**e-Portfolio**

**Cybersecurity Threats in IoT in the Government Sector**

**Module Title: Research Methods and Professional Practice**

**Table of Contents**

[1 Introduction 2](#_Toc211503781)

[2 Evidence of Learning and Application of Knowledge 2](#_Toc211503782)

[2.1 Literature Review Summary 2](#_Toc211503783)

[2.2 Research Methods and Proposal Evaluation 3](#_Toc211503784)

[2.3 Statistical Analysis (Units 8 and 9) 4](#_Toc211503785)

[3 Ethical and Professional Reflection Activities 6](#_Toc211503786)

[3.1 Ethics in AI and IoT Cybersecurity 6](#_Toc211503787)

[3.2 Data Misuse and IoT Parallels 6](#_Toc211503788)

[3.3 Application to Professional Practice 7](#_Toc211503789)

[4 Final Reflective Piece 7](#_Toc211503790)

[4.1 WHAT: My Learning Journey through Module 7](#_Toc211503791)

[4.2 SO WHAT: The Significance of My Learning 8](#_Toc211503792)

[4.3 NOW WHAT: Applying My Learning in Future Practice 9](#_Toc211503793)

[5 References 11](#_Toc211503794)

**Table of Figures**

[Figure 1: Task 8.2 Descriptive Statistics (source: self-made) 4](#_Toc211503763)

[Figure 2: Task 8.4 Differences by Batch (source: self-made) 5](#_Toc211503764)

[Figure 3: Unit 9 Chart Assessment (source: self-made) 5](#_Toc211503765)

# Introduction

The e-Portfolio reflects my learning experience on the topic of IoT cybersecurity in the government field, including its technical, ethical, and professional aspects. It shows how I used knowledge, independent research, and critical reflection acquired during the module. All the items in the portfolio are my literature review, reflective activities, and statistical exercises, and all these demonstrate my professional development in terms of analytical, ethical, and methodological skills. Collectively, these artefacts correspond to the learning outcomes of the module in research practice, data analysis, and professional integrity in computing.

# Evidence of Learning and Application of Knowledge

## Literature Review Summary

The Cybersecurity Threats in IoT in the Government Sector literature review discussed the interplay between the technological weaknesses, law, and ethics. It showed that the fast adoption of IoT in government infrastructures, including smart cities, military, and healthcare, has revolutionised the way the population receives their services and has created new security and privacy threats. Such typical technical vulnerabilities as weak authentication, default credentials, insecure firmware, and insufficient encryption are mentioned (Dawson, 2015). When utilised, these weaknesses may lead to serious violations, including distributed denial-of-service (DDoS) and ransomware attacks, that directly impact the national security and trust of the population (Park, 2020).

Regarding governance and ethics, the review revealed the fragmentation in the international and national regulatory frameworks, especially related to data protection and accountability (Corrêa et al., 2023). Ethical guidelines like the Menlo Report and the BCS Code of Conduct promote the ideas of justice, beneficence, and respect for persons, but these practices are not uniformly applied to the domain of the IoT in the context of the public sector (Finn and Shilton, 2023). Other researchers and journals, including BCS (2022) and Fjeld et al. (2020), also suggest that one of the ethical contradictions facing governments nowadays is the necessity to strike a balance between national security requirements and the civil liberties and the right to privacy of citizens.

In terms of methodology, the literature highlighted the shortcomings of existing research around IoT security. Most of the research is based on qualitative case studies, which offer good contextual insights, but they are not generalisable (Wohlin, 2021; Priya, 2021). On the other hand, quantitative researches tend to simplify socio-technical dynamics. The review emphasised the value of methodological pluralism and mixed methods following Saunders, Lewis, and Thornhill (2024) to enhance the validity and reduce the gap separating depth and generalisability. This realisation has informed my own thinking of the module process in terms of methodology, which has led me to understand that effective cybersecurity research is based on synthesising technical analysis, ethical contemplation, and systemic insights as opposed to isolating them.

## Research Methods and Proposal Evaluation

The research design concepts developed in Units 2 and 3 have greatly changed my perception of the research design, especially in writing the research proposal on Internet of Things cybersecurity in the government. First, technical vulnerabilities were more interesting. Nevertheless, the peer feedback process in discussion forums motivated me to take a wider approach that encompassed ethical, legal and professional aspects. This resulted in the integration of a mixed-methods design with qualitative interviewing and a case study with a quantitative survey and statistical analysis. The qualitative element was to collect the expert opinion on the vulnerabilities of the IoT and governance structures, whereas the quantitative element enabled to generalise of data in the sectors. Moreover, ethical implications inherent in my design, including informed consent, anonymisation, and adherence to the data protection legislation, proved that I have become more conscious of professional integrity and responsible data management (Finn and Shilton, 2023).

The feedback from tutors helped to affirm the clarity of the research design and alignment of the research questions with the available methods. To this, the proposal was modified so that every approach would respond to one of the four primary research questions of my literature review. This cyclic method has assisted me in shifting from a descriptive to a critical and reflective research attitude, with justification rather than assumption. It also enabled me to judge the validity, reliability and ethical consequences of methodological decisions better.

## Statistical Analysis (Units 8 and 9)

The statistical aspect of this module was created via the use of exercises in the form of Excel throughout Units 8 and 9, Tasks 8.1-8.6, A-F, and the Unit 9 Charts Assessment. These included data entry, cleaning, descriptive statistics, hypothesis testing and visualisation. The objective was mainly to learn how empirical data, which is related to cybersecurity research, can be recognised, correlated, and analysed using quantitative methods.

In the case of Task 8.2, as an example, the descriptive statistics were applied to compute the measures of central tendency (mean, median, mode) and dispersion (standard deviation) to aid in interpreting data consistency. Correlation and regression analyses were performed in Task 8.4 to evaluate the relationships among variables, including security investment and the frequency of incidents. These examinations have been useful in informing practice on the application of quantitative outcomes in policy recommendations that are evidence-based. The Unit 9 Charts Assessment also helped me to advance my data visualisation skills, which allowed me to better communicate the results.

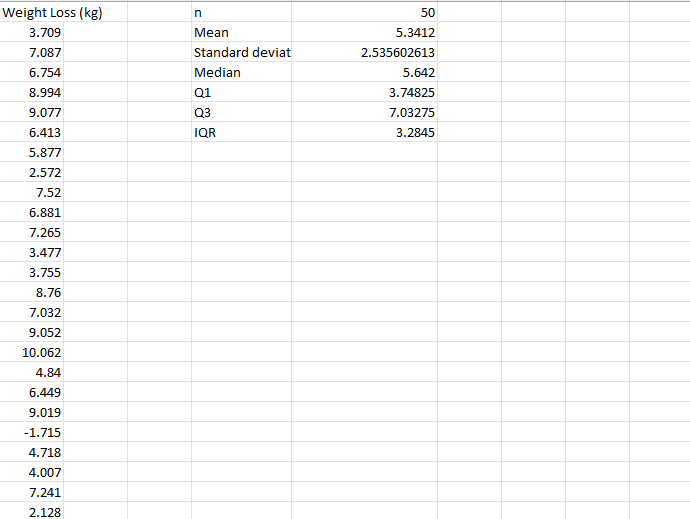


Figure 1: Task 8.2 Descriptive Statistics (source: self-made)

Figure 2: Task 8.4 Differences by Batch (source: self-made)

Figure 3: Unit 9 Chart Assessment (source: self-made)

By working on these exercises, data literacy and critical interpretation of statistical results were developed. It also strengthened the significance of accuracy, transparency, and reproducibility in research-values that are the focus in academic and professional practice. Through the correlation of the quantitative findings with qualitative findings of the reflection process and literature review, there acquired a balanced view of the issues of cybersecurity was acquired that unites the numerical analysis and the moral interpretation.

# **Ethical and Professional Reflection Activities**

## **Ethics in AI and IoT Cybersecurity**

Activity 1 discussed the overlap of ethical governance in Generative AI and IoT cybersecurity in government systems, and found that there are overlapping dilemmas in terms of privacy, accountability, and democratic values. They also got to know that although IoT technologies make smart cities more efficient and safer, they also put citizens at risk of mass surveillance and data abuse. This ethical fragmentation is further amplified by the lack of a set of international standards (Corrêa et al., 2023). Whether it is national security or civil liberties, the tension between them has never been fully resolved because intrusive monitoring can be facilitated by the same systems that are used to protect. The same issues can be observed in the case of AI governance, in which fairness and accountability are mostly abstract (Batool, Zowghi and Bano, 2025). The EU AI Act and GDPR are examples of legal frameworks designed to protect privacy, yet they tend to be a lagging force compared to technological progress. On a professional level, this reflection helped me realise the moral responsibility of IT professionals to ensure the balance between technical capability and the public interest in accordance with the BCS Code of Conduct, requiring the fairness, integrity, and respect of privacy.

## **Data Misuse and IoT Parallels**

Activity 2 investigated the Cambridge Analytica scandal, which provided similarities to the risks of privacy in IoT-based government infrastructures. They are similar in that they are both consent violations and data manipulation, which take advantage of knowledge and power asymmetries (Confessore, 2018; Jha and Jha, 2024). The Mirai Botnet attack also proved that ethical negligence can lead to the further development of the technical vulnerability (Carr, 2017). These examples made me understand that accountability, autonomy, and justice are the key aspects that any data-driven technologies should possess. I learnt that ethical awareness should focus on the proactive approach, that is, looking ahead and preventing harm instead of responding to it, and that responsible practice cannot be ensured by compliance alone.

## ****Application to Professional Practice****

The two reflections underlined the importance of ethical computing, which involves the incorporation of professional codes and moral reasoning. Some principles of justice, beneficence, and respect towards the public are given as the guiding principles in the BCS Code of Conduct (2022) and Menlo Report (Finn and Shilton, 2023). These now guide my practice, which encourages responsible innovation, transparency and ethical risk assessment. I will seek professional qualifications in cybersecurity and AI ethics to enhance my capacity to create secure, privacy-conscious technologies to balance innovation and integrity, justice, and trust of the people.

# ****Final Reflective Piece****

## ****WHAT: My Learning Journey through the Module****

Throughout this module, I got acquainted with the multi-layered environment of cybersecurity threats to the Internet of Things (IoT), especially in the government sector. The work with theoretical and practical studies allowed me to create a comprehensive picture of the intersection of technological innovation with ethical, legal, and professional requirements. At first, I had been more technical in my interests, focusing mostly on the vulnerabilities of the devices and system failures, but with time, I came to realise that it was more of a comprehensive approach that included ethical governance, responsible innovation, and social accountability. My initial significant accomplishment was the literature review, which has enhanced my knowledge of the dangers of bad encryption, default passwords, and poor firmware patches that jeopardise critical infrastructures like healthcare and defence. But I also learned that these vulnerabilities are also the result of disjointed administration and unstable moral principles. Research by Corrêa et al. (2023) and Fjeld et al. (2020) found that despite the existence of many AI and IoT ethical frameworks, not many are enforceable, which adds to the problem of how the lack of ethics directly leads to security threats.

My methodological skills were also improved in developing the research proposal. My early preference for quantitative methods was later changed to a mixed-methods design (expert interviews, case studies, and statistical analysis) upon peer and tutor advice. This method increases both depth and generalisability as proposed by Saunders, Lewis and Thornhill (2024). I also found out that good research is not only based on information but also on critical thinking, ethical consciousness, and openness. The statistical tasks in Units 8 and 9 helped me to develop the fundamental knowledge of using Excel for the application of descriptive statistics, correlations, and regression analysis. Through these activities, I learnt that quantitative data can be used to support qualitative data, which would help make balanced decisions.

Lastly, the reflective exercises related these technical and methodological lessons to ethical knowledge. Based on the case of the Cambridge Analytica scandal and the failure to regulate AI, it was evident that human choices are the most dangerous in terms of cybersecurity risks, primarily due to a lack of oversight, accountability, and neglect of moral principles. It has been an experience that has changed my identity as not a technical learner but a responsible professional who understands the societal impact of digital innovation.

## ****SO WHAT: The Significance of My Learning****

Reflectively, the module has transformed my perception of the concept of being a computing professional radically. Initially, my perception of cybersecurity was that of a completely technical profession that encompasses encryption, system protection, and vulnerability identification. However, I have gained the moral judgment, professional integrity, and interdisciplinary awareness, which are also essential to the effective practice of cybersecurity. The literature review allowed me to be aware of the importance of critical thinking and doubting premises. I also believed that such a framework as the GDPR ensured ethical compliance, but I also discovered that the most elaborate policies can only be symbolic and enforced without international cooperation. It is in accordance with the statement of Finn and Shleton (2023) that ethical frameworks must be actively controlled and responsible. The given observation also changed my assessment of the credibility of the research regarding methodological rigour and ethical transparency, rather than the authority to be published.

The composition of the mixed-method proposal improved my academic maturity. I also discovered that a combination of both qualitative and quantitative approaches is required in addressing real-life issues; methodological pluralism is a synthesis of qualitative and quantitative approaches. The dilemma of the professional field between efficiency and ethics also manifests itself in the fight over the accuracy of numbers and the interpretation of the situation.. This has enhanced my critical thinking and the criticality of justifying research design decisions. My data analysis activities have made me technically competent and confident in quantitative research. I was introduced to the idea of descriptive and inferential statistics, which can be used to establish the relationships that cannot be identified with the help of qualitative approaches. However, I also learned that data analysis is a scientific and ethical action- numbers must be perceived with moral consciousness to prevent concealing inequalities or biased policy results.

The moral reflection practices were also transformative. The IoT and the Cambridge Analytica scandal demonstrated the similarities in ethical manipulation between technology and psychology. These experiences have been based on the BCS Code of Conduct (2022) and Menlo Report (Finn and Shilton, 2023), and have taught me to embrace uncertainty as part of ethical thinking and that being a professional in the digital age requires the ability to accept complexity.

## ****NOW WHAT: Applying My Learning in Future Practice****

Reflectively, this module has given me a precise roadmap on how to grow professionally and apply ethics. The greatest shift in my attitude is the one that I am currently viewing cybersecurity as not only a defensive practice but also as a social duty based on ethical government. In my professional practice, I will apply the concept of responsible innovation to every project related to AI or IoT in the future. This involves ethical risk assessment, data minimisation, design and deployment transparency and accountability. This module has inspired me to seek professional accolades in Cybersecurity and AI Ethics, including Certified Information Systems Security Professional (CISSP) and BCS Foundation Certificate in Artificial Intelligence, to enhance my technical and ethical skills.

Mixed-methods approaches are the methods that I would implement in research. The quantitative information should be combined with the qualitative understanding, which guarantees not only the validity of the outcomes but also the social and ethical significance. I also hope to be able to contribute to the interdisciplinary research that would explore the way the technologies of the public sector can reconcile the national security goals with the civil liberties, with references to my technical and ethical education during this module. Personally, I have become more self-aware and reflective. I also know that reflection is not a retrospective process but an ongoing professional practice. Frequent critical self-evaluation will enable me to be accountable, enhance performance and adjust to the changing ethical issues in technology.

Finally, this module has assisted me in establishing what type of computing professional I would like to become, someone who upholds integrity instead of expediency, inclusivity instead of convenience, and ethical pro-activeness instead of reactivity. I have now understood that technological advancement should never be without morality. Through the application of the learned principles of transparency, justice, and respect for persons, I will strive to make a digital space that is not only safe but also reliable, fair, and human-oriented.

# ****References****

Ahmad, R. and Yunos, Z., 2012. The application of mixed method in developing a cyber terrorism framework. *Journal of Information Security*, *3*(3), pp.209-214.

Association for Computing Machinery (ACM), 2018. *ACM Code of Ethics and Professional Conduct*. Association for Computing Machinery. Available at: <https://www.acm.org/code-of-ethics>.

BCS, 2022. *BCS Code of Conduct | BCS*. www.bcs.org. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/.

BCS, 2023. *What are ethics in AI? | BCS*. www.bcs.org. Available at: <https://www.bcs.org/articles-opinion-and-research/what-are-ethics-in-ai/>.

Berenson, M., Levine, D., Szabat, K.A. and Krehbiel, T.C., 2012. Basic business statistics: Concepts and applications.

Biros, D., 2020. The challenges of new information technology on security, privacy and ethics. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2020*(2), p.1.

Carr, M., 2017. The Role of Transnational Expert Associations in Governing the Cybersecurity Risks of the Internet of Things.

Confessore, N., 2018. Cambridge Analytica and Facebook: the Scandal and the Fallout so Far. *The New York Times*. 4 Apr. Available at: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

Corrêa, N.K., Galvão, C.T. and Santos, J.W., 2023. Meet the authors: Nicholas Kluge Corrêa and Camila Trindade Galvão. *Patterns*, *4*(10).

Dawson, C.W., 2005. *Projects in computing and information systems: a student's guide*. Pearson Education.

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M.L., Herrera-Viedma, E. and Herrera, F., 2023. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, p.101896.

Duncan, R., 2020. What does ‘secure by design’actually mean?. *Network Security*, *2020*(8), pp.18-19.

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

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. and Srikumar, M., 2020. Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. *Berkman Klein Center Research Publication*, (2020-1).

ISACA, 2025. *2025 Volume 6 The New Triad of AI Governance Privacy Cybersecurity and Legal*. ISACA. Available at: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-6/the-new-triad-of-ai-governance-privacy-cybersecurity-and-legal>.

Jha, R.K. and Jha, M., 2024. Optimizing E-Government Cybersecurity through Artificial Intelligence Integration. *Journal of Trends in Computer Science and Smart Technology*, *6*(1), pp.67-87.

Mökander, J., Schuett, J., Kirk, H.R. and Floridi, L., 2024. Auditing large language models: a three-layered approach. *AI and Ethics*, *4*(4), pp.1085-1115.

Park, Y., 2020. Development and Evaluation of a Security Agent for Internet of Things.

Priya, A., 2021. Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application. *Sociological Bulletin*, *70*(1), pp.94-110.

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.

Wohlin, C., 2021. Case Study Research in Software Engineering—It is a Case, and it is a Study, but is it a Case Study?. *Information and Software Technology*, *133*, p.106514.

Yogar, B.N.A. and Sabarna, M.A.N., 2025. Bibliometric Analysis of Research Trends in Data Security and Privacy for E-Government Implementation in Indonesia. *Agile Governance and Innovation Measurement Journal*, *2*(1), pp.15-25.