E-Portfolio Activity unit 2: Literature Review Outline on topic- The role of cybersecurity threats to internet of things (IoT) in healthcare sector.

* **Introduction Statement:**

Advancement in technology is a continuous trend in today’s world and this is being experienced in healthcare sector. Junaid et al. (2022), stated that 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).

* **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).

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). 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. 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**

I would like to review the existing literatures on similar topics and identify the IoT cybersecurity vulnerabilities and threats. Also, analyse the shortcomings of the previous research and provide recommendation.

* **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 the mitigations techniques of IoT cybersecurity in healthcare?
* What are the regulatory frameworks to secure IoT cyberattacks in healthcare?
* **Research Methodology and Limitation:**

A qualitative review methodology will be 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.

* **Body of the literature review:**

**This be classified under the following headings which will be developed before the assignment is due for submission.**

* Cybersecurity threats and Vulnerabilities of IoT-devices in healthcare sector.
* Mitigation techniques on Cybersecurity-threats of IoT in Healthcare sector.
* Regulatory framework on Cybersecurity of IoMT
* **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. 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 will be recommended.

**References:**

* 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].
* 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].
* Nguyen.V and Yasin-Nur.A(2023). *Major Cybersecurity Threats in Healthcare During Covid-19 Pandemic.*
* 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].