



اُونِيْوَرْسِيْتِي تِيْكْنُولُوْجِي مَارَا
UNIVERSITI
TEKNOLOGI
MARA

CSP760

*PREDICTING VULNERABILITY SUSCEPTIBILITY IN
MALAYSIAN BANK USING SUPERVISED MACHINE
LEARNING*

STUDENT

NOR ADANI BINTI KAMAL MOHAMAD NASIR (2024782087)

SUPERVISOR

DR SITI ARPAH BINTI AHMAD

Date: 19 October 2025



اُونِيُوَرْسِيْتِي تِيكْنُوْلُوْجِي مَآرَا
UNIVERSITI
TEKNOLOGI
MARA

TABLE OF CONTENT

1

UPDATE WEEK 2

2

CHAPTER 1

UPDATE WEEK 2

Item	Input	Process	Output / Expected Outcome	Status
1. Orange Data Mining Software	Orange Data Mining (Open-source ML tool)	-Installed and explored Orange Data Mining interface. - Familiarized with visual programming workflow (widgets, data input, preprocessing, model training). - Tested sample datasets to understand data flow.	- Software successfully installed and operational. - Clear understanding of Orange Data Mining functions for ML model training phase.	✔ Done
2. GitHub Setup	GitHub platform	- Created GitHub account dedicated to FYP project. - Set up initial repository for version control and code storage. - Configured structure for dataset, script, and documentation folders. - Planned future integration with Streamlit for deployment.	- GitHub repository ready for collaboration and version tracking. - Organized code management system for upcoming development stages.	✔ Done
3. Dataset Findings	- Open-source datasets (Kaggle, Tenable, CVE, ExploitDB) - Internal VA reports (in progress)	- Collected CVE dataset (✔). - ExploitDB dataset collection ongoing. - Internal / historical data extraction in progress.	- CVE dataset ready for use. - Comprehensive dataset to be finalized after integrating all sources.	⚙ In Progress
4. Data Pre-processing & Cleaning	Raw dataset (Kaggle, Tenable, CVE, ExploitDB)	- Started cleaning raw data (handling missing values, duplicates, data type normalization). - Began preliminary Exploratory Data Analysis (EDA) using Orange. - Feature identification for model training (Plugin ID, Severity, CVSS, CVE, Family).	- Clean dataset under development. - Early data insights and visualization obtained.	⚙ In Progress
5. Report Update (Chapter 3 Revision)	Supervisor’s feedback	- Revised Chapter 3 based on comments. - Moved theoretical explanation to Chapter 2. - Reorganized methodology to emphasize step-by-step process and tools.	- Updated report aligned with supervisor’s feedback. - Improved chapter structure and clarity of methodology section.	⚙ In Progress

INTRODUCTION

Cyber threats are rising rapidly in Malaysia’s banking sector. Banks rely on Vulnerability Assessment (VA) tools, which only detect existing issues and not the future ones. This reactive approach leaves banks unprepared for new attack patterns. To address this, Machine Learning (ML) can analyze past VA data to predict potential vulnerabilities and improve threat mitigation. This study aims to use ML to make cybersecurity in Malaysian banks more proactive and predictive.

RESEARCH QUESTIONS

- What are the limitations of current VA tools in predicting future attacks?
- Can ML models improve how banks prioritize and fix vulnerabilities by forecasting attack trends?
- How effective is the ML-based model compared to traditional VA methods?

HYPOTHESIS

This study proposes that machine learning can enhance the predictive capability of vulnerability assessment in Malaysian banks.

RESEARCH OBJECTIVES

- Design an ML model to predict cyberattack susceptibility using VA data.
- Develop and test the ML system for predicting future vulnerabilities.
- Evaluate the model’s accuracy and effectiveness in forecasting potential attack

PROBLEM STATEMENT

- Current vulnerability assessment (VA) tools in Malaysian banks identify existing vulnerabilities but fail to provide predictive insights into future attack trends (Hanif et al., 2021), leaving organizations reactive rather than proactive in managing security risks (Gencer & Başçiftçi, 2021).
- Manual analysis of large-scale VA results is time-consuming, error-prone, and inefficient (Esposito & Falessi, 2024), hindering the ability to prioritize critical vulnerabilities effectively (He et al., 2024).
- The rapidly evolving nature of cyber threats needs an intelligent system such as, AI-driven system to predict potential attack vectors and mitigate risks before exploitation occurs (Zacharis et al., 2024).

RESEARCH SCOPE

1. Uses Supervised ML models:
 - a. Random Forest (Classification)
 - b. Neural Network Regression (Prediction)
2. Data sources: Kaggle and Tenable datasets.
3. Key attributes: Plugin ID, Severity, CVSS, Findings, CVE, Asset Type, Family.

SIGNIFICANCE OF STUDY

1. Knowledge Contribution
 - Fills research gaps in predictive cybersecurity for Malaysian banks.
 - Shifts from reactive to proactive threat management.
2. AI-Based Predictive Model
 - Reduces manual effort and time.
 - Enhances vulnerability prioritization efficiency.
3. Industry Impact
 - Strengthens financial institutions’ cybersecurity posture.
 - Promotes adoption of Industry 4.0 and AI innovation.
4. Proactive Risk Management
 - Enables early identification of potential attack vectors.
 - Supports continuous improvement in risk remediation.



اُونِيُوَرْسِيْتِي تِكْنُوْلُوْجِي مَآرَا
UNIVERSITI
TEKNOLOGI
MARA

CSP760

THANK YOU