**LITERATURE REVIEW TOPIC: THE ROLE OF CYBERSECUIRTY THREATS TO INTERNET OF THINGS (IoT) IN HEALTHECARE SECTOR.**

**Introduction:**

Advancement in technology is a continuous trend in today’s world and this is being experienced in healthcare sector. According to Junaid et al. (2022), the technology advancement in healthcare delivery services, have significantly improved many patients’ accessibility to advanced personalized healthcare especially in remote health monitoring, elderly care, chronic diseases and other fitness programs. One of the examples of healthcare technology advancement is the IoT devices which can be referred as Internet of Medical Things (IoMT) devices (Messinis et al, 2024). These devices have the capacity to collect basic health-related data, analyse, and transmit the data in the real-time activities through network communication to healthcare providers for management of patient’s health data. The invention of the IoMT devices has made health services efficient for the end-users however, the downside is the vulnerability of these devices to cyberthreats which could negatively impact the patients, healthcare-providers, and supply-chain vendors in the same ecosystem.

**Research Background:**

Cybersecurity threats to IoMT are those cyberattacks that affect IoMT devices vulnerabilities which cybercriminals execute for financial gains, reputations or hacktivism and these cyberattacks can be life-threatening to patients, reputational and damages to healthcare providers (Nguyen & Yasin-Nur,2023).

One of the main ideas behind IoMT is to enable objects generate data to interconnect through technologies like Radio Frequency Identification (RFID), actuators, sensors, and mobile phones (Rejeb. et al, 2023) for an effective monitoring of patients by healthcare practitioners. Unfortunately, these devices are prone to cyberattacks like data-privacy breach, malware. and DDoS and other IoT cybersecurity threats.

The objective of this literature review is to understand the potential cybersecurity threats of IoT in Healthcare sector, the mitigation mechanisms and regulatory framework on the research topic.

**Problem Statements:**

Integration of IoT technology in healthcare sector has created big opportunities for cybersecurity challenges such as cyberattacks on data storage and management system, and data transfers between devices etc (Sadek, et al 2022). Researchers emphasized that there is positive correlation between growth in IoT technologies and cybersecurity challenges based on the continuous transition from traditional to digitalization healthcare practices if the cyberthreats are not properly checkmated (Yamaganti, et al 2023).

Any cybersecurity breaches on these devices could be life threatening, or breach of patient’s data confidentiality could cause reputational damage for the healthcare providers. Imagine security breach on an implantable cardiac device, Infusion & insulin pump, oxygen supply equipment, or unauthorized access to patient’s information and the consequences on both the patients and other healthcare stakeholders. A continuous Investment on developing mitigation techniques on health-related IoT cybersecurity cannot be over-emphasized.

**Aim of the Research**

The aim of the research is to understand potential role of cybersecurity threats and vulnerabilities on IoT in Healthcare sector, solutions to the challenges and recommendation of further reviews in the field of study.

**Objective of Research**

In the research, I would like to achieve the following:

* Review existing literatures on similar topics.
* Research on IoT cybersecurity vulnerabilities and threats in the healthcare sector.
* Identify and analyse the shortcomings of the previous research.
* Provide recommendation and mitigation techniques**.**

**Research Questions:**

The following research questions will guide my literature review:

* What are the IoT devices in healthcare sector?
* What are the vulnerabilities and cyberthreats of these devices?
* What are current trends and impact of cybersecurity of IoT in healthcare sector ecosystem?
* What are the mitigations techniques of IoT cybersecurity in healthcare?
* What are the regulatory frameworks to secure IoT cyberattacks in healthcare?
* What is the future of IoT cybersecurity in healthcare sector?

**Research Methodology and Limitation:**

A qualitative review methodology was used in gathering relevant information from other researcher’s articles, academics journals, ScienceDirect, ACM digital library and Google scholars in understanding challenges of cybersecurity of IoT in healthcare sector. However, the review limitation is my inability to generate live data from interviews or questionnaires from stakeholders like hospitals, patients and IoT-applications providers**.**

**Definition of key terms**

* Internet Of Thing: IoT is a network of physical devices that can connect and exchange information (Gopalan et al, 2021).
* Internet of Medical Things: IoMT is a collection of medical devices and corresponding applications that connect to the healthcare IT systems through a computer network (Chacko & Hayajneh,2018).
* Cybersecurity is the measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam‐Webster 2020)
* Vulnerabilities: Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat (NIST SP 1800-17b).
* Artificial Intelligence: The application of computer algorithms to perform tasks generally associated with human intelligence (Messinis et al,2024)
* Blockchain: is technology for security-management solution for sharing information among authorized parties (Hireche, et al.2022).

**Summary**

The research has shown that cybersecurity is a major obstacle to great adoption of IoT in healthcare sector and according to Lu & Xu (2019), the traditional security protocols and mechanisms are not suitable in securing IoT in healthcare sector because the existing devices are limited at their low levels of scalability, integrity, and interoperability. Therefore, new methodologies and technologies should be developed to meet the security, privacy, and reliability requirements of IoT in Healthcare sector. My recommendation is further research on how deployment of advance AI-tools will contribute to an effective mitigation of IoT cybersecurity in healthcare sector based current technology trend of AI.

**Review on the Research**

**Cybersecurity threats and Vulnerabilities of IoT-devices in healthcare sector.**

Chacko & Hayajneh (2018) article stated that IoT gave healthcare sector the opportunity to redefine the sector’s workflow in-terms of service delivery efficiency and economic benefits. The authors estimated that two years from research, IoT-devices would reach approximately 50billion objects and great portion would be medical devices like pacemaker, infusion insulin pumps, mobile medical workstations etc. These are evidence of acceptability rate and importance of the new technology.

The study further pointed out that the interoperate capacity of the IoT-devices within internet infrastructures have increased the medical IoT-device vulnerability to cybersecurity threats. The authors referred to the IoMT like pacemakers, and infusion-pumps that receive and send information via internet can leave the patients vulnerable to cyberattacks example is where cyber-actor hacks IoMT devices to harm the patients such as unauthorized insulin injection or break into the device pre-programmed password with the aim of access the main medical database of a hospital. The authors concluded that any wireless medical devices on web-enabled IT-system are vulnerable to cyberthreats such as malware code-injection, DDoS, or data breaches etc and these attacks could be life threatening.

The authors further referred to a public release of malware code source that could build botnet for IoT-device attacks and stated that in 2015, two security researchers discovered 68,000 medical system that were exposed to online vulnerability and 12,000 of the system belong to one healthcare organisation whose operating system were connected to old version of window XP. Imagine the magnitude of cyberattacks on the organisation IoT-devices due to usage of outdated operating system.

Messinis et al, (2024) another researchers on enhancing IoMT security using AI gave a different dimension to understanding of the literature. The authors state that one of the debates in the field of IoMT involves trade-off between patient’s privacy, device usability, and data accessibility. And to maintain patient’s confidentiality while utilizing patient’s data for treatments and research purpose remain major challenge in the healthcare sector. They further analysis on how to use layered approach to classify the security of the IoMT-devices which includes: Perception layer that is device tampering, Networking layer which on compromise of system security such as device functionality, Distributed Denial-of-Service(DDoS) & spoofing attacks, Application layer that targets software, protocols and interfaces e.g. sybil and hole attacks and Transport layer which relates with data transmission which is highly prone to cybersecurity threats that comprise patient data confidentiality , device integrity and system availability.

Both reviewed articles adequately outlined varieties of potential cybersecurity threats on IoMT, but none gave depth review on AI cybersecurity threats related on IoMT considering the current era of AI technologies.

**Mitigation techniques on Cybersecurity-threats of IoT in Healthcare sector.**

Some of the strategies for mitigation of IOT cybersecurity-threats from my literature review are as follows:

Altulaihn et al, (2022) emphasised on end-to-end encryption, authentication and access control on physical layer of IOT architecture, Protocol & software application update, and deployment of network filtering such as secure MQIT and ABE algorithm.

According to Gopalan et al, (2021), they recommended the use of AI tools to protect medical IoT-device from cybersecurity-threats considering AI is the most efficient medium to process big data and get real-time accurate result. The processing of large volume of data generated by IoT-devices and reduce or eliminate cyber-vulnerability exposure could be achieved by use of AI methodology like Machine Learning (ML) based algorithm or Deep Learning (DL). The authors further proffer additional solution to the secure safety of data transmission by use of cryptography and steganography to analyse and detect any suspicious activities in the data transmission network.

Hirech et al, (2022) also provided mitigation mechanism based on Blockchain (BC) and AI- driven solutions. The blockchain technology is a secured security management solution that is used for sharing information among healthcare stakeholders and it combines with AI system to detect intrusion activities in the patient data and network traffic e.g. MEDSBA, an encrypted AI application that combines with BC. This encrypted mechanism uses two types of attribute-based encryptions, Key-Policy Attribute-Based Encryption and Ciphertext-Policy Attribute-Based Encryption that controls patients’ access to their own medical data which will automatically limit accessibility to patient’s data by cyber-actors.

In the above mitigations review, I observed that the authors did not mention human training as part of the mitigation strategies of IoMT cybersecurity knowing that the human buy-in is key to success of the strategy .Also, the authors that focused on AI-BC driven mitigation solution did not relate the mitigation solution to AI-driven cyberthreats in the same ecosystem and AI ethics implication was not also considered in the paper.

**Regulatory framework on Cybersecurity of IoMT**

In the interest of best practice and protection of healthcare stakeholder in context of IoMT cybersecurity threats, below are some regulatory frameworks around the subject.

Chacko & Hayajneh (2018) reiterated that the rise in hackable medical devices has forced the Food and Drug Administration (FDA) to issue guidance on joint responsibility of medical IoT-device cybersecurity measures by the device manufacturers and healthcare facilities for the purpose of protecting patient safety and device performance.

Thomasian & Adashi (2021) enumerated various regulatory bodies that aid securing of medical IoT from cybersecurity threats in United States and protects the patient’s data privacy in terms of confidentiality, integrity and availability of devices. Addition to Chacko & Hayajneh insight on FDA on premarket guidance, Thomasian & Adashi stated that FDA leverages on the National Institute of Standard and Technology’s (NIST)framework for improving critical infrastructure cybersecurity to promote security by design approach to device manufacturing. In 2017, FDA issued Design Consideration and premarket submission recommendation for interoperable medical device to address IoMT manufacturers complains on complexity of device architecture. All these efforts are to fortify mitigations on cybersecurity threats to IoMT.

The authors further explained that in 2019, NIST released ‘’IoT Device Cybersecurity Capability Core Baseline’’ as an agnostic and easily digestible guideline for device manufacturers, and in 2020 IoT Cybersecurity improvement Act was signed into law.

Thomasian & Adashi’s paper has depth analysis on regulatory bodies actions on improving mitigation strategies of cybersecurity threats of IoMT devices from architecture design to utilization of the device while articles from Chacko & Hayajneh emphasized only on FDA. Nevertheless, both papers focused on security of the device from manufactures responsibilities perceptive. There was no mention of General Data Protection Regulatory (GDPR) framework as one of primary objectives of protecting IoMT device is for patient data privacy.

**Conclusion and recommendation on the literature review**

The paper reviewed on potential cybersecurity threats and vulnerabilities of medical IoT and its impacts on healthcare sector stakeholders, possible mitigation mechanism and regulatory frameworks that aid securing of IoMT devices and patient’s data privacy. In the review I highlighted the fact that the integration of AI-tools such as ML and DL techniques in improving medical IoT cybersecurity seems more efficient considering the numerous advantages of AI technologies compared to core IoT cybersecurity counterparts. A further review on AI-based approaches for securing of IoT cybersecurity threats in healthcare sector, Potential AI-driven cyberthreats on medical IoT and Ethics in AI related cybersecurity of medical IoT are all recommended.

**References:**

* Altulaihn, E, Almaiah, A, &Aljughaimen, A (2022) MDPI. *Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions.*11(20)3330*.* Available from: [https://www.mdpi.com/2079-9292/11/20/3330[accessed](https://www.mdpi.com/2079-9292/11/20/3330%5baccessed) [Accessed 15 September 2024].
* Chacko, A, & Hayajneh, T. (2018). European Union Digital Library. *Security and Privacy Issues with IoT in Healthcare*. Available from: <https://eudl.eu/doi/10.4108/eai.13-7-2018.155079> [Accessed 13 September 2024].
* Gopalan, S, Raza, A, & Almobaideen, W, (2021). IEEE Xplore *.*2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA***)****. IoT Security in Healthcare using AI: A Survey.* Available from: <https://ieeexplore.ieee.org/document/9385711> [Accessed 9 September 2024].
* Hireche, R, Mansouri, H, & Pathan, A (2022*).* MDPI, Cybersecurities and Privacy*. Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis.*2(3)10. 3390.640-661. Available from: <https://www.mdpi.com/2624-800X/2/3/33> [Accessed 14 September 2024]
* Junaid.S, et al, (2022). National Library of Medicine*. PubMed Central. Recent Advancements in Emerging Technologies for Healthcare Management Systems*: A Survey.10(10):1940. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9601636/> [Accessed 8 September 2024].
* Lu. Y & Xu. L (2019). IEEE Xplore. *Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics*. 6(2) pg:2103-2115.Available from: <https://ieeexplore.ieee.org/abstract/document/8462745> [Accessed 10 September 2024].
* Messinis, S, Temenos, N, Protonotaris, N, Rallis, T, Kalogeras, D & Doulamis, N (2024). ELSEVIER. Computer in Biology and Medine. Enhancing *Internet of Medical Things security with artificial intelligence: A comprehensive review.* (170)108036. Available from: <https://www.sciencedirect.com/science/article/pii/S0010482524001203>[Accessed 15 September 2024].
* Nasiri.S, Sadoghi.F, Tadayon.M, & Afsaneh.Dl (2019). National Library Medicine. ACTA INFORMATICA MEDICA.Security *Requirements of Internet of Things-Based Healthcare System:* a Survey Study. 27(4):253-258, PCM7004290. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7004290/> [Accessed 8th September 2024].
* Nguyen.V and Yasin-Nur.A(2023). *Major Cybersecurity Threats in Healthcare During Covid-19 Pandemic.*
* Parihar.A, Prajapati.J, Prajapati.B. Trambadiya.B, Thakkar.A, &Engineer (2024). KeAi CHINESE ROOT GLOBAL IMPACT. Intelligent Pharmacy. *Role of IOT in healthcare: Applications, security & privacy concerns. Available* from: <https://www.sciencedirect.com/science/article/pii/S2949866X24000030#:~:text=Abstract,monitor%20over%20their%20medical%20condition.>[Accessed 15 September 2024).
* Rejeb.A, et al (2023). ScienceDirect. *The Internet of Things (IoT) in healthcare*: Taking stock and moving forward. Available from: <https://www.sciencedirect.com/science/article/pii/S2542660523000446> [Accessed 2 September 2024].
* Sadek.I, Codjo.J, Ul-Rehman.S & Abdulrak.B(2022). ELSEVIER. Computer Methods and Progress in Biomedicine Update. *Security and privacy on the internet of things healthcare systems: Toward a robust solution in real-life deployment. 2(100071). Available from:* <https://www.sciencedirect.com/science/article/pii/S2666990022000222>[Accessed 13 September 2024].
* Strielkina. A, et al (2018*).* EEE Xplore*. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment*. Available from: <https://ieeexplore.ieee.org/document/8409101> [Accessed 10 September 2024].
* Thomasian.N & Adashi.E(2021). ELSEVIER. Health Policy and Technology. *Cybersecurity in the Internet of Medical Things (10)100549*. Available from: <https://www.sciencedirect.com/science/article/pii/S2211883721000721> [Accessed 14 September 2024].
* Weir.C, et al (2023). IEEE Xplore.*A Lot Less Likely Than I Thought: Introducing Evidence-Based Security Risk Assessment for Healthcare Software.* Available from: <https://ieeexplore.ieee.org/document/10305607> [Accessed 8 September 2024].
* Yamaganti.R, Jyothi.N, & Manjari.S (2023). IEEE Xplore. The *Role of Internet of Things in Developing Competitive Healthcare Devices: A Case Study in the Digital Healthcare Industry*. Available from: <https://ieeexplore.ieee.org/document/10073802> [Accessed 3 September 2024).