Research Proposal Outline

Project Title:- Investigating the specific security vulnerabilities related to the human factor in IoT systems in Secondary Education

Introduction

Security is one of the primary challenges in the adoption of IoT in education, IoT devices can become vulnerable due to human errors such as using weak passwords and inadequate security practices. Furthermore, malicious actors can also take advantage of human behavior to obtain access to IoT devices by sending phishing email or developing fake websites that appear to be authentic instructional resources. This research aims to investigate IoT devices security and vulnerabilities in secondary education field which are related to human factors.

Significance/Contribution to the discipline/Research Problem.

This research will contribute to the expanding body of knowledge on IoT security in education. The findings of the study may be of interest to anyone concerned in education, security, and policymaking. The findings of this study can be used to improve security measures for IoT devices in secondary education.

Research Question

1. What are the specific security vulnerabilities related to the human factor in IoT systems in secondary education?
2. How do these human and behavioral factors impact the security of IoT devices used in secondary education?

Aims and Objectives

The fundamental aim of this study proposal is to investigate and comprehend the vulnerabilities caused by human and behavioral aspects in the context of IoT systems deployed in secondary school settings. This research’s objectives are to identify the human and behavioral elements that contribute to IoT vulnerabilities in secondary education, , assess their impact on security, and suggest measures for enhancement.

Key literature related to the project

Title	Author	Date
IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond	O'hearon et. al.	2021
Human factor, a critical weak point in the information security of an organization's Internet of things	Hughes-Lartey et. al.	2021
Human Factors in Cybersecurity: Risks and Impacts	Kadena & Gupi	2021
Human Factors in Cybersecurity: A Cross-Cultural Study on Trust.	Alhasan	2023
Understanding the Last Line of Defense: Human Response to Cybersecurity Events.	Rebensky et. al.	2021
Human Factor, Cyber Hygiene, Cyber-Physical Systems, and Industrial Control Systems in the Context of Cybersecurity.	Tuomala	2023
A Survey on Security Threats and Solutions in the Age of IoT	Ataç & Akleylek	2019
A Study of Threats, Vulnerabilities and Countermeasures: An IoT Perspective	Choudhary et. al.	2021
Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study	Davis et. al.	2020
A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices	Zhao et. al.	2022
Cyber Threat Intelligence for the Internet of Things.	Bou-Harb & Neshenko	2020

Computing Security Scores for IoT Device Vulnerabilities.	Rizvi et. al.	2019

Methodology/Development strategy/Research Design

An exploratory approach that collects a large amount of data before making precise conclusions is appropriate for researching the human factor's special vulnerabilities in IoT systems in the context of education.

Research methodology – Mixed:

As our research is requested to be secondary research, therefore, secondary data may be collected by studying research papers, industry reports, and previous news coverage and assessments of IoT-related incidents or data breaches. Analyzing publicly available IoT device data from manufacturers commonly used in educational institutions may also be incorporated.

Quantitative: Analyzing research papers, reports, and documents that include quantitative data on vulnerabilities, incidents, and breaches.

Qualitative: Analyzing qualitative sources such as literature, surveys, and case studies to get understanding about issues concerning the human factor in IoT systems security.

However, the real capstone project will include conducting surveys and interviews with teachers and IT experts based on the vulnerabilities identified from reviewed literature and available data sources to collect data about the IoT devices currently used and security incidents they have encountered.

Ethical considerations

1. Privacy Concern / Data Protection: The collection and examination of data concerning IoT vulnerabilities poses privacy concerns. For that reason, participants identities will be kept anonymous and confidential. as well as save them encrypted in secure storage for a short time.

2. Obtaining informed consent: Participants are provided pertinent information about the research, such as its aims, methods, and potential risks, so that they may make an educated decision about their participation.

Artefact

1. A comprehensive research report including the specific IoT vulnerabilities in secondary education which are related to human and behavior factors.
2. A guide detailing essential strategies and recommendations for addressing human and behavioral issues in IoT security in educational settings and improve IoT security may be established.

Timeline

- Literature review: (systematic literature review of academic research publications - Analyze industry reports - Investigate past news reports and analyses of IoT-related incidents or data breaches - Examine publicly available IoT device information from manufacturers commonly used in schools) = 2 months.
- Data collection: (surveys – interviews - case studies) = 2 months
- Data analysis: (Analyze the collected data) = 2 months
- Report writing: (comprehensive research report - summarizes the findings – recommendations) = 2 months
- Review and submission: (Review the research report – Submit) = 1 month

References

Alhasan, Isslam Yousef (2023) Human Factors in Cybersecurity: A Cross-Cultural Study on Trust. *Purdue University Graduate School*. DOI: https://doi.org/10.25394/PGS.23271581.V1.

Ataç, C., & Akleylek, S. (2019) A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology* : 36-42. DOI: https://doi.org/10.31590/ejosat.494066.

Bou-Harb, E., & Neshenko, N. (2020) Cyber Threat Intelligence for the Internet of Things. *Cham: Springer International Publishing*. DOI: https://doi.org/10.1007/978-3-030-45858-4.

Choudhary, Y., Umamaheswari, B., & Kumawat, V. (2021) A Study of Threats, Vulnerabilities and Countermeasures: An IoT Perspective. *Shanlax International Journal of Arts, Science and Humanities* 8(4): 39-45. DOI: https://doi.org/10.34293/sijash.v8i4.3583.

Davis, B. D., Mason, J. C., & Anwar, M. (2020) Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal* 7(10): 10102–10110. DOI: https://doi.org/10.1109/JIOT.2020.2983983.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021) Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* 7(3). DOI: https://doi.org/10.1016/j.heliyon.2021.e06522.

Kadena, E., & Gupi, M. (2021) Human Factors in Cybersecurity: Risks and Impacts. *Security science journal* 2(2): 51-64. DOI: https://doi.org/10.37458/ssj.2.2.3.

O'hearon, K., Mckee, M., Hossain, N., & Abdullah, C.M. (2021) IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond. Available from: https://www.researchgate.net/publication/354867275_IoT_Privacy_and_Security_in_Teaching_Institutions_Inside_The_Classroom_and_Beyond [Accessed 3 August 2023].

Rebensky, S., Carroll, M., Nakushian, A., Chaparro, M., & Prior, T. (2021) Understanding the Last Line of Defense: Human Response to Cybersecurity Events. *Cham: Springer International Publishing*. DOI: https://doi.org/10.1007/978-3-030-77392-2_23.

Rizvi, S., McIntyre, N., & Ryoo, J. (2019) Computing Security Scores for IoT Device Vulnerabilities. *In: 2019 International Conference on Software Security and Assurance (ICSSA). St. Pölten, Austria: IEEE.* DOI: https://doi.org/10.1109/ICSSA48308.2019.00014.

Tuomala, V. (2023) Human Factor, Cyber Hygiene, Cyber-Physical Systems, and Industrial Control Systems in the Context of Cybersecurity. fi=Ylempi AMK-opinnäytetyö|sv=Högre YHexamensarbete|en=Master's thesis| Available at: http://www.theseus.fi/handle/10024/798348. [Accessed 3 August 2023].

Zhao, B., Ji, S., Lee, W.-H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L., & Beyah, R. (2022) A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Transactions on Dependable and Secure Computing* 19(3):1826-1840. DOI: https://doi.org/10.1109/TDSC.2020.3037908.