Reflective Piece - Secure Systems Architecture

Student Name: *Pragadheesh Marimuthu*

Module: Secure Systems Architecture (October 2025)

Assessment 3: Reflective Piece

Word Count: *~623 (excluding references and captions)*

Reflection

Throughout the Secure Systems Architecture (October 2025) module, I engaged with a mixture of conceptual learning, modelling activities, coding tasks, seminars and collaborative discussions. Looking back across Units 1 to 6, I can see a clear progression in how my understanding of secure operating systems, distributed computing and system modelling developed. This reflection follows the Rolfe et al. (2001) structure.

Summary of Module Learning Outcomes

Across Units 1 to 6, the module strengthened my ability to identify operating-system risks, understand distributed-system behaviour and apply secure-design principles in practice. I learned to evaluate and refactor system components, build distributed prototypes and critically analyse system performance. The team-based tasks improved my virtual collaboration skills, while the coding and modelling activities helped me apply concepts such as reliability, traceability and structured security design.

WHAT - Description of the Experience

Unit 1 introduced OS foundations, processes, scheduling and their link to distributed systems. The Collaborative Discussion on UML vs SysML helped me understand how modelling languages shape engineering workflows.

Unit 2 expanded this into threat modelling and Python socket programming, giving me practical experience with client-server interactions that later informed my Assessment 2 prototype.

Unit 3 focused on SoS modelling and systems engineering. I proposed using Bhattacharjya's (2022) blockchain-enabled CPS/IoT case study because it aligned with SoS characteristics. The team agreed, and I drafted the document structure and produced the initial AD-tree in draw.io, which helped organise the group's work.

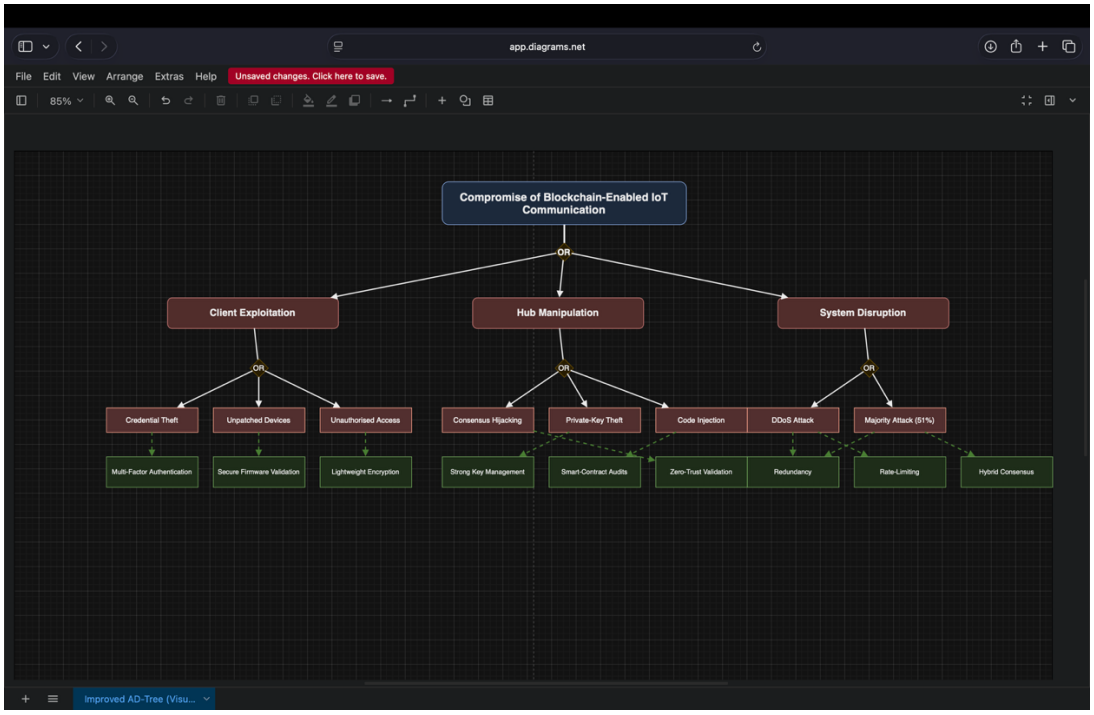
Units 4 and 5 emphasised QoS, the scientific method and teleological system design. These sessions shaped how I justified modelling choices and analysed distributed behaviour.

In Unit 6, I completed Assessment 2 by developing a Python prototype that simulated sensor behaviour under varying edge connectivity. I tested a Connectivity-based hypothesis from the ABCDE model, generated outputs, graphed the results and produced a detailed README explaining my analysis and conclusions.

Evidence of Work Completed:

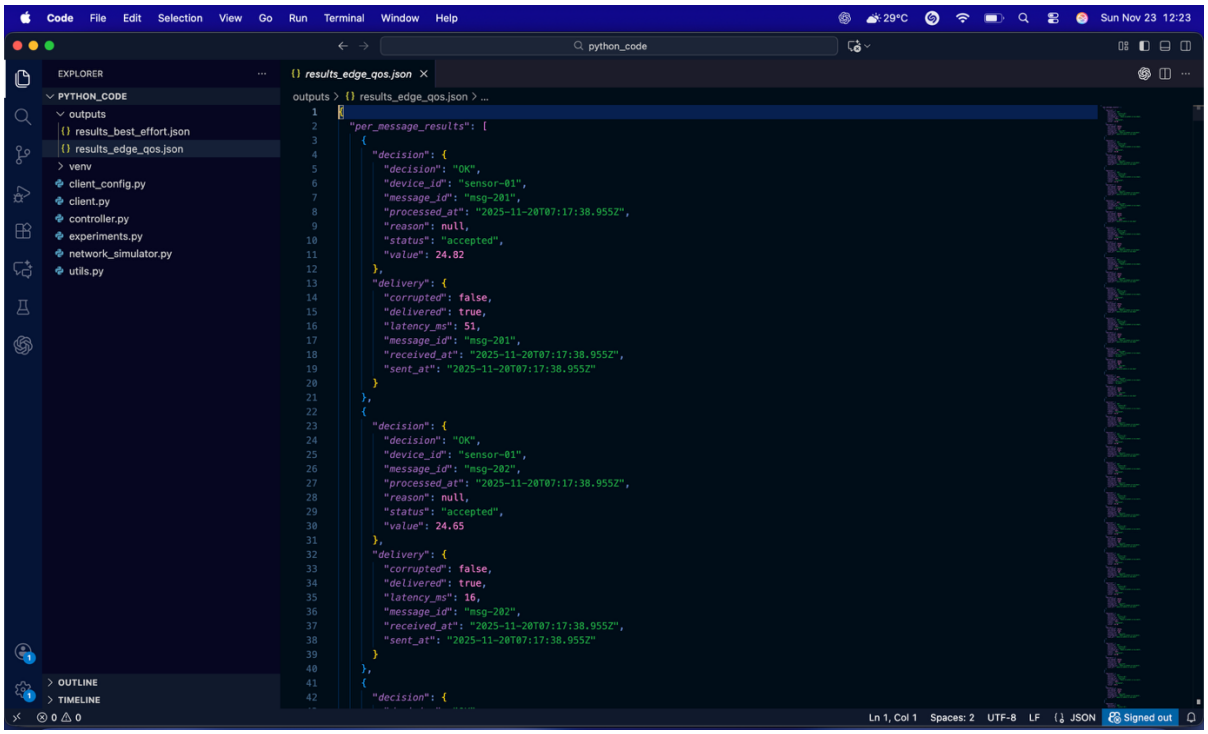
Screenshots below illustrate my contributions to the team design and individual prototype.

Figure 1. Attack–Defence Tree for Blockchain-Enabled IoT Communication



This figure shows my individual contribution to the team project: the initial AD-Tree I created in draw.io. It visualises the main attack paths, client exploitation, hub manipulation, and system disruption and the corresponding defence strategies relevant to the selected case study based on Bhattacharjya's (2022) blockchain-enabled CPS/IoT architecture.

Figure 2: Evidence of Individual Coding Contribution



View of my development environment in VS Code showing the generated results_edge_qos.json output created during my experiments for the individual project. This screenshot demonstrates my work on implementing the simulated distributed communication system and analysing QoS differences as part of Assessment 2.

SO WHAT - Analysis and Interpretation

Working with the same team from previous modules made collaboration smooth, and I felt comfortable contributing ideas. Although peer feedback was confidential, our communication reflected mutual trust. One key learning moment occurred when a teammate refined my initial AD-tree, reminding me that security modelling requires precision and correct notation—something reinforced in seminars that highlighted evidence-based and structured methodologies.

Tutor feedback on the team submission helped me refine my individual assessment. I focused more on clarity, modularity and traceability in the prototype. Seminar discussions on QoS and teleological design (Sáez et al., 2022) encouraged me to justify my implementation by linking system purpose to expected behaviour.

Emotionally, I progressed from early uncertainty with modelling tools to greater confidence after applying AD-modelling, socket programming and testing techniques. This growth improved my ability to analyse distributed architectures and think critically about system risk.

NOW WHAT - Learning, Actions and Professional Development

This module strengthened several areas of the professional skills matrix. Time management was essential while balancing two assessments in six weeks. Critical thinking improved as I analysed JSON outputs and compared connectivity scenarios. My IT and digital skills developed through building and debugging the distributed prototype. Research activities helped me justify modelling decisions, while teamwork reinforced constructive communication. Problem-solving improved through debugging interactions, and ethical awareness increased through modelling attack behaviour responsibly.

For future development, I aim to:

1. Improve precision in formal modelling notation.
2. Integrate more automated testing frameworks.
3. Support system-design decisions with deeper academic research.

Overall, the combined experience of team modelling, coding, seminars and discussions helped me meet the module's learning outcomes, particularly in identifying OS risks, designing distributed prototypes and evaluating secure system behaviours.

References

Bhattacharjya, A. (2022) 'A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication', *International Journal of Applied Mathematics and Computer Science*, 32(3), pp. 403-413.

Rolfe, G., Freshwater, D. and Jasper, M. (2001) *Critical Reflection in Nursing and the Helping Professions: A User's Guide*. Basingstoke: Palgrave Macmillan.

Sáez, A., Alonso, J. and García, C. (2022) 'A teleological approach to information system design', *Journal of Information Systems*, 36(1), pp. 12-25.

The University of Edinburgh *Reflection Toolkit*. Available at: https://www.ed.ac.uk (Accessed: 28 November 2025).