LIGHTWEIGHT AI INTRUSION DETECTION

INTRODUCTION

Intrusion detection systems (IDS) monitor network traffic for malicious activity. However, many AI-based IDSs are too resource-heavy for edge deployment, leaving resource-constrained parts of the network under-protected.

MAIN OBJECTIVE

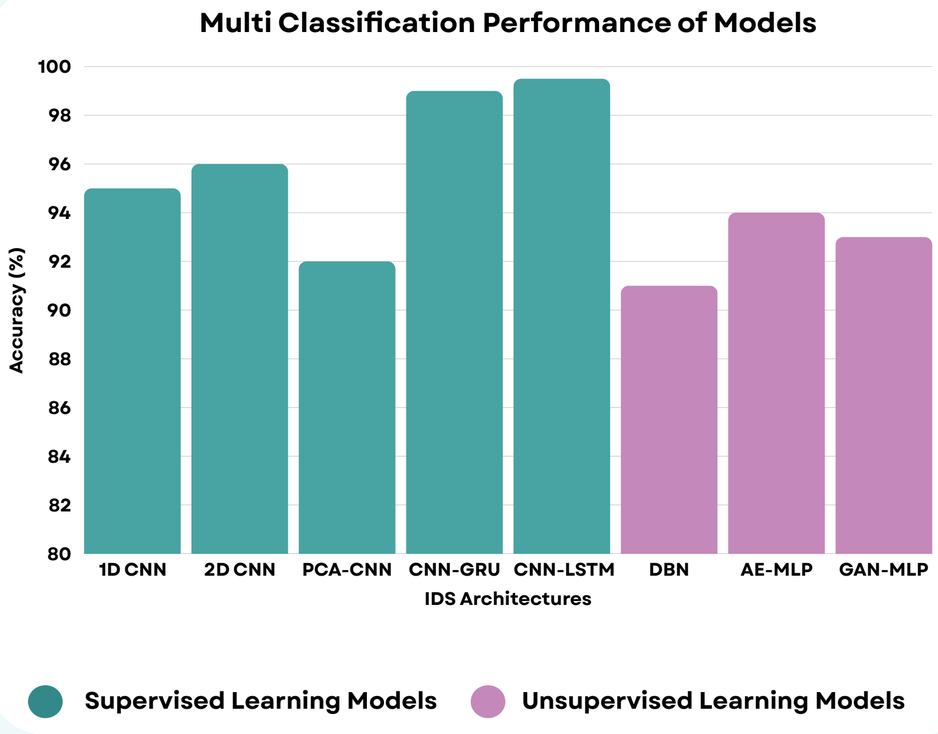
To investigate, develop and optimise several lightweight AI Intrusion Detection models for resource-constrained network environments, while maintaining strong detection performance to both known and unknown attacks.

GENERAL MODEL PIPELINE

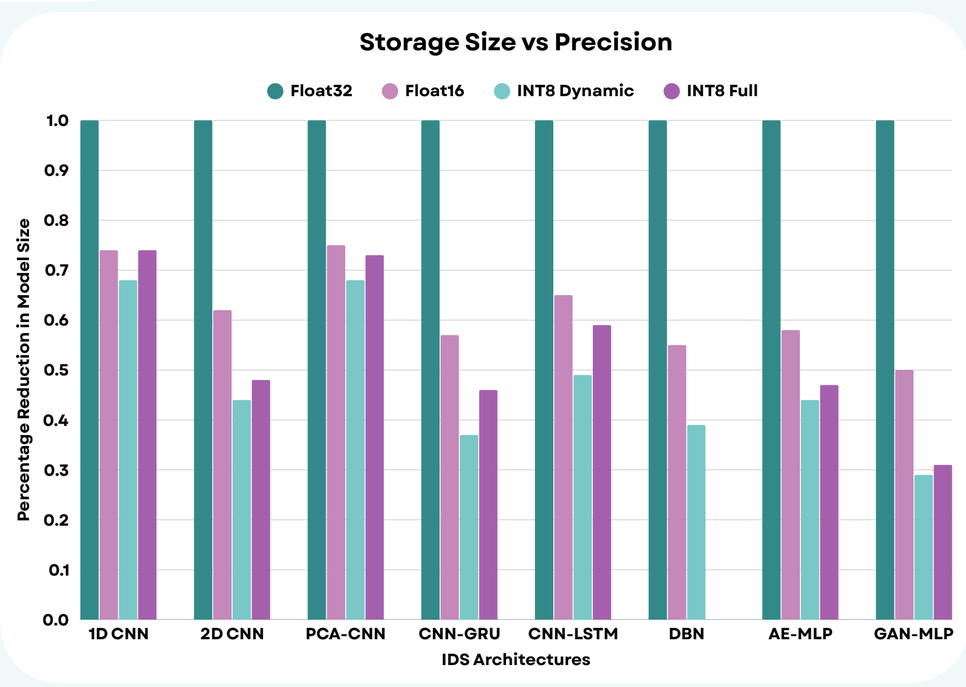
PREPROCESS DATA → TRAIN MODEL → TEST MODEL → PERFORM QUANTISATION → TEST GENERALISATION

Detection models were trained on the CICIDS2017 network dataset. To ensure all attack types were learned fairly, class imbalance was addressed. The models were saved based on their best multi-classification performance. After which they were simplified using Post-Training Quantisation to reduce memory usage and processing power. Finally, the models' abilities to detect new, unseen attack types were tested by holding out one attack type during training for evaluation.

RESULTS



- All models achieved a high level of classification accuracy, with the supervised models significantly outperforming their unsupervised counterparts.
- The 2D CNN consistently outperformed the 1D CNN across all multi-classification metrics and in zero-day attack detection.
- Post-Training Quantisation successfully reduced the models' memory requirements, making lightweight deployment viable.
- All models demonstrated the ability to detect zero-day attacks.



CONCLUSION

- The majority of the proposed models, along with their quantised variants, outperformed the baseline 1D CNN, with several displaying improvements across all evaluation metrics.
- CNN-GRU, CNN-LSTM and 2D CNN models are viable for real world deployment.
- Further testing on real-world edge devices is recommended for complete validation.

Christopher Blignaut
BLGCHR003@myuct.ac.za
Sian Caine
CNXSIA001@myuct.ac.za
Claire Campbell
CMPCLA004@myuct.ac.za

Superviser: Josiah Chavula

IT | SCHOOL OF IT

University of Cape Town,
Private Bag X3,
Rondebosch 7701,
South Africa
+27 21 650 9111