Code	D11
Title	Cybersecurity Dashboard for Small Businesses
Supervisor	Alex
Description	This project involves creating an intuitive and user-friendly cybersecurity dashboard tailored for small businesses to monitor and improve their cybersecurity posture. Small businesses often lack the resources and expertise to manage complex cybersecurity tools, leaving them vulnerable to attacks. The proposed dashboard will provide an all-in-one solution with features such as vulnerability scanning to identify weaknesses in systems and networks, password management to enforce strong authentication practices, and real-time threat alerts to notify users of potential risks. The dashboard will also include visual analytics, such as graphs and heatmaps, to help users understand their security status at a glance. Additionally, it will offer actionable recommendations to address identified vulnerabilities and improve overall security. The project will focus on accessibility, ensuring the tool is easy to use for non-technical users, while providing robust protection against common cyber threats.
Required Skills and Expectation	Intermediate programming (Python or JavaScript), knowledge of web development frameworks, and understanding of cybersecurity best practices.

Code	D12
Title	Social Engineering Awareness Tool
Supervisor	Alex
Description	This project focuses on building an interactive tool designed to educate users about social engineering attacks, such as phishing, baiting, pretexting, and tailgating. Social engineering exploits human vulnerabilities rather than technical flaws, making awareness and education critical in cybersecurity. The tool will simulate real-world scenarios, allowing users to experience and identify common tactics used by attackers. For example, users may interact with simulated phishing emails, malicious websites, or baiting attempts, learning to recognize red flags and avoid falling victim. The tool will include quizzes, gamified learning modules, and detailed explanations of each attack type, along with actionable tips for prevention. Additionally, the project will emphasize user engagement by incorporating visual aids, interactive elements, and real-time feedback. By raising awareness and improving user vigilance, this tool aims to reduce the success rate of social engineering attacks and strengthen the human element of cybersecurity.
Required Skills and Expectation	Intermediate programming (Python or JavaScript), creativity in designing user interfaces, and understanding of social engineering techniques.

Code	D13
Title	Blockchain-Based Voting System
Supervisor	Alex
Description	This project aims to design and implement a blockchain-based voting system to ensure secure, transparent, and tamper-proof elections. The system will leverage blockchain technology to store votes in an immutable ledger, preventing tampering and ensuring the integrity of election results. Each vote will be cryptographically secured and linked to the blockchain, guaranteeing transparency while maintaining voter anonymity. The project will explore the use of smart contracts to automate vote validation, tallying, and result publication. Additionally, the system will incorporate mechanisms to prevent double voting, ensure voter authentication, and provide audit trails for election authorities. The research will address challenges such as scalability, privacy, and accessibility to make the system practical for large-scale elections. By combining cybersecurity principles with blockchain technology, this project contributes to the development of a secure and trustworthy voting system that can be used in democratic processes worldwide.
Required Skills and Expectation	Intermediate programming (Python or JavaScript), understanding of blockchain concepts, and familiarity with frameworks like Ethereum or Hyperledger.

Code	D14
Title	Mobile Application Security Testing Tool
Supervisor	Alex
Description	Build a tool to test the security of moThis project involves designing and developing a comprehensive tool to test the security of mobile applications. The tool will focus on identifying common vulnerabilities such as insecure data storage, weak encryption, improper API usage, and insecure communication protocols. It will automate the process of scanning mobile apps for security flaws, providing developers and security professionals with actionable insights to improve app security. The tool will include features such as static code analysis, dynamic runtime testing, and API endpoint validation. It will also provide detailed reports highlighting vulnerabilities, their severity, and recommendations for mitigation. The project will emphasize user-friendliness, enabling developers with limited cybersecurity expertise to easily test their apps. Additionally, the tool can include support for both Android and iOS platforms, making it versatile for modern mobile app development. This project contributes to improving mobile app security and protecting user data from potential threats.bile apps. The tool should identify vulnerabilities like insecure data storage, weak encryption, and improper API usage.
Required Skills and Expectation	Intermediate programming (Python or Java), knowledge of mobile app development, and familiarity with security testing tools.

Code	L11
Title	Smart Book Sharing Platform
Supervisor	Bell
Description	This project requires student to design an android app to build a book sharing platform. Here are the details of the platform. - show all available books - borrow books - donate books
Required Skills and Expectation	Android studio Java programming Google Books API

Code	L12
Title	FYP Matching System for Students and Teachers
Supervisor	Bell
Description	This project requires student to build an automatic fyp matching system for students and teachers. The system should support different types of users such as teachers, students, and admin. The system may includes three stages: 1. student self-proposing projects; 2. teacher proposing projects; 3. final matching result.
Required Skills and Expectation	Web development skills: MERN

Code	L13
Title	An Interactive Series-Game for Mastering Cisco Packet Tracer Commands
Supervisor	Bell
Description	This project is to help course ELEC S315F Routing and Switching Technologies to design a series of games based on Cisco Pakcet Tracer. All students of ELEC S315 are allowed to play the games together in the multi-user mode in packet tracer. These games are used for students to be familiar with Cisco Packet Tracer command.
Required Skills and Expectation	Cisco Packet Tracer passed ELEC S315F

Code	L14
Title	Advanced Network Scanner Using Nmap
Supervisor	Bell
Description	The advanced network scanner will utilize the Nmap scripting engine. The scanner will utilize custom or pre-existing Nmap scripts to automate complex tasks and gather detailed information about networked devices and services. It will support various scanning techniques, including host discovery, port scanning, service enumeration, and vulnerability detection.
Required Skills and Expectation	Wireshark or other phising packet softwares Nmap

Code	L15
Title	Cybersecurity Awareness APP
Supervisor	Bell
Description	The cybersecurity awareness app can help users stay safe from identity theft, phishing, cyberbullying, and privacy violations. It is an engaging platform for cybersecurity awareness training that instructs users on safe behaviors, different risks, and how to spot and handle phishing efforts. The aim is to assist in defending school officials, instructors, and students against data breaches and cyberattacks. Lessen the impact of cyberattacks and teach teachers and students how to recognize and react to threats.
Required Skills and Expectation	Web development skills: MERN or Android studio, Java programming

Code	F11
Title	Malware Detection Tool for Python Package / IDE plug-in
Supervisor	Farah
Description	(HKT project) Develop a tool that scans Python packages / IDE plug-in on PyPI for obfuscated code and known malware signatures. The tool could use static and dynamic analysis techniques to identify potentially harmful packages/plug-in before they are installed.
Required Skills and Expectation	Deliverables: Report + tool ; Required Skills: any programmimg language, Python preferred

Code	F12
Title	EDR evasion
Supervisor	Farah
Description	(HKT project) Create a comprehensive study and toolkit that demonstrates various EDR evasion techniques. This could include methods like process hollowing, fileless malware, and other advanced persistent threat (APT) tactics.
Required Skills and Expectation	Deliverable: Report + demo Required Skills: set up vm networks

Code	F13
Title	C2 Traffic Analysis
Supervisor	Farah
Description	(HKT project) Study and build a simulation environment that mimics C2 communication protocols, develop a tool that analyzes endpoint process and/or network traffic to identify and classify C2 communications.
Required Skills and Expectation	Deliverable: Report + tool Required Skills: set up vm networks,any programmimg language

Code	F14
Title	Comparative Study of Rootkit Detection Methods
Supervisor	Farah
Description	(HKT project) Build a simulation environment that mimics the behavior of different types of rootkits, conduct a comparative study of existing rootkit detection methods, evaluating their effectiveness, performance, and ease of use.
Required Skills and Expectation	Deliverable: Report + demo Required Skills: set up vm networks

Code	F15
Title	Car price tracking system
Supervisor	Farah
Description	The project is to track the car price and find a good deal. The functions of the system includes: 1)collect the car price information automatically from the Internet by using web-crawling technologies. 2) filter high, low and average price for specific car models in a time range; 3) alert the user when a price below average is posted on websites; 4) plot the price of each car model with manufacture year over time to analyse the decreasing speed of a particular model; 5) create multiple roles to access the system, i.e. system administrator; registered user; public.
Required Skills and Expectation	Deliverable: a complete web application

Code	H11
Title	Wi-Fi Deauthentication Attack Prevention System
Supervisor	Hugh
Description	This project develops a real-time system to detect and prevent WiFi deauthentication attacks, where attackers flood networks with deauth frames to disconnect users. The solution will sniff 802.11 management frames, identify anomalies in deauthentication traffic, and alert administrators. Countermeasures may include filtering spoofed MAC addresses, switching channels, or enforcing WPA3 management frame protection. This enhances reliability for environments requiring uninterrupted WiFi access (e.g., hospitals, offices).
Required Skills and Expectation	- Wireless networking fundamentals (802.11 protocols). - Programming (Python/Scapy, C++) for packet sniffing and anomaly detection. - WiFi security tools (Aircrack-ng, Wireshark, Kismet). - Hardware: WiFi adapters capable of monitor mode. - Knowledge of encryption (WPA2/WPA3, PMF). - Expected to build a prototype that detects & mitigates deauth attacks in real time with a dashboard.

Code	S11
Title	Developing penetration testing framework for property management infrastructure
Supervisor	Steven
Description	This is an industrial collaborative project with a property management company. Traditional penetration testing tools may not address tge unique infrastructure and security challenges faced by property management companies. Student is expected to create a testing framwork that covers both IT and OT (Operational Technology) systems.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good understanding on penetration testing methods Good communication with industrial partners

Code	S12
Title	Developing privacy-preserving tenant behavior analytics platform
Supervisor	Steven
Description	This is an industrial collaborative project with a property management company. Property managers want to understand tenant behaviour to improve services and detect security threats. Student is expected to develop analytics without compromising individual privacy.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good communication with industrial partners

Code	S13
Title	Promoting cybersecurity education to the public (or specific groups) to raise the awareness on protecting digital assets
Supervisor	Steven
Description	Online scams are very common in today's internet. Student is expected to review on the existing promotion on cybersecurity and state the possible solutions for solving this problem. Designing a material for cybersecurity education and promotion is a plus.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good graphic design is a plus

Code	S14
Title	Analyzing the pattern and freqency of online scams to raise the awareness on protecting digital assets
Supervisor	Steven
Description	Online scams are very common in today's internet. Student is expected to review on the existing literature and figures related to cybersecurity and suggest some possible hidden patterns (i.e. specific date, time, location etc.) of online scams that can raise the awareness on protecting digital assets.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good data analysis skills

Code	S15
Title	Analyzing the impact of network and link blockages on message transmission in complex networks
Supervisor	Steven
Description	Undestanding the effect on link blockage in tranmissing messages can be important in the digital world as the retranmission can be costly and time-consuming. We can simulate the network to understand how it affect the whole system. Student is expected to write a code to generate the networks and links to get the results by several computer simulations.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good mathematics is a plus

Code	S16
Title	Analyzing the impact of virus spread from infected computers in complex networks
Supervisor	Steven
Description	The virus spread between computers can be a disaster. To understand how it spreads, we can simulate the virus in complex networks. Student is expected to write a code to generate the networks and links to get the results by several computer simulations.
Required Skills and Expectation	Basic programming (e.g. python, R or C++) skills Good mathematics is a plus

Code	T11
Title	Security Monitoring System for Real-World Asset Transactions on the Blockchain
Supervisor	Tabitha
Description	This capstone project addresses the critical need for proactive security in the rapidly evolving domain of tokenized Real-World Assets (RWA). The core objective is to research, design, and develop a prototype for an automated monitoring system that safeguards RWA investment portfolios by identifying malicious and anomalous transaction patterns on the blockchain. The project begins with a comprehensive analysis of the unique threat landscape facing RWA, including potential attack vectors such as liquidity rug pulls, oracle manipulation, wallet drainers, and transactions with sanctioned entities. The student will then architect a system that interfaces directly with a blockchain node—using libraries like Web3.py—to stream and index transaction data for a set of monitored wallet addresses. The final deliverable will be a full-stack software prototype featuring a backend that performs the data ingestion and analysis, and a simple web-based dashboard (using a framework like Flask or Django) that provides a real-time visualization of portfolio health, transaction history, and critical security alerts. This project provides invaluable hands-on experience at the intersection of blockchain technology, cybersecurity operations, and data science, preparing the student for a career in fintech security.
Required Skills and Expectation	-Programming Languages: Python -Security Knowledge: Blockchain data analysis, anomaly detection principles, understanding of DeFi/RWA-specific threats -Tools & Libraries: Web3.py or ethers.js library for blockchain interaction, databases, b

Code	T12
Title	Blockchain-enabled Trustworthy Digital Twin Management System
Supervisor	Tabitha
Description	This project designs and implements a blockchain-based management system to ensure trustworthiness and security in digital twin operations. Students will develop a framework where industrial digital twins (e.g., smart manufacturing equipment or energy system replicas) are securely mapped to blockchain identities, creating immutable records of their operational states and historical data. The system will integrate IoT data streams with distributed ledger technology, implementing smart contracts to automate verification processes and maintain data integrity across the twin's lifecycle. Key components include cryptographic verification of twin data, decentralized access control mechanisms, and tamper-proof audit trails for all interactions and updates. The project will evaluate system performance through metrics such as data synchronization latency, consensus efficiency, and resilience against unauthorized modifications, providing a secure foundation for critical digital twin applications.
Required Skills and Expectation	-Programming Languages: Solidity/Python/JavaScript -Knowledge: Cryptography fundamentals; IoT communication protocols (MQTT/CoAP); Smart contract development; Distributed systems concepts.

Code	A11
Title	Cyberattack Impact on Smart Grid Control
Supervisor	Adam
Description	Simulate a simplified smart power grid control system (frequency control or dispatch control) and investigate how cyberattacks (such as false data or delayed signals) can cause incorrect operational decisions. This project reflects real-world Smart Grid cybersecurity challenges faced by power companies and energy providers, a growing field in critical infrastructure protection. Completing it gives you skills directly applicable to roles in energy systems engineering, critical infrastructure security, and control system analysis.
Required Skills and Expectation	Basic Python/Matlab programming, simple data plotting, interest in power systems, willingness to learn basic control concepts. Expected Deliverables: 1) Python simulation of a simple smart grid control loop. 2) 2–3 cyberattack test cases with comparison results. 3) technical report with graphs showing attack impact.

Code	A12
Title	Cybersecurity Monitoring for a Smart Factory Digital Twin
Supervisor	Adam
Description	Build a simple digital twin simulation of a smart manufacturing process (e.g., conveyor belt or packaging line) and apply an open-source Intrusion Detection System (IDS) to detect abnormal network commands caused by cyberattacks. This mirrors how Industry 4.0 factories secure their automated systems against hackers. Experience with this project is valued in manufacturing automation, industrial IoT security, and operational technology (OT) engineering roles.
Required Skills and Expectation	Basic Python/Matlab programming, curiosity to learn simple network concepts, basic use of software like Snort. Expected Deliverables: 1) Python-based digital twin simulation of a small manufacturing process. 2) IDS configuration to detect at least 2 simulated cyberattacks. 3) Demo showing normal vs attacked operation with IDS alerts.

Code	A13
Title	Anomaly Detection in Industrial Control System Data
Supervisor	Adam
Description	Create a simple Python program that simulates industrial control system data (temperature, motor speed, etc.), inject anomalies (attacks or faults), and use basic machine learning to detect these irregular patterns. This matches how industries use predictive maintenance and industrial cybersecurity to keep production safe, making it valuable for jobs in data analytics, industrial automation, and ML-assisted monitoring.
Required Skills and Expectation	Basic Python/Matlab programming, familiarity with handling CSV data, basic use of ML libraries. Expected Deliverables: 1) Python script generating normal and abnormal industrial data. 2) Simple ML or rule-based anomaly detection model. 3) Graph or table showing detected anomalies.

Code	A14
Title	Security Evaluation of AI-Powered Industrial Chatbots
Supervisor	Adam
Description	Develop a Python-based LLM chatbot assistant for industrial operations (smart factory troubleshooting or smart grid helpdesk) and test how it can be tricked into giving unsafe or confidential answers (prompt injection, data leakage). Then implement a basic safeguard to block malicious queries. This project links to the fast-growing field of AI safety and industrial AI applications, valued by employers working on AI integration and secure automation.
Required Skills and Expectation	Basic Python programming, interest in AI tools, willingness to learn simple text processing and testing methods. Expected Deliverables: 1) Working industrial-themed chatbot (using a small LLM). 2) 2–3 security attacks demonstrated and logged. 3) Simple defense mechanism and results summary.

Code	A15
Title	Cybersecurity Risk Demonstration for a Smart Healthcare Monitoring System
Supervisor	Adam
Description	Simulate a basic smart healthcare IoT monitoring system (e.g., wearable heart rate monitor sending patient data to a hospital server) and study how cyberattacks, such as data tampering or eavesdropping, could compromise patient safety. Implement a simple security enhancement (like data validation or lightweight encryption) and evaluate its effectiveness. This project reflects real risks in connected medical device security, which is a fast-growing area in healthcare IT, IoT security, and medical data protection. Employers in health tech, embedded systems, and cybersecurity value this knowledge.
Required Skills and Expectation	Basic Python programming, ability to plot simple data trends, interest in IoT or healthcare applications. Expected Deliverables: 1) Python script simulating patient vital data (heart rate, blood pressure, temperature) being sent to a "cloud server". 2) Demonstration of 1–2 simple attacks (false data injection, interception).

Code	Y11
Title	Deep Reinforcement Learning-Based Intelligent Traffic Light Control System
Supervisor	Yaru
Description	Deep Reinforcement Learning (DRL) technology revolutionizes traffic scenarios by offering intelligent solutions for optimizing traffic flow, reducing congestion, and enhancing safety on the roads. DRL algorithms can dynamically adjust traffic signals based on real-time conditions, improving traffic efficiency and reducing emissions. In this context, corresponding traffic light control plays a pivotal role, enabling adaptive signal timings that respond to changing traffic patterns and prioritize movements to minimize delays. Efficient traffic light control algorithms based on DRL facilitate multi-agent coordination, ensuring synchronized movements at intersections and continuous learning from traffic data for ongoing improvement in traffic management strategies. In this project, the student is expected to learn the principles of the Markov Decision Process (MDP) and DRL and apply them to the traffic light control system based on currencies. Both synthetic datasets and real datasets are expected to be used in simulations. References: [1] M. Zhu, X. Liu, S. Borst, A. Walid, “Deep Reinforcement Learning for Traffic Light Control in Intelligent Transportation Systems,” arxiv, pp. 1-17, Feb. 2023. [Online]. Available: https://arxiv.org/abs/2302.03669. [2] X. Liang, X. Du, G. Wang and Z. Han, “A Deep Reinforcement Learning Network for Traffic Light Cycle Control,” IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1243-1253, Feb. 2019. Methodology: 1) Understand the principles of MDP and DRL. 2) Define the state, action, and reward of the MDP based on the traffic light control scenario. 3) Utilize DRL algorithms to solve the proposed MDP with the synthetic or real dataset. 4) Analyze the performance and identify areas for improvement.
Required Skills and Expectation	Language or framework: TensorFlow, PyTorch, etc.

Code	Y12
Title	Reinforcement Learning-Based Intelligent Light Adjustment Design
Supervisor	Yaru
Description	With the development of smart home technology, traditional lighting control methods (such as manual switching and fixed brightness) have become difficult to meet the demands of "on-demand lighting" and "energy conservation and consumption reduction". This project aims to design and implement an intelligent lighting adjustment system based on Reinforcement Learning (RL). By simulating or perceiving environmental states (such as light intensity, human presence, and time periods), the system can independently learn the optimal brightness adjustment strategy. Minimize energy consumption while ensuring the user's lighting comfort. Methodology: (1) Understand the principles of RL; (2) Define the state, action, and reward based on the intelligent light brightness adaptive adjustment scenario. References: (1) OpenAI Gym: https://www.gymlibrary.dev/; (2) H. Ladhiya and R. Malik, "Reinforcement Learning based Smart Energy Management System for Indoor Lighting".
Required Skills and Expectation	Language or framework: Python, PyTorch, etc.