. B. A. B. a. K. Imed Ben Dhaou, "Edge Devices for Internet of Medical Things: Technologies, Techniques, and Implementation," Multidisciplinary Digital Publishing Institute, 22 july 2021. [Online]. Available: https://www.mdpi.com/2071-1050/15/7/6177. |
| [27] | B. Bagath, "Enhancing Healthcare Data Security Using Quantum Cryptography for Efficient and Robust Encryption," *Journal of Electrical Systems 20(5s):1993-2000,* 2024. |
| [28] | H. Y. ,. a. J. Murtaza Ahmed Siddiqi, "5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices," *Electronics 2019,* vol. 8, no. 9, 2019. |

**Author**

**A person in a suit

Description automatically generatedChethana Amidu Rathnayaka,** Undergraduate B.Sc. (Hons) Information Technology Specialized in Cyber Security.The review article is done as an Applied Information Assurance.