Project Number: P11

Project Title Intelligent Security Compliance Check for Critical Infrastructure – PoC Development

Project Clients: Dr Mohammad Goudarzi, School of Computer Science and Engineering

Project Specializations: Web Application Development, AI (Machine Learning, NLP), Security/Cyber Security

Background:

A fundamental step to building a secure and trustworthy system is ensuring that devices comply with security standards to protect users and the organisations that develop, manufacture, or operate these devices. Compliance with security standards is important for various reasons, such as protection against threats, interoperability, user trust, legal and regulatory requirements, risk mitigation, and cost reduction.

We are a group of researchers developing tools for compliance checking IoT and networking devices against essential security standards. We work with several industry partners in Australia, and this project involves implementing innovative solutions based on research conducted by the research team. This project is a practical example of leveraging the latest AI/ML techniques to address cybersecurity challenges.

Requirements and Scope:

The goal of this project is to develop a proof-of-concept tool for AI-based compliance checking techniques using machine learning and web-based dashboards.

In this project, students will develop an intelligent tool for compliance-checking devices against pre-defined security standards and rules. The tool requires a user-friendly web-based UI where users interact to write queries (prompts) and check the outcomes. The user queries should consist of the name of a device, security standard/standards, and security rules (e.g., encryption). At the backend, the tool uses machine learning to understand the user queries, rank the pre-defined standards based on the query, and determine whether the device complies with the standards. Also, the tool should suggest the required elements to be added to the device to comply with the designated security standard.

Further details will be discussed in the client meetings.

Required Knowledge and skills:

- Python programming (Advanced level)
- Machine Learning (NLP, APIs)
- User Interface (UI) design and implementation
- Web service development

Expected outcomes/deliverables:

- Source code
- Technical documentation including user guide.
- Prototype demonstration