CHAPTER I
INTRODUCTION

This chapter offers a concise summary of the study, divided into six sections. It begins with an overview of the background, followed by the identification of the problem and the study objectives, the scope of work, the methodology employed, and the structure of the thesis. A more detailed explanation will be provided in the subsequent chapter.

1.1 Background

With the rapid advancement of network technologies, followed by the increasing dependence on the internet for healthcare [1], business [2], communication [3], and infrastructure [4]. Cybersecurity threats have become more sophisticated, ranging from brute force attacks to widespread distributed denial-of-service (DDoS) attacks, these threats have the potential to compromise individuals' data and even cripple organizations and government bodies [5]. It is important to think of a network as an ever-expanding spider web, which opens up great potential for network security to become increasingly difficult for humans to manage and mitigate. Nevertheless, Intrusion Detection System (IDS) have become a bulwark in defending against these threats. IDS play a crucial role in safeguarding networks by defensively monitoring network traffic and analyzing it to detect suspicious activities and other potential policy violations, as can be seen in the illustrasion in Figure 1.1.

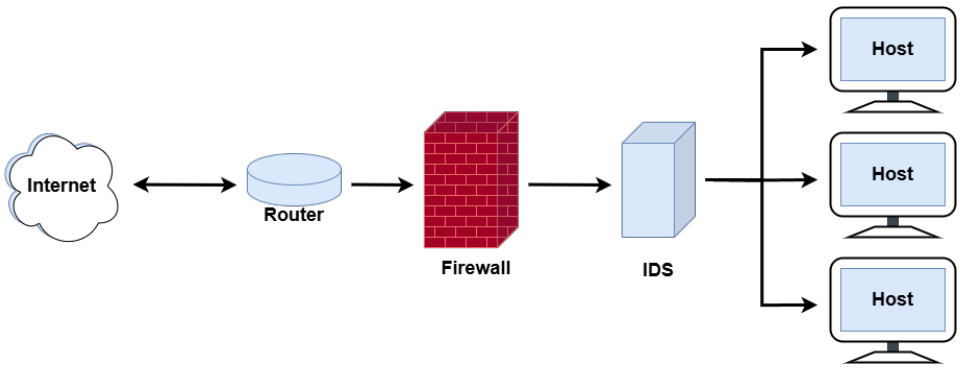

Figure 1.1 Intrusion Detection System

IDS can identify various types of attacks, such as unauthorized access, malware, and other unusual behaviors that may signal an attack and violate the information

security policies [6]. By alerting administrators, IDS provides an additional layer of security, allowing for a timely response aimed at mitigating risks before they escalate.

As cyber threats continue to evolve in complexity and scale, traditional IDS face limitations in effectively identifying novel or subtle attacks with already known signatures of attacks. This has led to the integration of Machine Learning (ML) and Deep Learning (DL) techniques into IDS, offering a more dynamic and adaptive approach to threat detection. By leveraging vast amounts of network data, ML-based and DL-based IDS can recognize patterns of normal and abnormal behavior, enabling them to identify previously unidentifiable threats that traditional signature-based systems might miss. These advanced systems can improve detection accuracy and reduce false positives, making them indispensable in modern cybersecurity defense frameworks. Table 1.1 will show the detailed view of a handful of studies regarding IDS and generalization.

Table 1.1 The Current State of IDS Studies

Citation	Model							Dataset	Year
	DT	SVM	RF	NB	CNN	DNN	LSTM		
Ashiku [7]					✓			UNSW-NB15	2021
Abed [8]					✓			UNSW-NB15, WSN-DS	2024
Azizjon [9]					✓			UNSW-NB15	2020
Ozdogan [10]	✓	✓	✓					NSL-KDD, KDD CUP99, MQTT-IoT-IDS2020	2024
Sudyana [11]					✓			CREMEv1, CREMEv2, CIC-IDS-2018, CIC-IDS-2017, CICIoT2023, IoT-ID20, UNSW-NB15	2024
Ravi [12]					✓		✓	KISTI, KDD CUP99, UNSW-NB15, CIC-IDS-2017, WSN-DS	2024
Biswas [13]	✓		✓	✓				CIC-IDS-2017, CIC-IDS-2018, NSL-KDD,UNSW-NB15, UNSB,2021 Bot-IoT	2024
Park [14]					✓	✓	✓	NSL-KDD, UNSW-NB15, IoT-23, Private Network Capture	2023
Kim [15]					✓			KDD CUP99, CIC-IDS-2018	2020
Shaaban [16]					✓			Computer Simulated, NSL-KDD	2019
Aksu [17]	✓	✓		✓	✓	✓		CIC-IDS-2017	2018
Salmi [18]					✓		✓	Computer Simulated	2022

Many studies have been conducted to create an ML-based or DL-based IDS, these studies shows promising results but only few have seen real-world implementation. All studies about AI-based IDS uses a range of methods and models, there are ML-based IDS model created using Support Vector Machines (SVM) [10, 19, 20], which is the most common method due to its high efficiency [21], Decision Tree (DT) [22–24], and Naive Bayes [13, 25] just to name a few. Most of this studies also uses multiple methods to perform an analysis between models. On the other hand, DL-based method doesn't have the same ammount of variety as ML-based, many models are created using Convolutional Neural Networks (CNN) [7–9, 11, 12, 14–16, 18, 26, 27] with other variety. Many of these models shows flying results, but only some address model generalization [11, 28] by train-

ing and testing on different datasets. This study will implement a novel method by leveraging TabNet transformer to create a model able to withstand multiple unknown datasets, simulating real-world network scenarios.

1.2 Problem Identification

The current studies surrounding DL-based IDS revolves around CNN as their main model, this proved to be inefficient due to the ironic 'intrusive' preprocessing of datasets to represent itself as an 'image' for the model to work correctly. Raw network datasets are typically stored as a tabular form, making TabNet a model to natively support this data form with minimal preprocessing unlike studies that uses CNN as their base model. Figure 1.2 illustrate the problems that can be found within many studies revolving DL-based IDS.

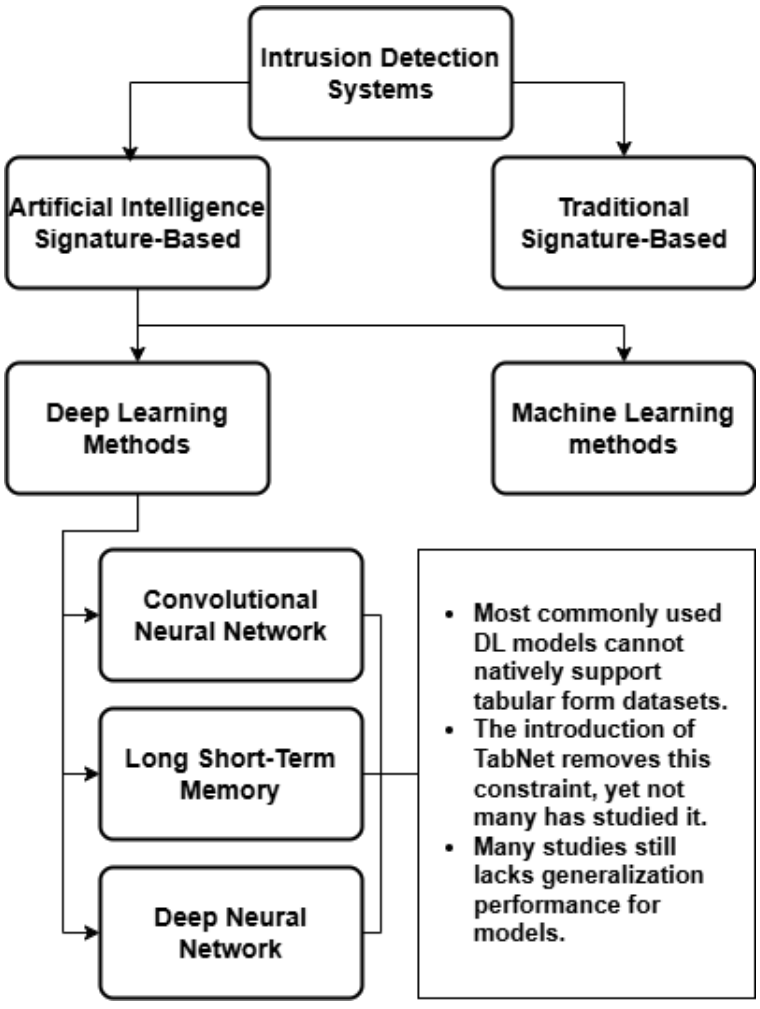

Figure 1.2 Problem of Recent Studies

To summarize, here are the main problems of this study:

1. **High False Positive Rates in Detecting Network Anomalies:** One of the key challanges in IDS is the high rate of false positives, this problem presents itself in both traditional and AI-based IDS. This is also the reasoning behind the lack of implementation for IDS models, one key reason of high false positive rate is that many IDS models cannot detect unseen pattern [29].A more refined model is needed to reduce this number.

2. **Imbalanced Dataset and Mismatched DL Models:** Many ML-based or DL-based IDS uses public datasets that have imbalance proportion of cyber attacks. This leads to many models struggle to detect less common type of attacks [30]. Not only that, many studies uses CNN as its base model which conceptually cannot support IDS datasets.

3. **Lack of Generalization Across Different Network Environments:** Many existing models from prior works lack the ability to generalize well across different network environments [28], meaning they will perform well on specific dataset but struggle when applied to unseen data.

1.3 Objective and Contributions

Based on the problems found within previous studies, this study whishes to address them by making them the main objective. Here are the key-points of this studies objectives:

1. **Enhanced Detection of Rare Cyberattacks:** By leveraging TabNet's native tabular learning capabilities, this study aims to improve detection of rare type cyber attacks, this can be achieved through proper balancing of imbalance dataset.

2. **Reduction of False Positives:** This study will implement a new novel technique to refine detection. By leveraging TabNet with Optuna as a hyperparameter tuning algorithm to efficiently search for the best parameters for each datasets.

3. **Improved Generalization Across Diverse Environments:** Focusing on the generalization of the model, this study will contribute to developing IDS that perform better in diverse network conditions, ensuring consistant performance in real-world scenarios.

1.4 Scope of Work

This study will focus on the following areas within the field of DL-based IDS:

1. **Dataset Selection and Preparation:** Four datasets will be employed on this study, the four dataset will be grouped into two sets of dataset. The first, an 'impact-based' dataset is consisted of CIC-IDS-2017 and CIC-IDS-2018. The second set is a 'lifecycle-based' dataset, consisted of CREMEv1 and CREMEv2.

2. **Implementation of Algorithms:** The TabNet architecture will be deployed for each datasets, it will train and test each datasets thoroughly by doing a cross validation within and outside the training dataset. For example, a model trained on CIC-IDS-2017 will be tested against it self, and also against CIC-IDS-2018. Other than that, XGBoost boost will also be employed as a baseline model to grade TabNet's overall performance.

3. **Performance Analysis:** A throughout analysis of both metric performance for detection and generalization will be conducted to better understand the model created. This study will create two models for each scenarios. One model for multiclass classification, and one for binary classification. Every model will be tested also for generalization across dataset.

1.5 Research Methodology

- **WP 1: Literature Review**
  This work package involves a comprehensive review of existing study on IDS. It will also explore recent advancements in deep learning, specifically TabNet. The objective is to identify gaps in current approaches and position the study within the existing body of knowledge.

- **WP 2: Data Collection and Preprocessing**
  This work package involves identifying and selecting relevant datasets, focusing on those with a mix of normal and malicious traffic. The datasets should also represent imbalanced class distributions to simulate real-world network conditions. The tasks will include cleaning, normalizing, and encoding the data to prepare it for the TabNet model. Additionally, feature engineering will be performed to optimize the input for the model.

- **WP 3: TabNet Model Development**
  In this work package, the implementation of the TabNet model for IDS will

be undertaken. The model will be tailored specifically for detecting rare and sophisticated cyberattacks.

- **WP 4: Model Evaluation and Performance Analysis**
  This work package focuses on evaluating the performance of the TabNet model using various metrics. Additionally, the generalization capabilities of the model across different datasets will be tested.

1.6 Research Plan and Action Point

This study is planning to follow the action points describe in table 1.2 down below:

Table 1.2 Monthly Action Plan

Month	Action Points
October 2024	Conduct searches on academic databases to gather information regarding IDS and TabNet.
November 2024	Write literature review, focusing on gaps in existing researches and potential contributions.
Desember 2024	Finalize literature review and compiling them with the study objective.
January 2025	Identify and gather datasets and begin exploring their characteristics.
February 2025	Begin data preprocessing by cleaning, normalizing, and encoding the data.
March 2025	Model development using TabNet, begin implementation using deep learning libraries.
April 2025	Evaluate TabNet model by running different tests and compiling the results.
May 2025	Tests TabNet model on different datasets to test for generalization.
June 2025	Writing the documentations regarding experiments.
July 2025	Writing the documentations regarding results and findings.
August 2025	Finalization of study.