University of Essex

Essex Futures BT– Masters Scholarship 2026-27

Project information: Protecting network from zero-day attacks in real-time using transparent machine learning.

Machine learning (ML) techniques have been increasingly used to enhance IDS capabilities. Unlike traditional signature-based IDSs, ML-based approaches can autonomously detect attack patterns. However, conventional ML models, including support vector machines and decision trees, face challenges in handling large-scale, complex cyber-attack problems. Deep learning (DL)-based IDSs offer improved detection capabilities but suffer from interpretability issues and require extensive retraining when faced with novel attack patterns.
This project aims to develop a self-improving, transparent IDS that integrates explainable machine learning techniques to enhance cybersecurity. The proposed IDS will continuously learn from labelled and unlabelled network traffic data to adapt to evolving threats, particularly zero-day attacks. An integrated Intelligent Incident Handling System (IIHS) will autonomously analyse identified threats and execute appropriate responses, ensuring real-time protection of network operations.

Objectives:
1. Extract measurable characteristics from network activities to model network and device behaviours.
2. Develop transparent machine learning models for real-time global and local network behaviour analysis.
3. Integrate multiple models into a unified IDS to detect malicious activities and compromised components.
4. Implement an IIHS to autonomously analyse and respond to identified threats.

Approach:
The project will employ a prototype-based learning framework to construct explainable predictive models that continuously refine their knowledge base. These models will monitor network states, detect anomalies, and execute responses to identified threats. Unlike black-box deep learning approaches, this transparent system will allow human experts to inspect, modify, and intervene in the decision-making process, ensuring greater control and trust in cybersecurity defence.

By addressing key challenges such as label scarcity, zero-day attacks, concept drift, and explainability, this project will contribute to the development of next-generation IDSs capable of real-time, adaptive,

and interpretable intrusion detection.

Use cases:
The developed IDS is relevant to attacks on BT Home Hubs