BİRUNİ
ÜNİVERSİTESİ
"Bilimin Geleceği"

Department of Computer Engineering
CMP402 Graduation Project Proposal Form

Advisor : Prof.Dr. Güray YILMAZ

Academic Year : 2025 - 2026 Semester: Fall ☐ Spring ☒

	Student No :	Name & Surname :	E-mail Address :	Signature :
1. Student:	210408017	Emir Kayra Bacak	210408017@st.biruni.edu.tr	

PROJECT TITLE: AI-Based Anomaly Detection in Network Traffic Using PCAP Data

DESCRIPTION: The aim of this project is to develop a machine learning–based intrusion detection system (IDS) capable of identifying anomalous network behaviors using features extracted from PCAP-based datasets. The project focuses on analyzing network traffic data, applying feature engineering techniques, and building classification models to distinguish between normal and malicious activities.

In the first stage, a supervised learning pipeline will be implemented using datasets such as CIC-IDS2017, employing algorithms like Random Forest and XGBoost to achieve high detection accuracy.

In the second stage, a simplified agent-based layer will be designed to simulate an autonomous decision mechanism. This "observer agent" monitors real-time predictions from the model and triggers preventive actions when anomaly probabilities exceed a certain threshold.

Although the system will not employ reinforcement learning at this stage, it lays the groundwork for a future adaptive defense mechanism where agents dynamically learn optimal responses to cyber threats through reinforcement learning methods.

Keywords: Artificial Intelligence, Machine Learning, Cybersecurity, Network Traffic, Anomaly Detection, Explainable AI

Requirements: Python, pandas, scikit-learn, XGBoost, SHAP, PCAP analysis knowledge

RECOMMENDED RESOURCES:

- ✓ Moustafa, N. & Slay, J. (2015). *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set).* Military Communications and Information Systems Conference (MilCIS), IEEE, pp. 1–6.
- ✓ Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). *A Survey of Network-based Intrusion Detection Data Sets.* Computers & Security, 86, pp. 147–167..
- ✓ Yuan, C. And Moghaddam, M.(2020).*Garment Design with Generative Adversarial Networks,* Academic Press, San Diego
- ✓ Xiao, Y., Xing, C., Zhang, T., & Zhao, Z. (2019). An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access, 7, pp. 42210–42219.
- ✓ Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A Deep Learning Approach to Network Intrusion Detection.* IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), pp. 41–50.

Project Advisor Prof. Dr. Güray YILMAZ	Head of Department Prof.Dr. Güray YILMAZ