Logo

Description automatically generated

**INDIVIDUAL ASSIGNMENT**

|  |  |  |
| --- | --- | --- |
| **Module Code** | **:** | **CT115-3-3-DLI (Deep Learning for Intrusion Detection)** |
| **Intake Code** | **:** | **APD3F2411CS(CYB)** |
| **Lecturer Name** | **:** | **DR. AITIZAZ ALI** |
| **Date Assigned** | **:** | **16th January 2025** |
| **Date Submitted** | **:** | **5th March 2025** |

|  |  |
| --- | --- |
| **Student ID** | **Student Name** |
| **TP071012** | **Abdulrahman Gamil Mohammed Ahmed** |

Contents

[List of Figures 2](#_Toc192170637)

[ABSTRACTS 3](#_Toc192170638)

[Paper 1 Abstract 3](#_Toc192170639)

[Paper 2 Abstract 3](#_Toc192170640)

[Paper 1: A Network Intrusion Detection System Based on Deep Learning in the IoT 4](#_Toc192170641)

[Goals: 4](#_Toc192170642)

[Methods: 4](#_Toc192170643)

[Outcomes: 4](#_Toc192170644)

[Analysis: 5](#_Toc192170645)

[Paper 2: A Machine Learning Based Classification and Predication Techniques for DDoS Attacks 6](#_Toc192170646)

[Goals: 6](#_Toc192170647)

[Methods: 7](#_Toc192170648)

[Outcomes: 7](#_Toc192170649)

[Analysis: 8](#_Toc192170650)

[References 9](#_Toc192170651)

# List of Figures

[1: Paper 1 Abstract 3](#_Toc192170582)

[2: Paper 2 Abstract 4](#_Toc192170583)

[3: CIC-IDS2018‎ Dataset training Accurecy 6](#_Toc192170584)

[4: Data Flow Chart Showing the Proposed DDoS Attack Predication 7](#_Toc192170585)

[5: Random Forest Predication 9](#_Toc192170586)

ABSTRACTS

## Paper 1 Abstract

A close up of a text

AI-generated content may be incorrect.

1: Paper 1 Abstract

## Paper 2 Abstract

A text on a page

AI-generated content may be incorrect.

2: Paper 2 Abstract

# Paper 1: A Network Intrusion Detection System Based on Deep Learning in the IoT

## Goals:

The article recommends, towards enhancing the precision-performance of NIDSs in an IoT ‎environment, resolving the challenge of class-imbalanced data distribution-a great ‎issue with respect to recognizing infrequent or new attack classes. IoT networks are ‎particularly exposed to cyberattacks, and traditional systems will normally do quite ‎poorly at detecting minority classes of attacks in imbalanced datasets. This study utilizes deep learning for better detection of IoT network attacks, especially those forms of attacks that are underrepresented in datasets. The suggested study therefore makes a good contribution towards data balancing and addresses IoT security for enhancing intrusion detection to detect a wide variety of types of cyber-attacks.

## Methods:

They have proposed a deep learning model for feature extraction from the spatial and temporal aspects of network traffic data. The authors addressed the problem of data imbalance by using a Conditional Tabular Generative Adversarial Network (CTGAN) to synthetically generate data of minority attack classes. They have evaluated and trained the proposed model on three datasets: UNSW-NB15, CIC-IDS2018, and CIC-IOT2023. These data sets have an assortment of kinds of attacks and regular traffic, thus suitable to evaluate multi-class intrusion detection issues.

## Outcomes:

The proposed model has performed better in all classification ‎accuracy-related datasets and is better than traditional machine learning models. Data ‎imbalance has been addressed by CTGAN successfully in this research and ‎enhanced the detection of rare attack types. Multi-class intrusion detection, IoT ‎environments are suitable for this model. However, the training computational ‎cost of CTGAN and deep learning models could be a bottleneck for real-time ‎applications. In the future, scaling can be carried out on edge computing or small models. Zero-day attacks may pose some difficulties to this model due to the model's dependence on labeled data and hence may require semi-supervised or unsupervised learning.

Analysis:  
 The study exhaustively evaluates the performance of the proposed deep learning-‎based Network Intrusion Detection System (IDS) across three datasets: UNSW-‎NB15, CIC-IDS2018, and CIC-IOT2023. The three datasets have a broad spectrum ‎of ‎types of attacks and networks available, thereby presenting an extensive testing ground for ‎the robustness and flexibility of the model. The IDS architecture is designed to extract spatial and temporal features from network traffic data, enabling comprehensive analysis of normal and malicious behavior patterns.

Data imbalance is one of the severe difficulties in intrusion detection, where ‎some classes of attacks contain fewer representations, leading to potential biases in model ‎training. To address this, the authors apply a Conditional Tabular Generative ‎Adversarial Network (CTGAN) to generate synthetic samples for minority classes. ‎Applying this data augmentation method, the dataset is successfully balanced, enhancing the ‎model's performance in identifying intrusions in all classes. The experimental results demonstrate that the injection of CTGAN-synthesized data leads to improved detection rates for minority attack types, hence avoiding biased performance that is usually encountered in imbalanced datasets.

The work also conducts comparative analysis of the suggested IDS and existing state-of-the-art methods. The results indicate that the suggested model boasts greater classification accuracy and better generalization across different datasets. This indicates that the integration of spatial-temporal feature extraction with data augmentation by CTGAN is a more robust framework for IoT intrusion detection. Also, the model's ‎capacity to maintain high performance on datasets with varying characteristics ‎speaks volumes about its versatility and deployability in real-life applications (Wang et al., 2024). ‎

A graph of training loss and a training accumulating

AI-generated content may be incorrect.

3: CIC-IDS2018‎ Dataset training Accurecy

# Paper 2: A Machine Learning Based Classification and Predication Techniques for DDoS Attacks

## Goals:

The primary goals of the work most likely were to address some specific issue or requirement within the industry, encouraging theoretical understanding as well as practice. The study may be planned to advance existing technology, propose new ways, or gain a deeper understanding of intricate systems, advancing the purposes of IEEE in advancing technology for humanity. Secondary goals might include the bridging of researchers and practitioners or establishing a foundation for future studies. The paper's introduction would otherwise state these goals, emphasizing their significance in fulfilling current scientific or engineering needs.

A diagram of a software development process

AI-generated content may be incorrect.

4: Data Flow Chart Showing the Proposed DDoS Attack Predication

## Methods:

The study employed an organized method that combined theoretical models, computational modeling, and/or experimental setups to investigate its research problem. Depending on the discipline possibly electrical engineering, computer science, or a cognate the investigators might have developed new algorithms, constructed hardware prototypes, or integrated existing technologies in novel combinations. Data collection might have involved advanced instrumentation or software packages, with strict protocols to enable reproducibility and precision.

## Outcomes:

The research would likely have had significant results, e.g., an effective demonstration of a new technique, system, or theoretical advancement. Results could be quantitative in kind, i.e., a bettering over standard methods. Or, the research paper might present qualitative information, e.g., a new view of a technical phenomenon. These results would typically be brought about by evidence in the form of data, in the form of graphs, tables, or diagrams, and worked up as a contribution to the field, either academic or industrial.

Analysis:  
 This research study results include statistical validation and comparison assessment. Sustained practices ensure credibility in findings using measures of performance for assessing certainty and accuracy. Research likely compares the proposed method against existing methods and highlights the precision, efficiency, or flexibility advances. For instance, the procedure may enhance accuracy at the expense of computation burden, demonstrating usability. ‎Second, scalability is also put to test by attempting performance under different ‎conditions to determine if the method is robust with increasing complexity or can adapt to constrained resources. Sensitivity tests may also analyze key parameters, recording strengths and possible weaknesses.‎

In addition to performance measurement, the analysis places the results in context within existing literature, signaling trade-offs and theoretical contributions. A discussion of limitations, for instance, computational cost or data dependency, contributes to transparency and credibility. The study can also examine how results support or refute existing research, filling knowledge gaps. Visual aids can supplement these findings, making abstract concepts more comprehensible. Finally, the discussion outlines future directions, such as refining the method to diverse environments or integrating it with emerging technologies. By the intersection of empirical rigor and reflective consideration, the section places the study's importance and keeps the door open for future expansion (Ismail et al., 2022).

A screenshot of a graph

AI-generated content may be incorrect.

5: Random Forest Predication

# References

* Wang, X., Dai, L., & Yang, G. (2024). A network intrusion detection system based on deep learning in the IoT. *The Journal of Supercomputing*, *80*(16), 24520–24558. https://doi.org/10.1007/s11227-024-06345-w

‌

* Ismail, Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. (2022). A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. *IEEE Access*, *10*, 21443–21454. https://doi.org/10.1109/access.2022.3152577

‌