Harnessing Machine Learning for Enhanced Internet of Things (IoT) Security and Attack Detection

Md Ahnaf Akif, Ismail Butun, and Imad Mahgoub
Department of Electrical Engineering and Computer Science (EECS), Florida Atlantic University,
Boca Raton, FL, USA
emails: *makif2022@fau.edu*, *ibutun@fau.edu*, *mahgoubi@fau.edu*

2024 International Symposium on Networks, Computers and Communications (ISNCC) | 979-8-3503-6491-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISNCC62547.2024.10759058

***Abstract*—The rapid growth in IoT devices has modernized connectivity across industries. It has also raised severe security concerns regarding IoT networks, making them a prime target of cyber attacks. In this work, we present an in-depth study on the detection of IoT attacks using state-of-the-art machine learning techniques such as Artificial Neural Networks, Random Forests, Extreme Gradient Boosting, and Convolutional Neural Networks. After underlining the careful cleaning and preprocessing of data, we have conducted several simulations on the IoT-23 dataset, which includes many attacks against devices, like Distributed Denial of Service and malware from the Mirai and Okiru botnets. In this paper, we present experimental results that show our approach significantly improves the accuracy and efficiency of attack detection in IoT environments with respect to the literature. Results point out that good data preprocessing lies at the very core of better detection performance; it provides a framework for developing practical, scalable, and reliable security solutions in the future for the IoT.**

***Index Terms*—IoT, Cyber-attacks, intrusion detection, ML, AI, ANN, RF, XGBoost, CNN, and DDoS.**

I. Introduction

The Internet of Things (IoT) represents one of the most important paradigm shifts in the interaction and communication patterns of devices and systems. It can trace its roots back to the development of Cyber-Physical Systems (CPSs) and Wireless Sensor Networks (WSNs), where the base ideas of interconnectivity between devices and data sharing have evolved.

The term 'Internet of Things' was coined by Kevin Ashton in the year 1999, when he had a vision that physical objects would be connected to the Internet to allow data collection and its management on an unprecedented scale. From a conceptual idea, IoT has emerged over two decades as a transformative technology, changing the world of healthcare, transportation, and agriculture, among other sectors.

Initially, CPSs served to fill in the gap between computational elements and physical processes. In this way, the system integrated sensors, actuators, and control systems to monitor and manage a physical environment, such as industrial processes and critical infrastructures. WSNs have been developed about the same time that networks of spatially distributed sensors have for collecting and transmitting environmental data for numerous applications like environmental monitoring, military surveillance, and structural health monitoring. The convergence of CPSs and WSNs paved the way for the development of IoT because they have proved the feasibility and advantage of interconnected, data-driven systems.

The proliferation of smart devices and mobile phones in the early 2000s increased the growth rate of IoT. Smartphones, having advanced computation, sensing, and connectivity capabilities, became an integral part of the IoT. They provided real-time interaction and served as data concentrators. Embedded with many sensors, like GPS, accelerometers, and gyroscopes, among others, they provided very useful context-aware data, thus enhancing the functionality of IoT and extending its applicability domain. As IoT advanced, smart devices incorporated sensors, processors, and communication modules. Devices such as wearable fitness trackers and intelligent home appliances extended IoT applications. The importance of the development of this technology was propelled by the wide availability of wireless technologies such as Wi-Fi, Bluetooth, Zigbee, and 5G, as well as the reduced costs of sensors and microprocessors.

Not very long ago, the IoT would have been coterminous with many people's idea of a 'connected world,' where everyday things are capable of sensing, processing, and communicating data. AI and ML further enabled this with IoT by adding predictive analytics, autonomous decision-making, and real-time process optimization. As it matures, the IoT vision is to create revolutions in various industries with actionable insight, enhanced efficiency, and quality of life made possible by a plethora of innovative applications and services.

On the other hand, the rapid proliferation of IoT devices, created major cybersecurity challenges wherein most of these gadgets would operate in diverse and dynamic environments, making them quite vulnerable to different forms of cyber threats [1]. The 2024 IoT Security Landscape Report reveals alarming statistics: home network devices experience an average of 10 attacks every 24 hours, and Bitdefender smart home security solutions block approximately 2.5 million threats daily, equating to around 1,736 threats per minute [2] (see Fig. 1, for a graphical compilation of various attacks).

Other major cybersecurity challenges toward IoT include unauthorized access, data breaches, Distributed Denial of Service attacks, and malware infiltration, among others. It

This work is done in the Tecore Networks Lab at Florida Atlantic University and is funded by the Office of the Secretary of Defense (OSD), Grant Number W911NF2010300.

979-8-3503-6491-0/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.

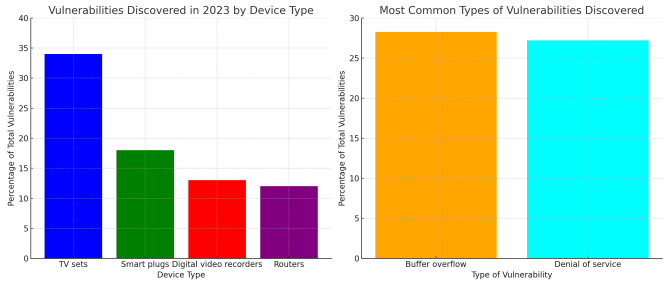

Fig. 1. Cyber attacks against IoT devices in 2024, a comprehensive view (a graphical representation of 2024 IoT Threat Report [2]).

also opens up a great risk to the individual user and critical infrastructure with its constrained computational resources and lack of standardized protocols in dealing with security concerns.

Technologies such as Artificial Intelligence (AI) and Machine Learning (ML) offer promising solutions for mitigating such cybersecurity challenges. Advanced anomaly detection systems can be developed with AI and ML that would help in the identification and mitigating of threats in near real-time. Only such technologies can analyze huge amounts of data generated from these devices, learning from the patterns, and detecting deviations indicative of cyber-attacks. For example, training machine learning algorithms on normal behavioral patterns of IoT devices can help in detecting anomalies that may indicate malicious activity.

In this paper, we focus on using ML methodologies to improve cybersecurity within IoT networks. Herein, we introduce various schemes of ML algorithms: Artificial Neural Networks (ANN), Random Forests (RF), Extreme Gradient Boosting (XGBoost), and Convolutional Neural Networks (CNN) for the detection and prevention of cyber threats. We place great importance on data cleaning and pre-processing to ensure that input data of quality is fed to the models to enhance their accuracy and reliability.

In order to validate our proposed methodologies, we are going to test our algorithms on a well-known IoT dataset called IoT-23 [3], which contains the largest variety of attacks, including DDoS attacks and malware attacks via the Mirai and Okiru botnets. Detailed simulations and evaluations of such scenarios will be run on this dataset to prove that our ML-based approach significantly improves cyber threat detection and mitigation in IoT environments.

Finally, it is logical to state that, AI and ML can be integrated into IoT cybersecurity frameworks to provide a robust mechanism for detecting and responding to cyber threats. The scalability and reliability for securing IoT networks against evolving cyber-attacks can be achieved through the use of these emerging technologies. The contribution we can make to the body of knowledge is through an in-depth study regarding the application of ML algorithms in securing IoT environments, which has promising implications for future IoT deployments.

In this paper, we address the above-mentioned problem(s) by expanding the highlighted topics in the existing literature. The remainder of the paper is organized as follows: Section I presents the challenges, pitfalls, and advantages of IoT, and also differences and similarities compared to CPSs and IoT. Related work is enlisted in Section II. Section III lays the foundation for the ML algorithms for the detection of cyber-attacks. Section IV evaluates the proposed methodology and cross-compares it to the existing approaches in the literature. Finally, Section V concludes the paper and projects the future work.

II. Related Work

The authors of [4] presented a new AI framework that detects malware in IoT devices to mitigate cyber-attacks. The authors focus on enhancing security in various use cases for smart environments through an all-inclusive AI-enabled approach in this paper. Experimental setup: Emulation of a smart environment using the Raspberry Pi and NVIDIA Jetson as gateways in logging data from IoT devices connected via the MQTT protocol, which allows monitoring of real-time malware attacks for their prediction. In this work, many models of AI have been evaluated, among which the DNN model demonstrated superior accuracy and classification capability with an F1-score of 92% and detection accuracy of 93% on Edge-IIoTset and IoT-23. Concerns about the impact on system resources by specifying metrics are drawn to traffic and CPU usage on both devices, while challenges in view include the lack of ground-truth data in most cyberattacks. Future research shall be on few-shot learning, lightweight model implementation, deep learning state-of-the-art techniques, penetration testing, and the use of additional sensor and actuator data to enhance the anomaly detection system.

The work by [5] addresses feature extraction from IoT data using the IoT 2023 dataset as a comprehensive benchmark. This involves the assessment of traditional statistical techniques and machine learning-based methods to further improve the understanding of characteristics and potential applications that could be associated with the dataset. In the context of IoT, feature extraction becomes very important due to the ”curse of dimensionality,” whereby it is known that an increase in dimensions increases complications related to processing and analyzing data. The various techniques have been surveyed to place them in the context of their strengths in capturing relevant information, reducing dimensionality, and improving performance in IoT analytics. Some key findings in this respect include the Hughes phenomenon: classifier performance may get better with more features up to some optimal point before deteriorating. In this paper, via ample experiments and performance analysis, guides the choice of suitable feature extraction methods to be deployed for various IoT applications. This will, therefore, help in the practical development of IoT solutions in 2023 and beyond. Besides, according to the authors, little effect of reducing features on the model performance is up to an accuracy of 93.04% using Decision Trees and 93.05% using Random Forest models.

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.

This paper reviews CNN for anomaly detection within the Internet of Things networks [6], thus, tries to evaluate the performance of dimensions CNN1D, CNN2D, and CNN3D in the presence of normal and anomalous network data. It shows the models' trustworthiness in detecting different cyber-attack types and maintaining the integrity of the IoT network traffic. Various datasets are used, including Bot-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-23, IoT-DS-1, and IoT-DS-2. As a conclusion from this study, CNN1D and CNN2D are highly effective in detecting anomalies in IoT networks, and this is due to their high levels of accuracy and performance. Thus, from the current and future perspectives, these models are very promising in building a solid structure for intrusion detection in the network of computers. Moreover, the authors recommend that future research should be directed along the lines of other deep learning approaches, such as FFN, RNN, and GAN, that are suitable for transforming this system into a high anomaly detection one to rise up to the challenges of the shifting paradigm in cyber security.

The authors of [7], evaluate different algorithms of anomaly detection and classification using the IoT-23 dataset. They found that, out of those, the Random Forest algorithm was most effective with an accuracy of 99.5% and precision. It can be seen that ANNs have biases toward classes with higher occurrences, possibly due to neuron weight configurations, and the Support Vector Machine turned in the poorest result at an accuracy of 60%—can't predict benign captures, but it turned in a relatively high recall rating. The study concludes that Random Forest is the best algorithm for detecting and classifying anomalies in the IoT-23 dataset, which was also revealed in the past by related studies, and proposes further research into the causes of high accuracy by simpler models and the potential of advanced neural networks to enable improved performance.

III. Utilizing ML techniques for IoT security

A. Various ML techniques to be considered

In the context of Internet of Things (IoT) security, various machine learning algorithms are employed to enhance anomaly detection and threat mitigation:

1) Artificial Neural Networks (ANNs): ANNs constitute computational models inspired by the human brain, which allow one to identify complex patterns within large datasets. ANNs perform well in IoT due to their inherent learning and adaptive capabilities in dynamic environments that make them fit for detecting sophisticated cyber threats.

2) Random Forest: Random Forest (RF) is an ensemble learning method where, during training, many decision trees are created and output the mode of their predictions for classification tasks. RF benefits IoT security through enhanced predictive accuracy and reduced over-fitting of intrusion detection systems, thus making them more reliable.

3) Extreme Gradient Boosting (XGBoost): XGBoost is a most refined ensemble method designed to combine the predictions of several weak models into a strong model. With the added ability to process large-scale and sparse data, it can very well be applied in IoT environments characterized by heterogeneous voluminous data.

4) Convolutional Neural Networks (CNNs): Though conventionally used for image and spatial data, CNNs have been adopted in IoT applications that analyze time series and sensor data. With their excellence in feature extraction and hierarchic learning, they can recognize complex patterns within streams of IoT data and thus improve anomaly detection capability. All of these algorithms offer robust tools to secure IoT networks against a wide array of cyber threats.

B. Considerations on how to apply ML to IoT

Application of machine learning in IoT ecosystems requires design considerations that take into account the unique characteristics and challenges of an IoT environment. The first consideration is related to data diversity and heterogeneity: IoT devices generate massive amounts of data which differ considerably by type, format, and quality. This calls for efficient preprocessing techniques that ensure consistency and reliability in this diverse data. Proper techniques—normalization of the data, noise reduction, handling missing values—are in order during the preparation of data for ML algorithms.

It considers the "resource constraints" of IoT devices. Most IoT devices have limited computational power, memory, and energy. Therefore, lightweight ML models, such as Decision Trees and optimized versions of more complex algorithms like Extreme Gradient Boosting, are more desirable. These models should be developed and implemented in a manner that keeps the consumption of resources as low as possible while maintaining high accuracy and performance.

Another critical factor is "Scalability". This is so because IoT networks can comprise hundreds or thousands of devices, each generating continuous data streams. For this reason, ML algorithms need to be scalable to handle this huge amount of data efficiently. Distributed computing and edge computing, where data processing happens closer to the source of data, may decrease problems of scalability by reducing latency and bandwidth usage for sending data to some central servers.

Real-time processing is essential for effective security in IoT devices. Given the dynamic nature of the environment in an IoT, to function effectively, the ML models have to be developed with real-time data analysis and threat detection capabilities. Algorithms such as CNN and ANN can be optimized for real-time inference that identifies anomalies and a reaction to intrusion promptly. Moreover, it is capable of using online learning methods so that it will keep updating the model whenever new data arrives to make it adapt to changes in patterns or newly emerging threats.

This will, therefore, make "robustness and resilience" the major priority in the face of adversarial attacks. Sophisticated cyberattacks against IoT devices constantly try to dupe these ML models. Techniques such as adversarial training enhance the robustness of ML models by training them using normal examples and adversarial examples. Techniques like RF can add another line of defense by fusing several models to

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.

increase detection accuracy and hence minimize successful attacks.

Lastly, there are critical considerations of "privacy and security of data". In many cases, IoT devices gather sensitive information, thus making the question of the privacy of data a serious one. It is possible to enhance privacy and security by training models using privacy-preserving machine learning techniques such as federated learning on decentralized data without having to move the raw data. In addition, ensuring compliance with data protection regulations and applying encryption procedures at all levels offers another layer for guaranteeing the integrity and confidentiality of data.

In other words, any effective application of ML to IoT would require a multi-dimensional approach to issues of data heterogeneity, resource-constrained devices, scalability, real-time processing, robustness to adversarial attacks, and data privacy. Provided that these challenges are taken into account, the design of effective and efficient ML solutions can be achieved through tailoring to meet the unique demands of IoT environments for bolstering security and functionality in IoT networks.

IV. Evaluation of the proposed Methodology

A. Evaluation Analysis Methods

To evaluate the performance of the aforementioned algorithms, we employed a set of established metrics, which will be discussed in detail in the 'Results' section. Before delving into these metrics, it is essential to introduce four fundamental concepts [1]:

- **True Positives (TP):** The number of actual positive instances correctly identified by the model.
- **True Negatives (TN):** The number of actual negative instances correctly identified by the model.
- **False Positives (FP):** The number of actual negative instances incorrectly identified as positive by the model.
- **False Negatives (FN):** The number of actual positive instances incorrectly identified as negative by the model.

1) Precision: Precision score is a metric used to evaluate the performance of a model by calculating the fraction of correctly identified positive instances. It is defined as the ratio of TP to the sum of TP and FP.

2) Accuracy: Accuracy score is a metric used to evaluate the performance of a model by calculating the fraction of correct predictions over the total number of predictions. It is defined as the ratio of the sum of TP and TN to the total number of instances, which includes TP, TN, FP, and FN.

3) Recall Score: Recall score is a metric used to evaluate the performance of a model by calculating the fraction of actual positive instances that were correctly identified. It is defined as the ratio of TPs to the sum of TPs and FN.

4) F-1 Score: The F1 score is a metric used to evaluate the performance of a model by combining precision and recall into a single measure. It is defined as the harmonic mean of precision and recall, providing a balance between the two metrics.

B. Evaluation Challanges

Working with this full IoT-23 dataset was quite a challenge throughout the entire data processing and machine learning pipeline, estimated to be of size 21 GB. It was considered necessary to do this at the level of "sifting through the data", where detailed effort is required for the identification and extraction of relevant information from the huge raw data. That was pretty labor-intensive given the huge volume and the diversity of the data types that comprise the IoT-23 dataset.

Organization of the data required that the data be structured coherently for analysis by focusing on data attributes and relationships so that efficient subsequent processing was achieved. Data cleaning regarded the usual problems of missing values, inconsistencies, and noise. Extensive pre-processing techniques were applied to ensure high data quality, including techniques for normalization, outlier detection, and data transformation. Training and validation of machine learning models on the large IoT-23 dataset were computationally intensive, sometimes taking 8 to 12 hours or more, even on high-end laptops. This procedure has been resource-intensive because of model complexity, data size, and requirements of runs against hyper-parameters to attain optimal performance. Much of the computational load was to be expected for the validation and testing of the model since hundreds of simulations against unknown data were needed to validate and test it for its robustness and accuracy. This has therefore entailed striking a balance between full validation and practical time constraints.

The handling of the full IoT-23 dataset was therefore a strict, demanding exercise both in careful data management and huge computational efforts to develop and validate the machine learning models. Despite these challenges, the success in processing and analyzing such a large dataset underpins the strength and effectiveness of the proposed methodologies in improving IoT security.

C. Details about Evaluation Related Data Processing

1) Data Analysis: In the IoT23 Dataset, there are a total of 61,721,382 observations and 2 classes which are Malicious and Benign, and each has 30,860,691 observations so the class ratio is 50/50. Below is the bar graph (Fig. 2a) of the class distribution:

2) Pre-Processing:

a) Data Splitting: Before preprocessing, we split the data into a train, test, and validation segment. We used 50% for training, 30% for testing, and 20% for validation. Below is the bar graph (Fig. 2b) of that distribution:

b) Missing Data Handling: Missing data handling means handling the missing values in a way that will not affect the prediction of the target in a bad way. For the IoT23 dataset, we handled the missing values by replacing the empty values of numerical features with 0 and there was a categorical feature named service which also contained empty values and had been populated with a value 'unknown'.

c) Data Scaling: Scaling is an effective normalization technique when working with a dataset that has continuous characteristics of several sizes. There are so many types of

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.

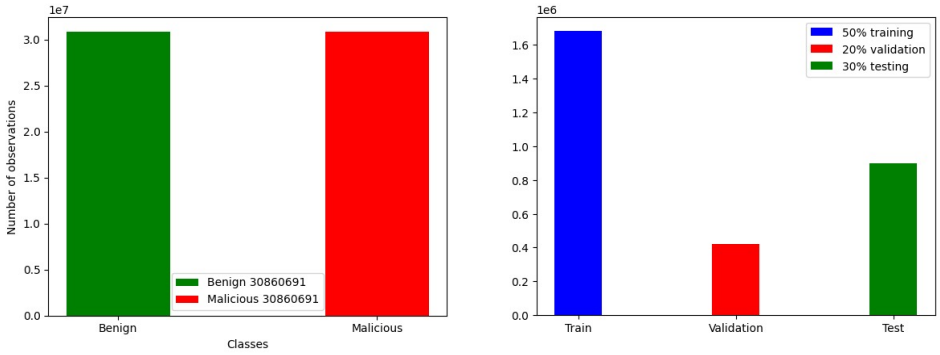

Fig. 2. a) Class distribution, b) Train Test Validation distribution

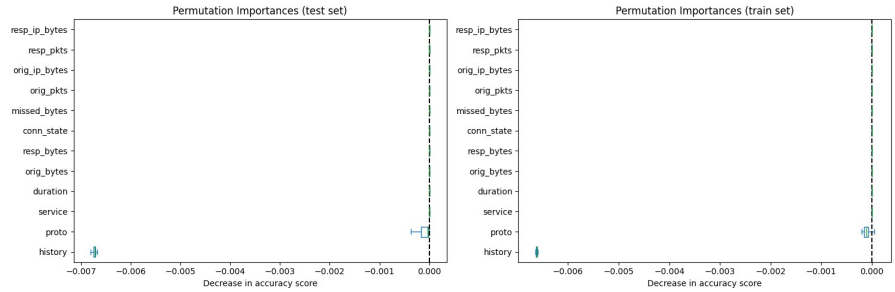

Fig. 3. Permutation Feature Importance Check indicating the Class Importance

data scaling methods like standardization, min-max scaling, data normalization, etc. For our dataset, we used min-max scaling. Below is the description of how the min-max scaler works:

- First, it finds out the minimum and maximum values of the column
- Then it subtracts the minimum value and divides it by the difference between the maximum and minimum value for every observation.

Below is the equation (Equation 1) of min-max scaling:

$$x_{\text{scaled}} = \frac{x - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}} \tag{1}$$

3) Feature Engineering: For feature engineering first, we extracted information like whether it is a global or a private IP from some of the IP Address columns that are not unique for every observation and used those extracted features as some new features and after that removed those IP Address columns because it will over-fit the model with training data which is not good for our model. There are some more ID columns and timestamp columns which are also removed because the values of those features are unique for every observation. After that, we used permutation importance to check the importance of the rest of the features and found that history has the least importance compared to the other features in both the training and testing dataset because it will not increase any error and on the most negative side so, we have removed that feature too. Above (see Fig. 3) is the graph of the permutation importance check:

We have also used one hot encoding for the categorical features which will convert it into 0 and 1 and it will also increase the number of features.

TABLE I
COMPARISON OF BOTH WORKS IN AN EXTENSIVE WAY

Model #	Paper	Accuracy	Precision	Recall	F1-Score
DNN/ ANN	paper-1	0.930	0.970	0.920	0.940
	ours	0.985	0.987	0.987	0.989
RF	paper-1	0.950	0.59	0.44	0.50
	ours	0.998	0.998	0.997	0.998
XG-Boost	paper-1	N/A	N/A	N/A	N/A
	ours	0.989	0.985	0.987	0.989
CNN	paper-1	N/A	N/A	N/A	N/A
	ours	0.995	0.990	0.990	0.995

D. Evaluation Results and Summary

Within the light of the evaluation results presented in Table I, our model performance was compared to the one reported in a referenced study [4], denoted as paper-1, which we observed an improvement in all metrics assessed. Its accuracy, precision, recall, and F1-score in the DNN(ANN) were 0.985, 0.987, 0.987, 0.989; against paper-1 scores of 0.930, 0.970, 0.920, and 0.940 correspondingly. That is a significant improvement of the model in detecting and classifying the anomalies occurring in the IoT networks (please observe the training/validation loss curve for our ANN implementation, see Fig. 4).

Our result also implemented the algorithm of RF, which gave very high scores of 0.998, 0.998, 0.997, and 0.998 in

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.

terms of accuracy, precision, recall, and F1-score, which were near perfect. This is very much different from inconsistencies seen in the paper-1 result, which reported 0.950 in accuracy and notably, the precision, recall, and F1-score values of 0.59, 0.44, and 0.50, respectively.

Especially for the ANN(DNN) and RF methods, the methodologies described in Feature Engineering (Section IV-C3) helped us to achieve significantly improved results when compared to paper-1.

Paper-1 did not implement XG-Boost and CNN, as opposed to our work. Our XG-Boost model resulted in an overall accuracy of 0.989, along with very promising precision, recall, and F1-scores of 0.985, 0.987, and 0.989, respectively. On the other hand, the CNN model resulted in better results, in an overall accuracy of 0.995, with precision, recall, and the harmonized F1-score around perfect, i.e., 0.990, 0.990, and 0.995, respectively (please observe the training/validation loss curve for our CNN implementation, see Fig. 5).

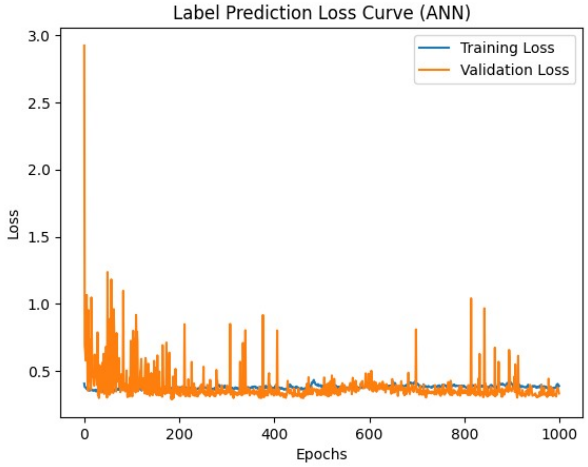

Fig. 4. Training loss vs Validation loss for ANN

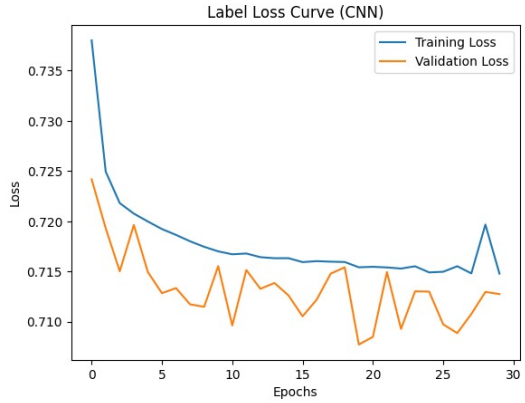

Fig. 5. Training loss vs Validation loss for CNN

V. Conclusions and Future Work

From Fig. 6, the ROC curve analysis of the designed and evaluated algorithms reveals that XGBoost outperforms the other methods. This is evident from its superior testing accuracy, precision, recall, and F1 score. Additionally, the ROC curve shows that XGBoost has an Area Under the ROC Curve (AUC) value of 1, which is the highest among the evaluated models. Thus, we can confidently conclude that XGBoost is our best-performing model.

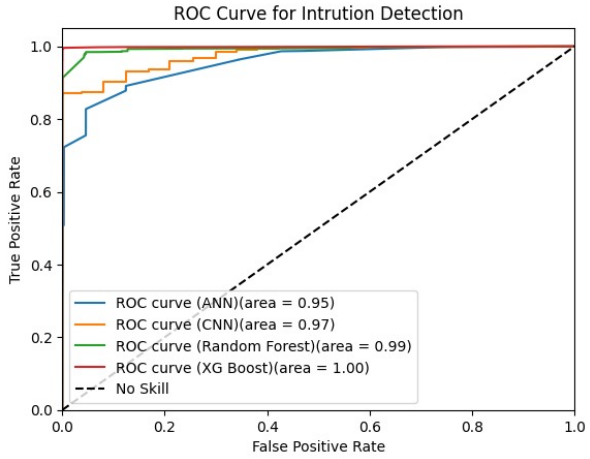

Fig. 6. ROC curve for all models

In conclusion, our results demonstrate the superior performance of our implementation methodologies in enhancing IoT network security through effective anomaly detection and threat mitigation.

Future work on this proposal might involve the application of DNN and, more importantly, also application of hybrid methodologies such as DNN and CNN mixed together, as well as the application of transfer learning methodologies.

Acknowledgement

This work is done in the Tecore Networks Laboratory at Florida Atlantic University (FAU) under the department of EECS and is funded by the Office of the Secretary of Defense (OSD), Grant Number W911NF2010300.

References

[1] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[2] Netgear, "2024 iot threat report," 2024, accessed: 2024-07-24. [Online]. Available: https://www.netgear.com/hub/network/2024-iot-threat-report/

[3] A. Parmisano, S. Garcia, and M. J. Erquiaga, "A labeled dataset with malicious and benign iot network traffic," *Stratosphere Laboratory: Praha, Czech Republic*, 2020.

[4] G. Bhandari, A. Lyth, A. Shalaginov, and T.-M. Grønli, "Distributed deep neural-network-based middleware for cyber-attacks detection in smart iot ecosystem: A novel framework and performance evaluation approach," *Electronics*, vol. 12, no. 2, p. 298, 2023.

[5] M. V. R. Sarobin, J. Ranjith, D. Ashwath, K. Vinithi, V. Khushi *et al.*, "Comparative analysis of various feature extraction methods on iot 2023," *Procedia Computer Science*, vol. 233, pp. 670–681, 2024.

[6] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in iot networks," *IEEE Access*, vol. 9, pp. 103 906–103 926, 2021.

[7] N.-A. Stoian, "Machine learning for anomaly detection in iot networks: Malware analysis on the iot-23 data set," B.S. thesis, University of Twente, 2020.

Authorized licensed use limited to: Florida Atlantic University. Downloaded on April 06,2025 at 17:42:04 UTC from IEEE Xplore. Restrictions apply.