Edinburgh Napier UNIVERSITY

Utilizing the Ensemble Learning and XAI for Performance Improvements in IoT Network Attack Detection

Sampath Kalutharage Xiaodong Liu Christos Chrysoulas Oluwaseun Bamgboye

c.kalutharage@napier.ac.uk , x.liu@napier.ac.uk , c.chrysoulas@napier.ac.uk , o.bamgboye@napier.ac.uk

Edinburgh Napier University, Edinburgh, UK

Edinburgh Napier
UNIVERSITY

Outline…

- Introduction
- Related Work
- Methodology
- Results and Evaluation
- Conclusions

Introduction

- IoT devices run a significant risk of being the target of cyberattacks [1].

Introduction

- Due to the complexity of threats, traditional signature-based intrusion detection systems (IDS) have been inefficient in identifying these attacks [2].
- AI systems present advanced solutions that exhibit improved capabilities in detecting and mitigating the impact of cyberattacks and potential threats on IoT.

Introduction

- The primary benefit of AI-based approaches is their ability to operate without seeking specific targets,
- Eliminating the requirement to comprehensively define all known attack vectors
- Continuously update this attack dictionary [3]

Introduction

- IoT devices are characterized by limited resources
- The application of AI-based security mechanisms on IoT devices faces memory capacity limitations, necessitating the design of lightweight models [4].
- Many security datasets are complex and demand significant computational power.

Edinburgh Napier UNIVERSITY

Introduction

- Binary detection methods, while common, are limited in providing comprehensive security as they only detect intrusions.
- It's essential to categorize specific attack types for effective defense and decision-making.
- However, multi-class detection techniques may have lower hit rates compared to binary methods, making some attacks challenging to detect.

Contribution

- We introduced a methodology that refines attack detection datasets by emphasizing the most influential features, using principles from Explainable Artificial Intelligence (XAI).
- Our paper introduces an ensemble approach for IoT attack detection, merging unsupervised learning with XGBoost for improved accuracy.
- We've developed an efficient model surpassing the state-of-the-art approach and comprehensively evaluated it using the CIC-IDS dataset.

Related Work

- Ikram et al. [5] proposed an ensemble intrusion detection model that merged different neural network types, such as Long Short Term Memory (LSTM), Back propagation Network (BPN), and Multilayer Perceptron (MLP).
  - However, the study did not employ explainability for feature selection, and it also omitted the use of feature reduction techniques to create a more lightweight model

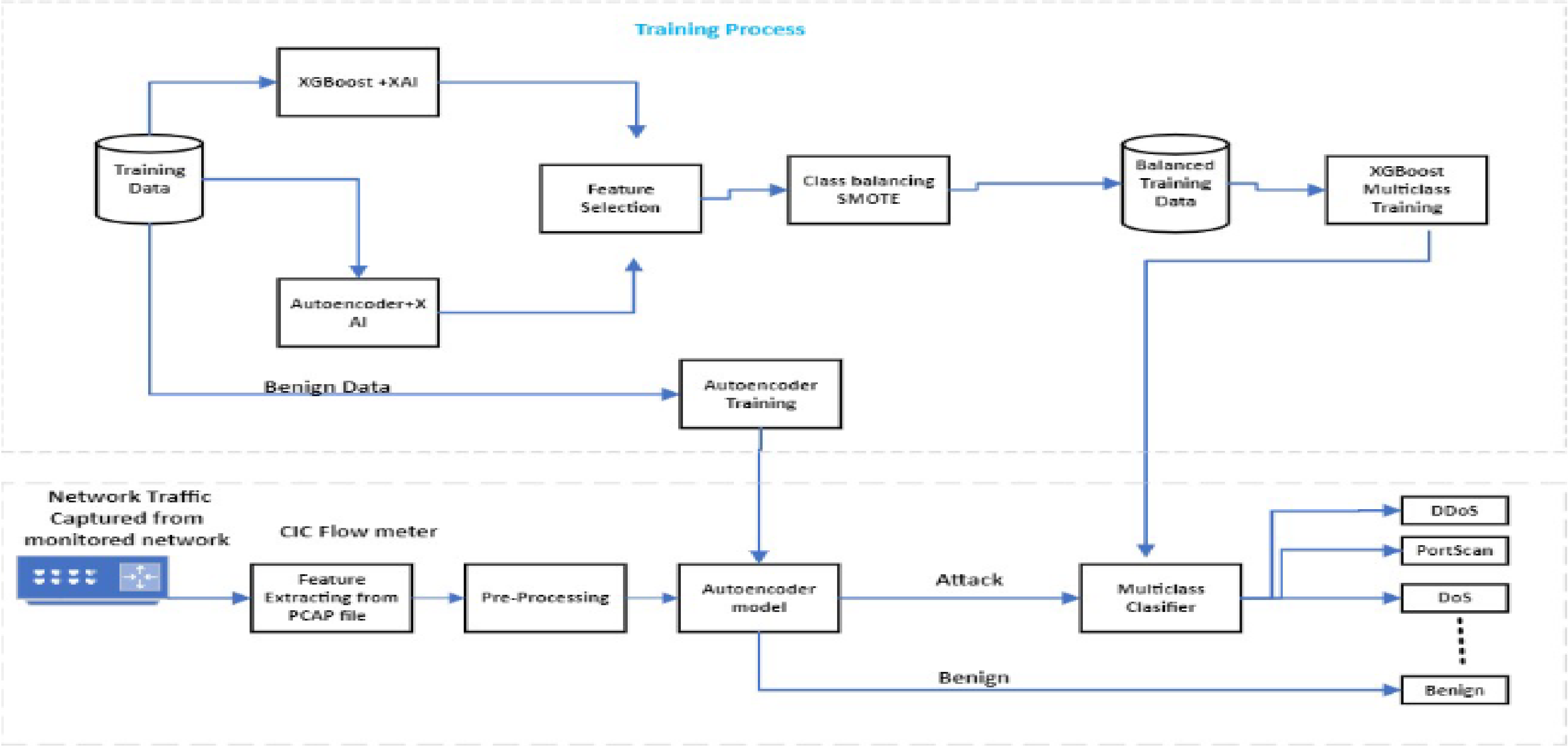
- hunhe Song et al. [6] proposed an intrusion detection system method that combines deep learning and feature-based techniques. The method uses a Bayesian approach to tune XGBoost' hyperparameters for maximum performance while minimizing performance loss due to incorrect parameter selection.
  - This method does not cater to the resource constraint demand of IoT networks, and it also lacks the utilization of explainability for achieving more precise results

Related Work

- Rabavathy et al.[7] proposed a new intrusion detection method based on Sequential Online Extreme Learning Machine (OS-ELM) for fog computing environments.
  - The proposed method uses multiclass detection, but this makes it more difficult to identify attacks that involve privilege escalation and probing

- Blanco et al. [8] proposed a method for multi-class network attack classification that can be installed in a router. The method is based on a Convolutional Neural Network (CNN).
  - However, the work did not consider the IoT setting.

Methodology



Edinburgh Napier UNIVERSITY

Results

Table 1. Results of comparison of each attack type with current state of the art

	DNN [6]		RF [6]		ET+Multi Cla [6]		**Proposed model**	
	PRE	REC	PRE	REC	PRE	REC	PRE	REC
Benign	98.81	99.91	98.88	99.78	98.96	99.58	99.96	99.80
BOT	99.77	99.88	99.62	99.77	99.99	99.90	86.78	82.89
DDoS	99.47	99.88	99.91	99.91	99.99	99.94	100	100
DoS	95.32	89.61	96.35	89.26	97.38	88.13	100	100
FTP-Patator	-	-	-	-	-	-	100	100
Heartbleed	-	-	-	-	-	-	100	67.97
Infiltration	44.10	01.79	29.60	07.08	28.46	13.50	100	64.87
Portscan	-	-	-	-	-	-	99.77	100
SSH-Patator	-	-	-	-	-	-	100	100
Web Attack	100	39.29	92.31	42.86	39.34	85.71	99.92	99.23

Conclusions

- The proposed model incorporates XAI to identify the most influential features for attack detection and to reduce the feature space for a lightweight model.
- An autoencoder is employed for anomaly detection in the first stage, allowing agile release of benign traffic and enabling more robust inspection using the XGBoost approach for unidentified events.
- The initial experiments conducted on the CIC-IDS dataset have shown promising results. However, future work will focus on evaluating the proposed approach using additional benchmark datasets, such as BoT IoT3 and the NSL-KDD4 security dataset

Future Direction

- we will deploy the approach on a Raspberry Pi device using TensorFlow Lite, allowing us to test it on a low-cost, embedded platform. Once successful on the Raspberry Pi, we will explore the potential of deploying the approach on other embedded systems or MCUs.
- our plan includes simulating the system on real-world IoT and critical infrastructure networks to assess its effectiveness in real-time intrusion detection

Reference

1. Samaila, M.G., Neto, M., Fernandes, D.A., Freire, M.M., In´acio, P.R.: Challengesof securing internet of things devices: A survey. Security and Privacy 1(2), e20 (2018)
2. Sampath Kalutharage, C., Liu, X., Chrysoulas, C.: Explainable ai and deep autoencoders based security framework for iot network attack certainty (2022)
3. Mitchell, R., Chen, I.R.: A survey of intrusion detection techniques for cyberphysical systems. ACM Computing Surveys (CSUR) 46(4), 1–29 (2014)
4. de Souza, C.A., Westphall, C.B., Machado, R.B.: Two-step ensemble approach for intrusion detection and identification in iot and fog computing environments. Computers Electrical Engineering 98, 107694 (2022). https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107694, https://www.sciencedirect.com/science/article/pii/S0045790622000155
5. kram, S.T., Cherukuri, A.K., Poorva, B., Ushasree, P.S., Zhang, Y., Liu, X., Li,G.: Anomaly detection using xgboost ensemble of deep neural network models. Cybernetics and information technologies 21(3), 175–188 (2021)
6. Song, C., Sun, Y., Han, G., Rodrigues, J.J.: Intrusion detection based on hybrid classifiers for smart grid. Computers & Electrical Engineering 93, 107212 (2021)
7. rabavathy, S., Sundarakantham, K., Shalinie, S.M.: Design of cognitive fog computing for intrusion detection in internet of things. Journal of Communications and Networks 20(3), 291–298 (2018). https://doi.org/10.1109/JCN.2018.000041
8. Blanco, R., Malag´on, P., Cilla, J.J., Moya, J.M.: Multiclass network attack classifier using cnn tuned with genetic algorithms. In: 2018 28th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS). pp.177–182 (2018). https://doi.org/10.1109/PATMOS.2018.8463997

Edinburgh Napier
UNIVERSITY

Thank you!

napier.ac.uk