RESEARCH METHODOLOGY PROPPOSAL PRESENTION TRANSCRIPT

[00:00:00] Njideka Ozoemena, and my research proposal presentation title is qualitative and quantitative analysis on the role of cyber security threats to Internet of things in a health sector and its mitigation. The module tutor is Dr. Steph Paladini.

[00:00:22] Content for the research paper is research background, significance of the research problem, research questions, research aim and objective, the preliminary literature review, research design and methodology, the ethical consideration and risk assessment, the research proposal timetable, and my reference.

[00:00:44] Research to understand the role of cyber security threats on Internet of things in a healthcare sector is crucial because the utilization rate of Internet of things technology is an upward trend and this come with cyber security threats challenge. This rapid growth in integration of Internet connected medical devices across healthcare systems have significantly posed cyber security risk on medical Internet of things devices.

[00:01:19] A further research have found that 82 percent of the healthcare companies have experienced Internet of things related cyber attacks (Landi, 2019). Such as bridge of patient's data, internet of things device operational downtime and reputational damages, et cetera, et cetera. Most of the literature or literatures on this topic focused on.

[00:01:47] Cyber security threat of Internet of things in a healthcare and its mitigations without covering the critical role of emerging technologies such as artificial intelligence, blockchain and machine learning in relation to cyber security threats on medical Internet of things devices. In this research, I will use both qualitative and quantitative methodology for a proper understanding of the role of cyber security threats in healthcare sector and its mitigation.

[00:02:22] This study is very important because the implication of Internet of Things is that Cybersecurity threat could lead to patient death, financial losses, and reputational damages. (Alghamdi,2022).

[00:02:41] Significance of the research problem. This study will address the role of cybersecurity threat on internet of things in a health system, its impacts solutions and possible future studies. The cyber security threats could be life threatening, or breach of patient data confidentiality due to unauthorized disclosure or access to information, or non availability of Internet of 18 devices and infrastructure because of denial-of-service attacks.

[00:03:11] We have other internal cyber security threats, (Thomasian & Adashi,2021). This study will contribute to the understanding of Internet of Things cyber security threats in healthcare, providing foundation for future research and strategic planning to safeguard sensitive healthcare information against cyber security threats.

[00:03:35] Aim and objective. The aim of this research is to assess the role of cybersecurity trait on internet of things in a healthcare sector and its mitigation, whereas the research objective is to identify various cybersecurity threats and vulnerabilities in the Internet of things in a healthcare sector and the consequence of cyber security threat, the literature on gaps in addressing the challenges.

[00:04:04] Finally, possible solution for mitigation. Research questions, these are questions that will guide me in my research, and they include what are the cyber security threats and vulnerability of medical Internet of things devices? What are the effects of these Internet of things devices cyber security threats on healthcare sector?

[00:04:30] What is the current trend of these challenges in the healthcare sector? What are the possible solutions to prevent or reduce this cyber attack on medical Internet of things devices? Are there any regulatory framework guiding cyber security threats of Internet of things devices in healthcare ecosystem? What is the future Internet of things cyber security threat in healthcare sector?

[00:05:01] Preliminary literature review. According to Ali (2023), internet of things devices in healthcare sector has created opportunities for remote monitoring, data collection, and diagnostics. This has contributed to operational efficiency in service delivery to patients. However, the technology has introduced vulnerabilities that could be exploited by cyber criminals with the integration of various connected devices like pacemakers, ventilators, and insulin pumps.

[00:05:35] Also, WATI (2024) classified internet of things devices are more the 10-cybersecurity trait in a healthcare sector? It is also a growing threat and on unsecured internet of things devices often lack robust security features and can easily be prone to cyber attack. To further bore stress this importance of understanding the role of cyber security threat in a health sector.

[00:06:05] (Thomasian & Adashi,2021) emphasize that some of these Internet of Medical Things cannot accommodate installation of agents or can be easily patched or even lack in built control attack, thereby posing increased cyber risk and using the Internet of things devices As the entry point into the entire hospital facility network system, all reviewed papers adequately outlined varieties of potential cybersecurity traits on internet of medical things, but non gave deep review on AI cybersecurity threats as is related to internet of medical things considering the current trend of AI technologies.

[00:07:00] Mitigation of the seminary literature review. I have their mitigation techniques on cybersecurity threats of Internet of things in the healthcare sector. Some of the mitigations of Internet of things and cybersecurity threats from my literature review are as follows. (Altulaihn, 2022), emphasize on end-to-end inscription.

[00:07:24] Use of multiple factor authentication and also access control on physical layer of internet of things architecture, protocol and software application updates and deployment of network filtering such as secure MQIT and ABE are algorithm. TCS (2023) also recommended a comprehensive risk assessment of Internet of things medical devices to identify potential vulnerability, it's impact on patient care and the regulatory implication of these breaches. Also, (Gopalan, 2021) recommended the use of AI tools to protect medical internet of things devices from cyber security threat considering AI is the most efficient medium to process big data and get real-time accurate results, such as use of cryptography and steganography to analyse and dictate any suspicious activity in data transmission network.

[00:08:39] New framework on Internet of Medical Devices Cybersecurity Threats. I have (Thomasian & Adashi,2021), Enumerated Various United State regulatory bodies that aid securing of medical internet of things from cybersecurity threats. Guidelines on protection of patient’s data privacy in terms of confidentiality, integrity, and availability of devices.

[00:09:05] The author stated that FDA leverages on the National Institute of Standards and Technologies NIST framework for improving critical infrastructure in cybersecurity. TCS (2023) also highlighted the regulatory bodies in Europe and United Kingdom. EU medical device regulation emphasizes on cyber security as a component of medical safety.

[00:09:35] While NHS in UK released device security guidelines which was updated in June 2022 post EU Britain on regulatory policy of medical Internet of things devices. My conclusion and recommendation on the literature review. The paper reviewed on potential cyber security threats and vulnerability of medical Internet of things.

[00:10:01] It's impact on healthcare sectors stakeholders’ possible mitigation mechanism and regulatory framework that edge securing of internet of medical team devices and patient data privacy. An AI based approach for securing of internet of cyber security threat in health sector, potential AI Driven Cybersecurity Threats on Medical Internet of things, Ethics in AI Related Cybersecurity of Medical Internet of things, are all recommended for further review.

[00:10:38] Research Design and methodology. The primary research method for this study is literature reviews. I will use both quantitative and qualitative methodology in analysing all the data collected through questionnaires and interviews from healthcare facilities, IOMT device manufacturers, and randomly picked patients.

[00:11:04] The following research statistic tools will be used for data collection analysis.

[00:11:09] 1. Descriptive statistics: here, a multiple dimension contagious table will be used to summarize and virtualize data Berenson (2020), such as categorizing and representing frequency occurrence of various identified cyber security attacks.

[00:11:30] 2. Inflation statistics this would be used to take the hypothesis from other literatures and draw conclusions, test data relationship, the correlation, and predict the data behaviours (Literature-cast unit 7).

[00:11:50] 3 basic principle of probability will be used to evaluate the likelihood of some cyber security threat happening. This will be represented on a histogram graphics. Every research proposal, there are ethical consideration and risk assessment that need to be done. I intend to fulfill the research ethical guidelines. In line with the principle stated by Enago Academy (2023). 1. Validity of research design. My research design should address my respective research questions.

[00:12:32] 2. Voluntary participation and informed consent. The participant must fully understand what they are going into and the potential risks and benefits. 3. Sampling. I need to ensure that the selected participants do not require any legal or ethical permission to conduct the search. Example, parental permission of any minor that is one of my participants.

[00:13:02] 4. Confidentiality. According to the Economic and Social Research Council, ESRC. Confidentiality of information supplied by participants and anonymity of any respondent must be respected.

[00:13:23] 5. Risk of harm. I must ensure that the participants are not exposed to any potential risk because of the research result.

[00:13:32] Example, physical, emotional, or psychological risk. The last one, research methodology. I intend to ensure that the appropriate methodologies are used to reflect the true position of the research result. Lastly, I need to reconfirm from University of Essex Policy whether it requires any ethical approval for my research methodologies because it involves human participation.

[00:14:08] The University of Essex Health and Safety assessment template as a guideline. 1. The social risks are disclosures that could affect participants in the community.

[00:14:19] 2. The legal risk activity that might lead to participants disclosing criminality activity to a researcher and each result to lawsuit or civil claim for competition.

[00:14:30] 3. Economics harm. Any financial harm to participant because of information disclosure.

[00:14:37] 4. The reputational risk. This is the reputational damage to any participant based on outcome of the research report. 5. The safety guideline risk. This is to ensure that safety of the young participant, vulnerable adults and no exploitation of the participant.

[00:14:54] 6. Health and safety risk. This is to ensure that the participant will not be either physically or psychologically harmed as a result of the research. This schedule is for 7 months. Stage 1. Meeting my supervisors to agree on particular research title. This ends by 5th November 2024.

[00:15:12] Stage 2. This is to start reading all the relevant papers on the research topic, compare contracts on various arguments, identify research problems and gaps.

[00:15:41] All these tasks ends by 15 December 2024. Stage 3. This is a research design planning around the choosing methodology which include both quantitative and qualitative methodologies. I will design my The hospital facility, the IMT device manufacturer, and randomly pick patient I need to liaise with University of Essex on my introductory letter to the corporate participants, I need to research for other relevant statistic from academic publication articles and nutrition. Finally, on sampling and data analysis methods to be used, which must complete by Jan 5th, 2025. Stage 4 is data collection, here . I will send out all the questionnaires and conduct interviews with the selected participants and it ends by 15th February.

[00:16:35] The data analysis of various data using Excel and graphics to be concluded, stage 6 is writing of the paper. I will put all the findings together, proofread it and send it out for my peers and academic mentors to review and feedback. I will clean up and send back for my supervisor to review and give me feedback.

[00:16:58] Then I will send a second review for my supervisor's comment. Finally, I will prepare the paper and submit for defense. My references which are inline with the guidelines. Thank you.

Reference

* Alghamdi.A(2022). IEEE Xplore. *Cybersecurity threats to Healthcare Sectors during Covid-19*. Available from : [https://ieeexplore.ieee.org/document/9711659[accessed](https://ieeexplore.ieee.org/document/9711659%5baccessed) [Accessed 29 September 2024].
* Ali,N,(2023).TSC. *Healthcare cyber security: IoT device security, FAQs and how to ensure patient safety*. Available from: [https://thesecuritycompany.com/the-insider/healthcare-cyber-security-iot-device-security-faqs-and-how-to-ensure-patient-safety/[accessed](https://thesecuritycompany.com/the-insider/healthcare-cyber-security-iot-device-security-faqs-and-how-to-ensure-patient-safety/%5baccessed) [Accessed 5 October 2024],
* Berenson,L.Levine,D.Szabat,K,& Stephen,D(2020*).Basic Business Statistics: Concepts and Applications.*14th.Harlow:Pearson*.Avaliable from:* [*https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=5731462*](https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=5731462) *[Accessed 5 October 2024]*
* Dr Steph Paladini (2024*)* MSc Lecurecast(unit 7*). Inferential Statistics and Hypothesis Testing.* RMPP\_PCOM7E,JULY, 2024.University of Essex
* Enago Academy (2023). *What Are the Ethical Considerations in Research Design?*.Available from: <https://www.enago.com/academy/what-are-the-ethical-considerations-in-research-design/> [Accessed 01 October 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].
* Landi,A.(2019). FIERCE Healthcare. *82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds* .Available from: <https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds> [Accessed 28 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 04 October 2024].
* TSC(2023). *Healthcare cyber security: IoT device security, FAQs and how to ensure patient safety.* Available from: [https://thesecuritycompany.com/the-insider/healthcare-cyber-security-iot-device-security-faqs-and-how-to-ensure-patient-safety/[accessed](https://thesecuritycompany.com/the-insider/healthcare-cyber-security-iot-device-security-faqs-and-how-to-ensure-patient-safety/%5baccessed) [Accessed 5 October 2024].
* Tuscano, A.&Joshi, S. (2023). IEEE Xplore. 2023 Somaiya International Conference on Technology and Information Management (SICTIM). *Significance of Cyber Security of IoT devices in the Healthcare Sector.* Available from: [https://ieeexplore.ieee.org/document/10104657/authors#authors](https://ieeexplore.ieee.org/document/10104657/authors) [Accessed 28 September 2024].
* University of Essex(nd). *Research risk assessment.*Available from: <https://www.essex.ac.uk/student/postgraduate-research/research-risk-assessment> [Accessed 01 October 2024].
* WATI Cyber security (2024). *Top 10 Cyber Security Threats in Healthcare.* Available from: [https://www.wati.com/top-10-cyber-security-threats-in-healthcare/#:~:text=Unsecured%20IoT%20Devices%3A%20A%20Growing,them%20easy%20targets%20for%20cyberattacks](https://www.wati.com/top-10-cyber-security-threats-in-healthcare/) [Accessed 6 October 2024].