**CYBERSECURITY THREATS IN IOT IN THE GOVERNMENT SECTOR**

**Student Name: [Your Full Name]  
Student ID: [Your Student ID]  
Module Name: Research Methods and Professional Practice  
Module Code: RMPP\_PCOM7E  
Instructor Name: [Instructor's Full Name]  
Date: [Submission Date]**

TABLE OF CONTENTS

[1. Unit 1 Discussion Forum (Peer Review and Response to Peers) 3](#_Toc210407118)

[2. e-Portfolio Activity 2: Research Methods and Data Collection for IoT Security 3](#_Toc210407119)

[3. e-Portfolio Activity 3: Ethical Issues and Professionalism in Securing IoT Devices in Government 4](#_Toc210407120)

[4. e-Portfolio Activity 8: Data Analysis and Findings on IoT Vulnerabilities 4](#_Toc210407121)

[5. e-Portfolio Activity 9: Conclusion and Reflection 5](#_Toc210407122)

[References 6](#_Toc210407123)

# Unit 1 Discussion Forum (Peer Review and Response to Peers)

In response to the other participants in the Unit 1 discussion board, I have read three posts, which proved to be informative regarding the topic of IoT security and ethical concerns. Peer X has stressed the need to balance transparency and privacy and stated that transparency is required, which can be against the requirement to keep personal information confidential. I agree with this view but would add that as encryption and privacy-sensitive technologies evolve, we will become able to achieve transparency without jeopardising security.

Peer Y did not ignore the necessity to set standards of regulation of IoT security within the governmental framework in a less complex manner. This resembles my study, in which such ethical standards as the Menlo Report are needed to regulate the use of IoT systems. I was stimulated by the concept of how AI could be abused within security systems, as Peer Z was concerned. Like the high-level security benefits of AI, ethical-related concerns, particularly those relating to accountability and control, also exist. My study supports the premise that AI tools may prove helpful in threat detection, but it should be done with a sharp consideration of the ethical dimension (Finn and Shilton, 2023).

# e-Portfolio Activity 2: Research Methods and Data Collection for IoT Security

The mixed methodology of this study of the risk of cybersecurity attacks on IoT in government is based on the mixed methodology. The qualitative aspect involves case studies and interviews with professionals to see the flaws of government IoT systems. Its quantitative component, consisting of surveys and statistical analysis, will be the extrapolation of the findings to other sectors of the government and estimations of the larger impact of IoT vulnerabilities on the service providers of the population (Saunders, Lewis, Thornhill, 2024). Nevertheless, the peer reviews throughout the Unit 1 discussions did influence my methodological decisions, specifically regarding the usefulness of including qualitative information in the general quantitative statistics. It will give a thorough understanding of the IoT vulnerabilities that may be overlooked with the help of a single method. According to Ermel et al. (2021), the two qualitative and quantitative methodologies support more concrete outcomes because the two research methods provide a versatile perspective on complex issues, which is critical when addressing cybersecurity dilemma in IoT systems.

The applied ethical approach is in accordance with the principles of informed consent, data anonymization, and data protection laws (Finn and Shilton, 2023). With such a mixed-method approach, I ensure that depth and generalization is achieved and the course learning outcomes of ethics in research and AI security are achieved.

# e-Portfolio Activity 3: Ethical Issues and Professionalism in Securing IoT Devices in Government

There is a significant ethical concern about the safety of the IoT devices in the government sectors, particularly in terms of the privacy of the data. States must find a compromise between the openness of the security practice and the right of citizens to privacy. The British Computer Society (BCS) and the Menlo Report Code of Conduct provide a list of how to ensure that IoT protection is done ethically, not infringing the right to privacy (BCS, 2018; Finn and Shleton, 2023).

Individually, breaches of data through IoT can ruin any trust and confidence of the individuals in the institutions of the government. Such violations may also expose sensitive data, which is a danger to national security. Rodrigues et al. (2024) show that social impacts of violations within the population and the business sector are not that different, and a robust legal framework based on ethics is required. Cybersecurity professionals must be highly professional to ensure that the IoT systems are deployed as per the ethical standards. Ethical training and professional codes of conduct is crucial to deciding on the side of IoT security and data protection. The peer reviews emphasised the importance of ethical principles of IoT security and how government officials have to navigate through the complex ethical landscape of maintaining the confidentiality of sensitive information.

# e-Portfolio Activity 8: Data Analysis and Findings on IoT Vulnerabilities

The most common points of weakness in IoT security were identified, including data encryption and authentication, by analysing the qualitative data in the form of expert interviews and case studies (Corrêa et al., 2023). Quantitative analysis of statistical tests of chi-square and regression revealed significant correlations between network vulnerabilities and security measures used based on quantitative data analysis. Breach can be detected and prevented with intelligent AI-based tools because they can be used to automate threat detection. Even though these tools can lead to improved security of IoT systems, new ethical concerns are introduced by the implementation of the tools. The aspect of autonomy in AI and the possibilities of biased decision-making would have to be discussed in a manner that these tools can be ethically applied to the government.

The results suggest that there is the necessity to develop tighter policies and regulatory tools that can be used to address the weaknesses identified. The deployment of AI technologies toward security progress should be professional and ethical practice, considering that this should not pose a threat to the privacy of individuals or the accountability of the government. The experience of communicating with other participants in the Unit 1 discussion board was helpful as it enabled me to understand the practical consequences of applying AI to the situation to Internet of Things (IoT) security and how that changes my understanding of the issue of technological advancement and responsibility.

**e-Portfolio Activity 9: Conclusion and Reflection**

The study reflects the enormous threat of cybersecurity challenges associated with IoT in government, especially data breaches and the possibility of hacking. Not only are these weaknesses that endanger national security, the people have their word to keep. The ethical decision-making process of securing the IoT systems is needed in order to address these threats and provide the safety of the citizens. In the future, I will investigate AI-based security systems further in terms of the ethical aspect of this technology. I also allege to become certified in cybersecurity so that I could expand my knowledge in securing the IoT systems and guarding the moral conduct within the same field. I can align my future objectives based on AI security and ethical applications of IoT technologies with the proposed research. Tasks that have been carried out in this e-Portfolio have also helped in gaining an additional knowledge of the ethical, legal and professional duties in the realm of security in IoT.

# References

BCS, 2018. *British Computer Society*. Bcs.org. Available at: <https://www.bcs.org/>.

Corrêa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N., 2023. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, *4*(10).

Dawson, C., 2015. Projects in Computing and Information Systems 3rd edn: A Student's Guide.

Ermel, J., Taylor, S., & Andersson, M., 2021. *Ethical Considerations in Scientific Research and Literature Review Methodology*. Journal of Applied Research in Technology, 22(3), pp. 45-68.

Finn, M. and Shilton, K., 2023. Ethics governance development: The case of the Menlo Report. *Social Studies of Science*, *53*(3), pp.315-340.

Rodrigues, G.A.P., Serrano, A.L.M., Vergara, G.F., Albuquerque, R.D.O. and Nze, G.D.A., 2024. Impact, compliance, and countermeasures in relation to data breaches in publicly traded US companies. *Future Internet*, *16*(6), p.201.

Saunders, M.N., Lewis, P. and Thornhill, A., 2024. Research Methods for Business Students.