

Enhancing Network Intrusion Detection Systems Using Machine Learning Techniques

Student Name: Keval Mahendra Motivaras

Student ID: 2515743

Module Code: ACFA7004

Module Title: Research Methods and Professional
Development

Programme: MSc Cybersecurity and Digital Forensics

University: University of Wales Trinity Saint David
(UWTSD) – London Campus

Module Leader: Dr. Suresh Shanmugasunadaram

Submission Date: 01/05/2026

Abstract

As cyber threats evolve rapidly, some of the limitations of Intrusion Detection Systems (IDS), like their use of signatures and inability to recognize zero-day attacks, become more apparent. This project proposes an investigation into enhancing network intrusion detection with the use of machine learning (ML). While existing studies prove the ability of ML based IDS to increase its accuracy and improve adaptability, there are still important problems of high rate of false positives, class imbalance, and poor real-time performance to be addressed [1], [2].

The proposed research will be conducted using a quantitative methodology, which includes applying benchmark data sets (NSL KDD, CICIDS2017) to build several different machine learning and deep learning-based IDS (Random Forest, SVM, neural networks), followed by data processing and tuning of parameters to handle class imbalance and maximize model accuracy.

The expected result of the research is the development of optimised ML based IDS, which would accurately identify malicious patterns and detect both known and zero-day attacks in real time.

Table of Contents

Introduction	4
Context and Background.....	4
Research Problem	4
Aim	4
Objectives.....	5
Significance of the Research	5
Literature review	5
Overview and organisation	5
Intrusion detection techniques.....	5
Research gaps.....	7
Research design	8
Research methods and materials.....	8
Methods	8
Materials	9
Expected outcomes, implications and limitations	10
Timeline.....	10
Recommendations and Future Work	11
Conclusion	12

Introduction

Context and Background

Modern network infrastructures lie beneath virtually every area of our daily life; at the same time, cyber-attacks such as DDoS attacks, ransomware, scanning and infiltration become common. Intrusion Detection System (IDS) becomes an important part of network security as it monitors network traffic and computer behaviours to identify malicious actions and alert the users. IDS uses two main detection strategies: anomaly based, which identifies suspicious changes to established network behaviours; and signature based, which compares network activity to a database of known malicious behaviours [1]. Hybrid approaches to IDS, which combine anomaly detection and signature recognition, are commonly used today [1]. Despite this, traditional IDS continue to exhibit poor adaptability to changing conditions and produce many false alarms.

The increased usage of network infrastructure because of cloud computing, Internet of Things and Bring Your Own Device (BYOD) practices lead to an increase of amount of traffic on network. In order to improve IDS, machine learning techniques, such as supervised classification or deep learning, were proposed for automated pattern detection [2]. One of the crucial issues associated with this approach is a class imbalance between the number of benign and malicious records. Due to this, machine learning algorithms tend to choose benign class as the main class, leading to many false negatives for attacks. Addressing class imbalance via resampling and cost sensitive learning allows to mitigate this problem to some extent [2]. Nevertheless, more advanced algorithms and techniques are required.

Research Problem

Traditional signature-based IDS have a good ability to recognize known attacks, yet cannot detect novel attacks; on the other hand, anomaly-based IDS can easily detect novel attacks, but produce many false positives. Even ML based IDS exhibit poor real time detection performance and limited generalization abilities with respect to novel types of traffic [2]. Class imbalance in network data only makes this problem worse, contributing to poor ability of algorithms to detect minority classes [2]. Thus, the research problem of this project is:

How to improve the ability of IDS to detect cyberattacks by using machine learning techniques?

Aim

The goal of the research is to propose and assess machine learning based IDS, which is superior to current methods in terms of detection accuracy and adaptiveness.

Objectives

- **Literature analysis:** conduct literature analysis on intrusion detection methods, with a focus on machine learning algorithms, and identify gaps in existing research;
- **Data acquisition and preprocessing:** identify and acquire appropriate benchmark datasets (NSL KDD, CICIDS2017) and perform data processing, including preprocessing, feature extraction and balancing procedures;
- **Model Development:** implement several machine learning algorithms (Random Forest, SVM, Gradient Boosting, ANN) and deep learning models (CNN, LSTM) to classify traffic;
- **Evaluation:** test the implemented models and analyse performance indicators (accuracy, precision, recall, F1 score), comparing them with IDS built without ML and analysing effectiveness of resampling techniques;
- **Optimization and validation:** identify optimal machine learning algorithms and techniques for their optimization (cost sensitive learning, hyperparameter tuning); assess chosen models using cross-validation and real-time simulations;
- **Reporting and dissemination:** create and present research report and a brief summary of results.

Significance of the Research

The research aims to investigate and address one of the important needs in network security, improving performance of IDS in the presence of evolving threats. Application of machine learning and deep learning approaches can allow decreasing rate of false positives, detect zero-day attacks, and increase adaptability of IDS. This may provide new insight into solving such problems as class imbalance and model optimization, creating more practical solutions for implementing adaptive IDS in enterprises, clouds and IoT infrastructure.

Literature review

Overview and organisation

This literature review surveys current research on network intrusion detection, emphasising ML-based methods, benchmark datasets and evaluation metrics. The review is structured thematically: it begins with the conceptual foundation of IDS, then examines datasets used for training and evaluation, discusses ML algorithms and deep-learning models applied to IDS and concludes with identified research gaps.

Intrusion detection techniques

Anomaly- vs. signature-based detection

Stamus Networks highlight three principal IDS detection types: anomaly-based, signature-based and hybrid [1]. Anomaly-based systems build statistical profiles of normal

behaviour and flag deviations, enabling detection of novel attacks. Signature-based systems rely on a database of known attack signatures and compare incoming traffic to these patterns; this approach provides high accuracy for known attacks but struggles with zero-day threats [1]. Hybrid systems combine both techniques to balance detection of new attacks with the low false-positive rate of signature-based detection.

Class imbalance problem

A recent study in *Electronics* notes that one of the most significant challenges in IDS is the class imbalance of network traffic data, where benign flows overwhelmingly outnumber attack instances [2]. This imbalance hinders ML models from recognising minority attack classes. Resampling techniques—Random Under-Sampling (RUS), Random Over-Sampling (ROS), SMOTE and ADASYN—are commonly employed to address imbalance [2]. Cost-sensitive learning can also be used to penalise misclassification of minority classes. The same study emphasises that the evolving cybersecurity landscape, including 5G and IoT, demands IDS capable of real-time detection and adaptability [2].

Machine-learning algorithms

Various supervised algorithms have been applied to IDS. Ajagbe *et al.* compared linear SVC, logistic regression, Random Forest, decision tree and XGBoost classifiers on the UNSW-NB15 dataset and found that RF and XGBoost outperformed other models, with accuracy exceeding 92 % [3]. Other studies evaluate k-nearest neighbours (k-NN), Naïve Bayes, Support Vector Machines and ensemble methods. Evaluation metrics typically include accuracy, precision, recall, F1-score and area under the ROC curve. Confusion matrices are widely used to compare models [3]. Although supervised methods achieve high accuracy on benchmark datasets, their performance on imbalanced or real-time traffic can degrade.

Deep learning approaches

Deep-learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks have been explored to automatically extract features from raw traffic. Mohammed *et al.* applied CNN, RNN and LSTM to time-series network data and showed that hybrid models—specifically a CNN+RNN+LSTM combination—achieved an F1-score of 0.86 and precision of 0.92 [4]. Their study emphasises that deep learning can improve detection accuracy while reducing false alarms, thereby addressing some limitations of traditional IDS [4]. Nonetheless, deep models require significant computational resources and large amounts of labelled data.

Benchmark datasets

CICIDS2017. The Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick developed the CICIDS2017 dataset to overcome limitations of earlier datasets. It contains benign and up-to-date attack traffic (e.g., Brute Force FTP/SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS) captured over five days. The dataset includes

labelled flows generated using the CICFlowMeter tool, which provides over 80 network flow features extracted from packet captures [5]. Naturalistic traffic was generated by modelling the behaviour of 25 users across protocols such as HTTP, HTTPS, FTP, SSH and email. These characteristics make CICIDS2017 a realistic and comprehensive benchmark for evaluating IDS models.

NSL-KDD. NSL-KDD is a cleaned and refined version of the KDD'99 dataset and is widely used for IDS research [6]. It contains four subsets—KDDTrain+, KDDTrain+_20 %, KDDTest+ and KDDTest-21—derived to address redundancy and complexity issues [4]. Each record in NSL-KDD consists of 43 features, 41 describing the traffic characteristics and two labels indicating normal or attack and the severity score. The dataset includes four attack categories—Denial of Service (DoS), Probe (surveillance), User-to-Root (U2R) and Remote-to-Local (R2L)—each representing a different attack behaviour. The class distribution is heavily skewed, with normal traffic constituting most records while U2R and R2L attacks appear infrequently [2]. As with other datasets, NSL-KDD suffers from imbalance and limited representation of contemporary attacks, but its widespread use facilitates comparative evaluation across studies.

Research gaps

In spite of the advancements made in machine learning based IDS, there are still some areas that require attention:

- **Real-time implementation:** Most researches consider algorithm testing offline using past data, while few have tested their model in real-time situations. Optimization techniques are yet to be exploited.
- **Imbalance resolution:** There are different ways of addressing the issue of imbalance but there is still no best practice adopted by all. Comparisons have been done only on selected data sets.
- **Transfer learning:** Algorithms developed using one set of data are not transferable to another network because of variations in traffic and attacks. Adaptation strategies are necessary to generalize algorithms.
- **Feature Engineering:** In spite of the ability of deep learning to engineer features, most models depend on human feature engineering skills. Research on automation of feature engineering could improve performance.

These shortcomings are responsible for the need for research on ML based IDS. Research design and methodology

Research design

The study will adopt a quantitative experimental design, using simulation and dataset experimentation to evaluate ML models for IDS. This design is appropriate because it allows systematic comparison of algorithms under controlled conditions and produces measurable evidence of performance improvements.

Research methods and materials

Methods

1. Data acquisition and preprocessing. The NSL KDD and CICIDS2017 datasets will be downloaded from their respective websites. In terms of preprocessing, missing value imputation, normalization of numeric attributes and one hot encoding of categorical variables will be performed. To handle class imbalance, resampling techniques such as RUS, ROS, SMOTE and ADASYN will be explored alongside cost sensitive approaches [2]. Feature selection and dimensionality reduction methods, e.g., recursive feature elimination, mutual information and PCA respectively, will be utilized.
2. Model development. Several supervised learning approaches will be implemented using Python and scikit-learn and TensorFlow among others. Baseline methods that will be used include Logistic Regression, Decision Tree, Random Forest, Gradient Boosting (XGBoost), SVM and k-Nearest Neighbours (k-NN). As part of deep learning, CNN, LSTM, and Hybrid CNN-LSTM models will be developed using Keras/PyTorch libraries. Hyperparameter tuning will be done via grid search/Bayesian optimization. Assembling strategies such as model stacking can be utilized. Model training will follow a stratified approach (e.g., 70% train/15% validation/15% test) as outlined in the literature [3]. Cross validation (e.g., 5 folds) can be applied to validate model performance.
3. Evaluation and comparison. Evaluation measures will be based on classification performance indicators namely accuracy, precision, recall, F1 Score and Confusion Matrices [3]. Other measures such as ROC curves, Area Under the Curve (AUC), Matthews Correlation Coefficient (MCC) and Detection Latency will also be calculated. The effect of different resampling techniques in detecting minority attacks will be analysed. Comparisons among the proposed models will be done using appropriate statistical test(s) (e.g., Wilcoxon signed rank).
4. Proposed system architecture. The system will have four major components:

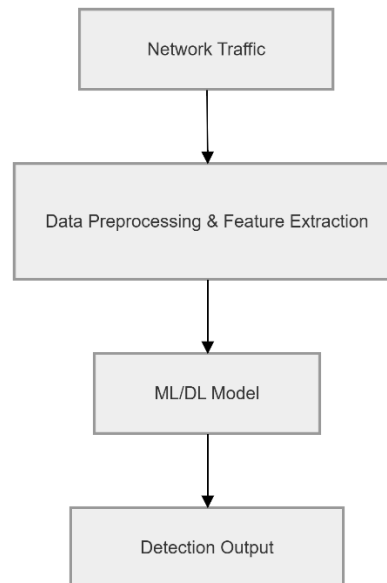
Traffic Capture: Raw network traffic or network flows are captured. In case of simulation, pre-processed offline dataset will serve this purpose. For realistic purposes, packets are generated as per the traffic distribution in a real environment.

Pre-processing and Feature Extraction: This entails data cleaning, normalizing, balancing the dataset and feature vectorization.

Classification: ML and deep learning models predict whether incoming flow is normal or an attack.

Alert Generation: Aggregated classification results lead to alert generation indicating occurrence of an attack.

A general flow chart is provided below:



Materials

- **Datasets:** CICIDS2017 dataset contains realistic network traffic with labelled benign and attack flows for multiple protocols. NSL KDD dataset is a clean and well-balanced one containing 43 attributes and four types of attack categories [4]. The two datasets will be used to validate model training. Additionally, other relevant datasets (e.g., UNSW NB15) will be employed for cross-validation depending on time availability.
- **Software:** Python (version ≥ 3.8) will be used for code development. Main libraries are scikit learn for traditional ML algorithms, xgboost for gradient boosting, TensorFlow/Keras/Pytorch for DL models, pandas/NumPy for data manipulation and Matplotlib/seaborn for visualisation. Jupyter notebooks will enable easy data exploration. Imbalanced learn library will allow implementing various resampling techniques. Project version control will be done using git.
- **Hardware:** As for hardware requirements, at least a development computer with CPU containing 8GB RAM should be used. GPU (NVIDIA card) may prove useful for experiments related to deep learning models and computing power. However, models developed in this project will be optimised in order to perform efficiently on general computers.

- **Ethical considerations:** Since all the datasets are public and anonymised (no personally identifiable information), the research does not raise any ethical issues. Institutional ethical guidelines will be considered in the course of the research, which includes the filling of an ethics form indicating the use of secondary data.

Expected outcomes, implications and limitations

Expected results. It can be anticipated that ensemble approaches (Random Forest, Gradient Boosting) and deep learning models would surpass logistic regression model in the task of IDS performance (both in terms of accuracy and recall). Combining resampling and cost sensitive learning would increase the detection rate for rare classes. Hybrid CNN LSTM model can capture temporal dependencies in the network traffic and have very good F1 score [4]

Implications. First, a more accurate IDS could help organisations detect attacks more quickly and avoid false negatives. Second, better performance in the task of imbalanced classes detection would result in a better IDS. Moreover, the developed model can be further used in order to create real-time IDS for enterprises or even IoT networks. From an academic standpoint, the contribution will come in the form of comparison of balancing approaches and ML/DL techniques on several IDS datasets and algorithm/hyperparameter selection tips.

Limitations. The first limitation is related to the scope of available datasets, as CICIDS2017 and NSL KDD datasets might not adequately reflect modern-day encryption challenges or multi-stage attacks. Second, we will employ only offline datasets, which means that our model might not accurately represent real-time performance of an IDS. Third, some deep learning models might need additional computing power or even GPUs, which is not available in the current project. Fourth, time consumption associated with hyperparameter tuning is another challenge.

Timeline

Phase	Weeks (approx.)	Description
Literature review & proposal refinement	1–2	Conduct detailed literature review; finalise research problem, aim and objectives.
Dataset acquisition & preprocessing	3	Acquire NSL-KDD and CICIDS2017 datasets; perform data cleaning, feature engineering and balancing.
Model development (classical ML)	4–5	Implement and tune ML algorithms (LR, DT, RF, SVM, XGBoost).

Phase	Weeks (approx.)	Description
Model development (deep learning)	5–6	Design and train deep-learning models (CNN, LSTM, hybrid architectures).
Evaluation & analysis	7	Evaluate models using cross-validation; compare performance metrics; conduct statistical analysis.
Report writing & presentation	8	Compile research findings; draft the final report; prepare presentation slides and ethics form.

This timeline is provisional and may be adjusted based on the complexity of experiments and results. A Gantt chart will be created in the full project report to visualise dependencies and milestones.

Recommendations and Future Work

Recommendations for improving IDS based on machine learning could include several important directions. Hybrid and ensemble learning could be used to maximise the efficiency of detecting attacks based on multiple types of attacks. This may be achieved by implementing multiple models using different combinations of Random Forests, gradient boosting and deep learning models. The problem of class imbalance requires an adequate approach to be implemented. For this purpose, advanced approaches like SMOTE and cost sensitive learning could be employed [2].

Finally, it is important to integrate real-time data processing and stream-based analytics to make the deployment of IDS feasible in real time environment. Offline evaluation should be expanded by introducing real-time simulation to increase the efficiency and scalability of IDS. Furthermore, feature selection and dimensional reduction should be implemented in order to achieve higher performance of detection.

The possible future directions of IDS research may include further improvements in transfer learning and adaptability of the models used to detect various attacks. These directions could contribute to creating IDS models that would be portable between different networks. The deep learning architecture should be improved by implementing hybrid CNN-LSTM model in IDS to capture both spatial and temporal properties of network traffic [1]. It is also important to explore the impact of encryption on network traffic and emerging technologies, e.g., IoT and 5G, on the process of detecting intrusions.

Conclusion

Intrusion detection remains a serious issue in network security. Traditional IDS models lack efficiency, resulting in high rates of false positives and poor adaptation to novel attacks. The proposed research aims at developing a method of enhancing IDS through using machine learning and deep learning, overcoming the problem of class imbalance, and optimising models for more accurate and efficient detection. Through systematic evaluation of classical and deep learning models of detection and employing resampling and cost sensitive learning, this study aims at delivering effective IDS models with lower rates of false positives.

References

- [1] D. Robinette, "What are the Three Types of IDS?" 2024, Available at:
<https://www.stamus-networks.com/blog/what-are-the-three-types-of-ids>.
- [2] M. AlZubaidi, "Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches," vol. 14, no. 1, pp.69, 2024,
- [3] S. A. Ajagbe, J. B. Awotunde and H. Florez, "Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset," vol. 5, pp.1028, 2024,
- [4] A. A. A. Mohammed, "Improving Intrusion Detection Systems by Using Deep Learning Methods on Time Series Data," vol. 15, no. 1, 2025,