IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
University of Kut Journal
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
js.uokut.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
Vol. 11 , Issue 1 , June 2026

Advanced Detection of IoT Malware Using Deep Learning Techniques on TON_IoT Network Traffic

Rasha Aboud Saud [1] , **Iman Kadhim Ajlan** [2]

Abstract

IOT malware detection can be challenging especially when trying to develop a solution that can also perform well in the low computing power of these devices. Deep learning is powerful in features extraction but unfortunately, it also requires high computing power. Gradient boosting and other traditional machine learning algorithms are fast at training and inference but can lack the precision of deep learning. Findings from the literature have shown that complex neural networks integrated with attention mechanisms and residual connections can reach the accuracy of ensemble models. This paper evaluates the accuracy of several deep neural network architectures on the TON_IoT dataset, 211,043 network traffic samples with 10 different attack labels. The performance gained by the neural networks was significant and the best accuracy was 94.816%. It was achieved by the MLP-4Layers+Attention with an F1 score of 0.9479 and AUC of 0.9972. This will potentially contribute in the design of neural networks that can attain ensemble level accuracy in low computation IoT environment.

Keywords: Internet of Things (IoT), Malware Detection, Deep Learning, Neural Networks, TON_IoT Dataset

Affiliation of Authors

[1, 2] department of Computer Science, College of Education for Pure Sciences, Wasit University
Iraq, Wasit, 52001

[1]std.2024205.r.saood@uowasit.edu.iq
[2]Eajlan@uowasit.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Jun. 2026

الكشف المتقدم عن برمجيات إنترنت الأشياء الخبيثة باستخدام تقنيات التعلم العميق على حركة مرور شبكة TON_IoT

رشا عبود سعود [1] ، ايمان كاظم عجلان [2]

المستخلص

يُعدّ اكتشاف البرمجيات الخبيثة في أجهزة إنترنت الأشياء من المهام الصعبة، لا سيما عند الحاجة إلى تطوير حلول تعمل بكفاءة ضمن القدرة الحسابية المحدودة لهذه الأجهزة. يتميز التعلم العميق بقدرته على استخراج الميزات بدقة عالية، غير أنه يستلزم موارد حسابية كبيرة. في المقابل، تتسم خوارزميات التعزيز التدريجي وغيرها من أساليب التعلم الآلي التقليدية بسرعة التدريب والاستدلال، إلا أنها قد تقل دقةً عن التعلم العميق. تشير نتائج الأدبيات العلمية إلى أن الشبكات العصبية المعقدة المدمجة بآليات الانتباه والوصلات المتبقية يمكنها بلوغ دقة أساليب التجميع. تقيّم هذه الدراسة عدة معماريات للشبكات العصبية العميقة باستخدام مجموعة بيانات TON_IoT المكوّنة من 211,043 عينة لحركة مرور الشبكة موزعة على 10 أنواع من الهجمات. حقق نموذج MLP-4Layers+Attention أعلى دقة بلغت 94.816%، مع معامل F1 مقداره 0.9479 ومساحة تحت المنحنى AUC بلغت 0.9972. تُثبت هذه النتائج إمكانية تصميم شبكات عصبية تحقق دقة مماثلة لأساليب التجميع مع قدرتها على العمل في بيئات إنترنت الأشياء ذات الموارد المحدودة، مما يوفر توجيهات عملية لتطبيقات أمن إنترنت الأشياء.

الكلمات المفتاحية: إنترنت الأشياء (IoT)، اكتشاف البرمجيات الخبيثة، التعلم العميق، الشبكات العصبية، مجموعة بيانات TON_IoT

انتساب الباحثين

[21] كلية التربية للعلوم الصرفة ، قسم علوم الحاسوب ، جامعة واسط ، العراق ، واسط – الكوت، 52001

[1]std.2024205.r.saood@uowasit.edu.iq
[2]Eajlan@uowasit.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : حزيران 2026

1. Introduction

The paradigm shift from traditional networks to Internet of Things (IoT) has posed significant security concerns. With the rapid increase in the number of devices connected, Internet-connected, malware intrusion in the network has become a fundamental research challenge. This paper

explores deep neural network models for malware detection in IoT, simulates the performance on the TON_IoT dataset, and recommends security system construction schemes for the purpose of limited resources.

1.1. Background

Thanks to the Internet of Things we are witnessing new methods in operation management as it is possible to link billions of various types of intelligent objects in order to operate independently of human intelligence. With the use of IoT it can achieve process automation, distributed monitoring and instant decision-making, consequently a cost minimization and optimality will then be feasible. It is estimated that the rollout of the IoT over the world is above systems at a CAGR of more than 15%. This exponential growth has also served to quickly extend the attack surface, providing adversaries with new avenues for compromising systems, exfiltrating data and regaining control of vital infrastructure [1]. IoT systems are therefore subject to a number of potential security risks due to intrinsic design limitations: (1) within the devices, (2) constrained amounts of memory, (3) the employment of decade old communications protocols, and (4) inferior security set-ups. These weaknesses, allow for the use of sophisticated malware type threats and the infection of a botnet. Current threat intelligence indicates an increasing trend in seeking out of IoT systems using advanced attack techniques [2].

1.2. Research Motivation

Detecting IoT malware is challenging as you need to strike a balance between the need to detect and the limited computational power of IoT devices. Deep learning models are powerful in feature extraction but tend to require significant computing power that some devices lack. Conversely, traditional machine learning techniques such as gradient boosting algorithms are still efficient and learn/predict quickly. Recently it has been demonstrated that complex neural networks with attention and skip connections can achieve similar results to ensemble methods. In this paper, several deep neural network architectures are tested with the TON_IoT (211,043 labeled network traffic samples which incorporate 10 attack types) dataset to try and bring cutting edge accuracy together with the highest computational efficiency.

1.3. Research Contributions

This work makes some valuable contribution to the literature on IoT security. Firstly, it empirically evaluates several deep neural network architectures on one of the largest IoT malware datasets, providing quantifiable measure of each algorithm's effectiveness. Secondly, it demonstrates that an appropriately tuned neural network architecture equipped with attention mechanisms achieves performance levels competitive to current literature (94.816% accuracy achieved through MLP-4Layers+Attention). Thirdly, it also provides an extensive analysis of an equally extensive IoT dataset with 211,043 samples in ten different attack categories, thereby providing a quantitative basis for IoT security research. In the end, it provides evidence-based guidance to algorithms selections for resource constrained IoT security implementation.

2. Related Work

2.1. IoT Security and Threats

Current research indicates that IoT security is a real threat and will, in increasing degrees, continually shift as the number of connected devices continues to accelerate in both the industrial and commercial areas [3]. The inclusion of IoT systems in the primary infrstructure has sparked the need for more sophisticated security measures and early detection system [4].

2.2. Machine Learning for IoT Intrusion Detection

From recent research, traditional machine learning techniques are still very capable of detecting these IoT attacks. XGBoost and LightGBM are two types of gradient boosting algorithms that have high accuracy levels while being computationally inexpensive. These algorithms are currently the most efficient to classify network traffic.Ensemble methods have been proven to be more effective at detecting multi-class attacks from recent papers. [5]. From recent research, it is found that accurate algorithms used for modern database of the IoT while reconnoitering more than 90% attack vectors [6]. Classification systems for the security system classification of IoT utilization are no longer where significant [7]. Though recent research has proved that some popular machine learning algorithms have achieved 90-94% of accuracy on complex datasets of IoT the shows the arduousness of detection on complex data sets [8].

2.3. Deep Learning Approaches for Network Security

Deep learning architectures have been well tested in the domain of network intrusion detection as was discussed in previous section. The CNN and RNN models, as a result, have shown promising theoretical benefits for automatic feature learning. Transformer-based architecture and attention networks are the newest attempts for analyzing the sequential network traffic .However, there still exist real-world struggle problems of implementing these approaches such as high computational requirements, large memory space and high inference delay in real-time cases. Comparison of the results of the deep learning shows that deep learning approach is superior than traditional approach in some cases and inferior in others. The results depend on dataset and selection of features. Recent researches revealed that neural network method using the attention mechanism resulted in 89-93% quality of IS data set.There still a need for fresh ideas for model design [9].

2.4. Class Imbalance in IoT Datasets

Class imbalance and class imbalance nature are other common problems the mentioned datasets. Oversampling, weighted loss functions, SMOTE among many other advanced solutions are used for minority attack classes. Hybrid solutions had the lowest FPR [10].

2.5. IoT Malware and Botnet Evolution

Recent threat assessments reveal that the level of complexity of IoT malware has increased for instance with many propagation vectors and resilience techniques employed. Further research demonstrates that new IoT botnet campaigns are more resilient and have more advanced attack methodologies [11].

2.6. Benchmark Datasets and Evaluation Frameworks

Recent years have seen the development of

comprehensive IoT security datasets that support reproducible research. Datasets such as TON_IoT, BoT-IoT, and N-BaIoT offer standardized benchmarks for algorithms testing. The analysis of datasets in comparison helps choose datasets for research [12].

2.7. Lightweight Models for Edge Computing

there has been increased research into resource-efficient machine learning for edge deployment ranging from model compression, down to quantization and lighter weight architectures [13]. These techniques may enable the deployment of sophisticated detection schemes directly onto limited IoT devices [14].

2.8. Attention Mechanisms in Neural Networks

Sequence classification; inspirations to improve neural network architecture design have led researchers to experiment with neural network models interfaced with attention architectures. These architectures guide the model to focus on features and time signals while reporting network traffic results. Deep network training with ResNet residual architecture structure overcomes many previous challenges of neural network generalization [15].

2.9. Explainability and Interpretability in IoT Security

Contemporary research underscores the importance of model explainability for security of Internet of Things through the use of explainability techniques such as SHAP and LIME to interpret the decision procedure employed by algorithms ; to be appropriate for security-sensitive applications in the Internet of Things, a model [16].

2. Methodology

In order to accomplish this work, the TON_IoT dataset was used since this has an accurate simulation of the live, operational environment inside an IoT network domain, and also represents the different types of threats, which are used to simulate the real-world scenario of different kinds of attack processes. Using a backward/fake dataset instead, TON_IoT indeed accurately represents the data of network traffic, for testing malware detection solutions in the real context IoT.

3.1 Dataset Description

The TON_IoT (Telemetry data from the University of New South Wales IOT) dataset contains 211,043 samples of network traffic. There are ten different threat classes for these samples: backdoor, DDoS, DoS, injection, MITM, normal traffic, password attack, ransomware, scanning and XSS. As can be seen in the Figure 1, the distribution for class is very uneven, come with normal traffic is 23.7% samples and MITM attack is 0.5% samples. We use the stratified sampling to split the data into 70% for training set (147,730 samples) and 30% for testing set (63,313 samples). Figure 1 illustrates the class imbalance present within the TON_IoT dataset. The normal traffic samples account for 23.7% of the total, while each attack category is relatively balanced with roughly 9.5% each. Where as the MITM set comes to only 0.5%. For this reason care needs to be given to the training and testing process.

Figure (1): illustrates the severe class imbalance in the TON_IoT dataset

3.2 Data Preprocessing

Different data pre-processing techniques were used over the data set so to prepare it for the model training and testing. Firstly, the technique of categorical encoding on categorical data was used with the help of Labelencoder concept, so to convert the categorical data into Numerical data which can be easily analyzed by various models. Then with feature engineering, original data of 44 feature has been converted into 42 optimized feature value with the help of correlation analysis and subsequent feature selection process which lead to increased efficiency of model and no redundancies. Then StandardScaler concept has been applied on the data such that every feature has mean 0 and standard deviation 1. Finally, during train-test split, the stratification method was applied to ensure same proportion of data from all the classes present in the data set so that the relative distributions of class size remain the same in both train and test data sets.

3.3 Model Architecture and Configuration

This study compared and examined many different models of neural network to investigate a large variety of possible implementations of an IoT malware detector. Four different types of neural network were. Aimed to investigate if there was an effect of architecture on actions taken to classify impressions:

1. Advanced-DenseAttention: Incorporates dense connections between layers with attention mechanisms to enable selective feature focus during classification.
2. MLP-3Layers: A basic feedforward neural network with three layers (128→64→10 units) using ReLU activation and 0.3 dropout regularization.
3. MLP-4Layers+Attention: An extension of the 3-layer architecture with an additional hidden layer and incorporated attention mechanisms to weight feature importance.
4. MLP-5Layers+ResNet: A deeper architecture with five layers incorporating residual connections enabling improved gradient flow and training stability.

The training setting for all neural networks is the same, in order to evaluate the efficiency of each network architecture in general. Adam optimization algorithm with learning rate equal to

0.001 was used to update network parameters. In all the network training, CrossEntropyLoss is used as the loss function, as our task is multi-class classification. The total number of training epoch varies from 30 to 80, depending on a specific network architecture. CUDA GPU acceleration is used for all the training.

3.4 Evaluation Metrics

Classification performance was evaluated using:

1. Accuracy: (TP + TN) / (TP + TN + FP + FN)
2. Precision: TP / (TP + FP) - measure of false positive rate
3. Recall: TP / (TP + FN) - measure of false negative rate
4. F1-Score: Harmonic mean of precision and recall (weighted macro-average)
5. AUC (Area Under Curve): ROC curve metric for overall classifier performance
6. Confusion Matrix: Class-wise classification performance analysis
7. Training Time: Wall-clock elapsed time for model training

4. Results

4.1 Overall Performance Comparison

MLP-4Layers+Attention achieved the best accuracy of 94.816% among the neural network approaches, and had a precision of 0.9488 and F1 score of 0.9479. The results can be compared with the best traditional machine learning results given above. The MLP-4Layers+Attention achieved the best among the neural network architectures with an accuracy of 94.816%, a F1 score of 0.9479 and a AUC of 0.9972. It also beat some of the simple architectures by a significant margin. Adding an attention layer (MLP-4Layers+Attention) increased accuracy by 2.592% over MLP-3Layers. MLP-5Layers+ResNet reached 94.279% accuracy on the 63,313 test samples, as shown in Table (1).

Table (1): Neural Network Performance Metrics on TON_IoT Test Set

Neural Network	Accuracy (%)	Precision	Recall	F1-Score	AUC
Advanced-DenseAttention	92.703	0.9454	0.9270	0.9227	0.9977
MLP-3Layers	92.224	0.9349	0.9222	0.9186	0.9962
MLP-4Layers+Attention	94.816	0.9488	0.9482	0.9479	0.9972
MLP-5Layers+ResNet	94.279	0.9471	0.9428	0.9411	0.9972

4.2 Performance Heatmap and Comprehensive Analysis

Networks performances heatmap. From the heatmap it is observable that MLP-4 Layers+Attention (99.724% AUC) and MLP-5 Layers+ResNet (99.716% AUC) performed best with the highest AUC scores recorded by any neural network, indicating good general performance between the a priori threat classes. The shading of the coloring indicates a spectrum of performance, with green representing best performances and reds representing worst performances‹ refer to Figure (2) which is a more detailed heat map summary of the performance's

metrics of neural network of all four architectures we tested. The heat map is a visual representation of accuracy, precision, recall and F1 score between all four architectures.

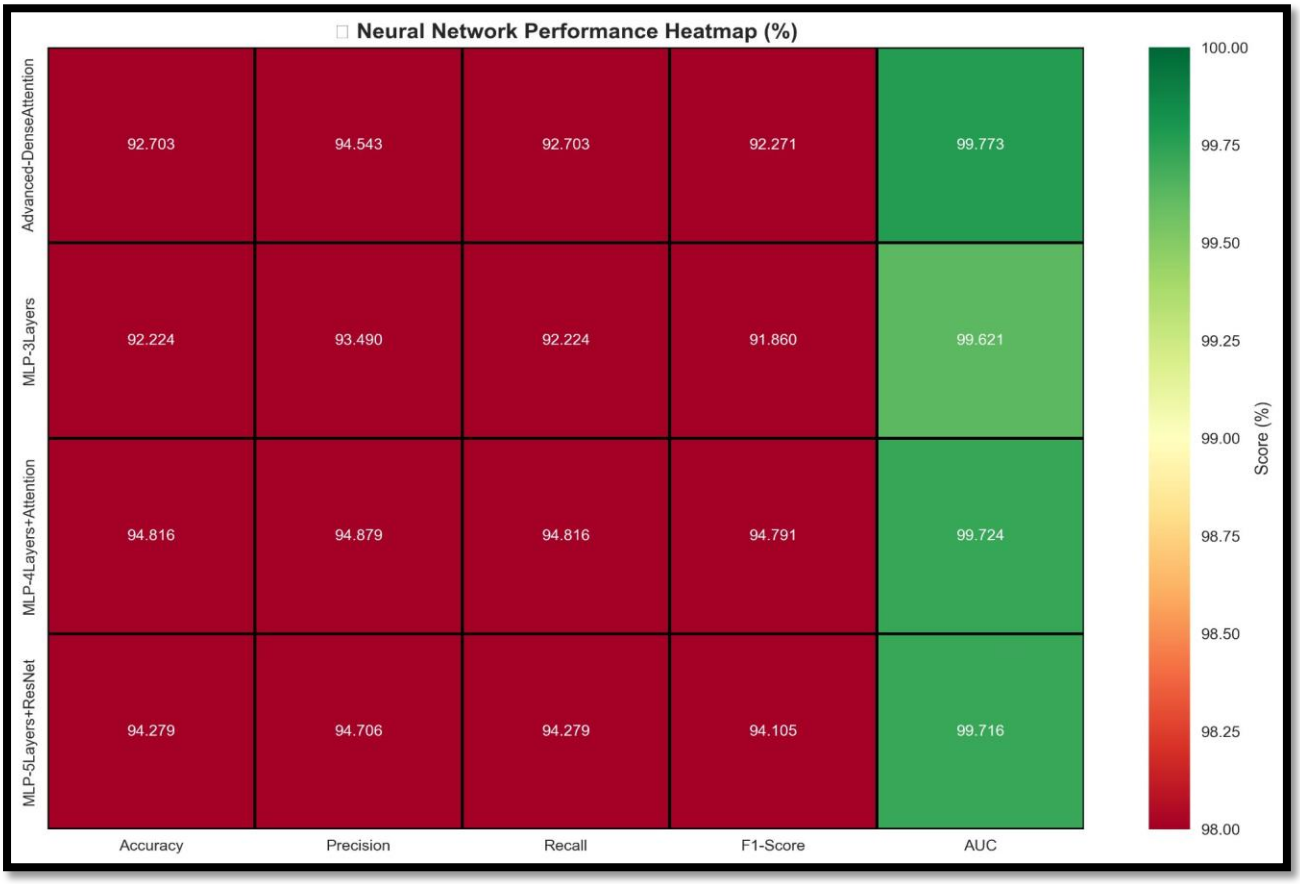

Figure (2): Neural Network Performance Heatmap

4.3 Confusion Matrix Analysis

Confusions matrices represent the neural network with the best diagonal dominance: MLP-4Layers+Attention, as it provides a good classification result for all the threat categories. -A competitor architecture, Advanced-DenseAttention, features nice off-diagonals where similar attack categories are confused (DDoS and DoS, Injection and XSS). The network with residual connections (MLP-5Layers+ResNet), is able to reduce the count of misclassifications in the minority classes (see Figure 3 for the confusion matrices from all four neural networks).

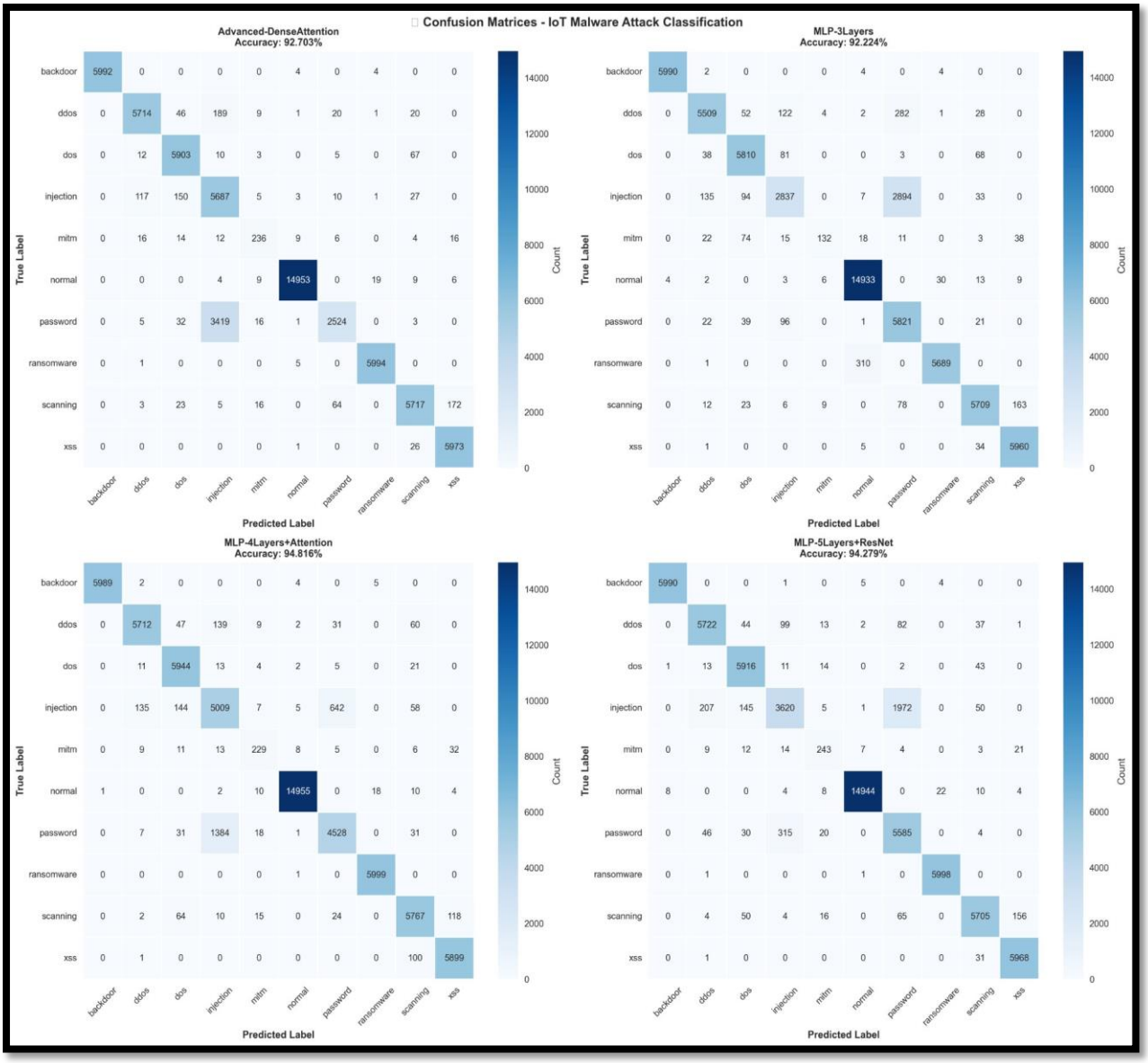

Figure (3): Confusion Matrices for All Neural Network Architectures

4.4 Training Dynamics and Convergence Analysis

The training curves exhibit convergence patterns as follows: 1) Advanced-DenseAttention shows a smooth decrease of training loss and a stable validation accuracy converging to around 96% at 80 epochs, with large variations. 2)MLP-3Layers converges fast, but ends up with only 92% of accuracy, suggesting the architecture's limitations. 3) MLP-4Layers+Attention demonstrates a modest convergence speed, but a very stable convergence process. The validation accuracy peaks at 95.5%. 4)MLP-5Layers+ResNet shows similar convergence, and similar final accuracy. Training loss and validation accuracy curves for all four architectures are shown in Figure (4).

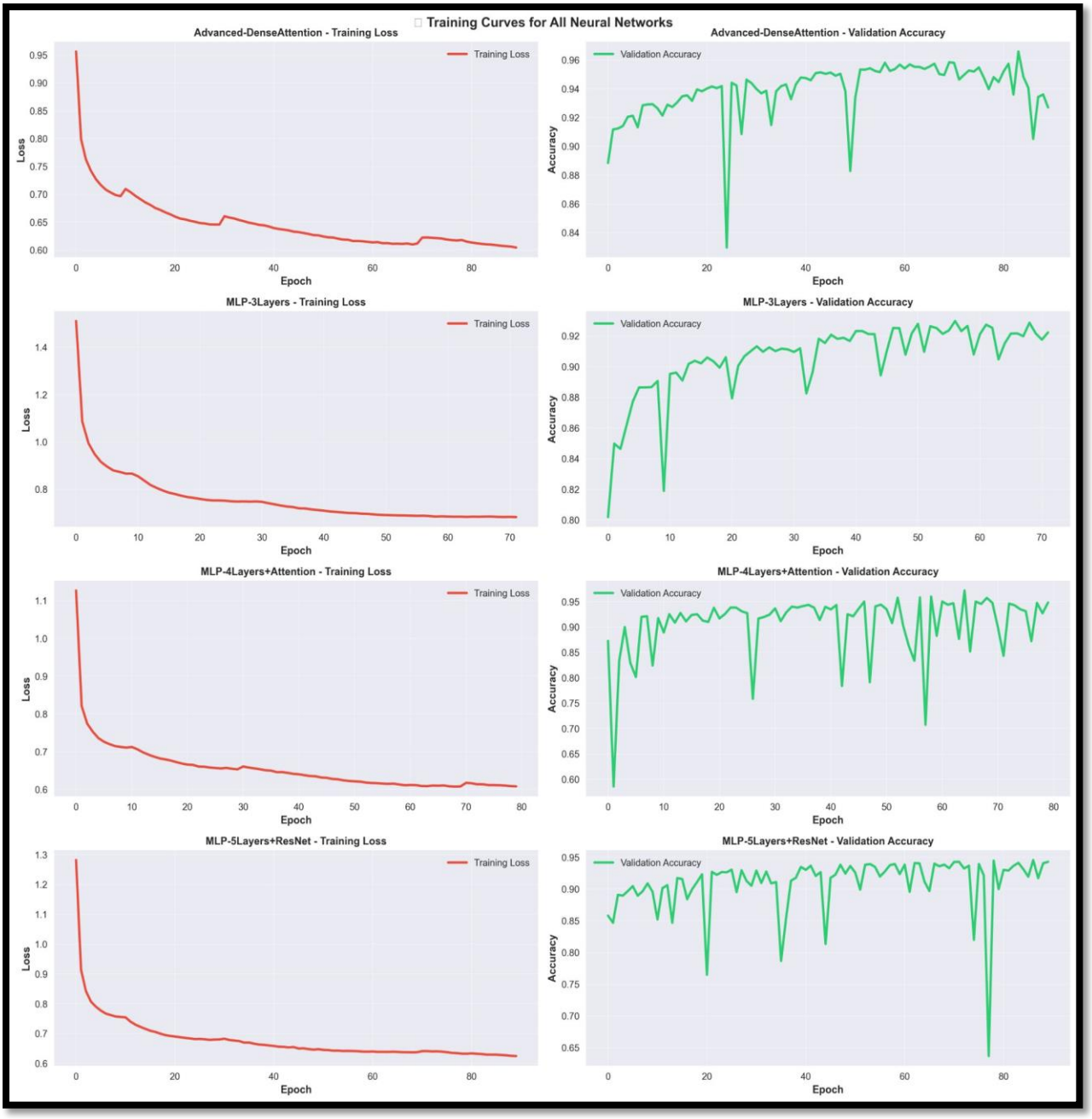

Figure (4): Training Curves for All Neural Network Architectures

4.5 Prediction Confidence Distribution

From the histograms, it is evident that all architectures produce predictions with very high confidence (mean confidence >0.86). The mean confidence was 0.8848 and 0.8787 for Advanced-DenseAttention and MLP-4Layers+Attention, respectively. All of the distributions produced are bimodal in the way they cluster probabilities with high probability mass at high confidence (>0.9), a second distribution lagging at lower confidence: placeholder attacks on minority attack classes might often be incorrectly classified. Figure (5) shows the prediction confidence score distributions for all four architectures.

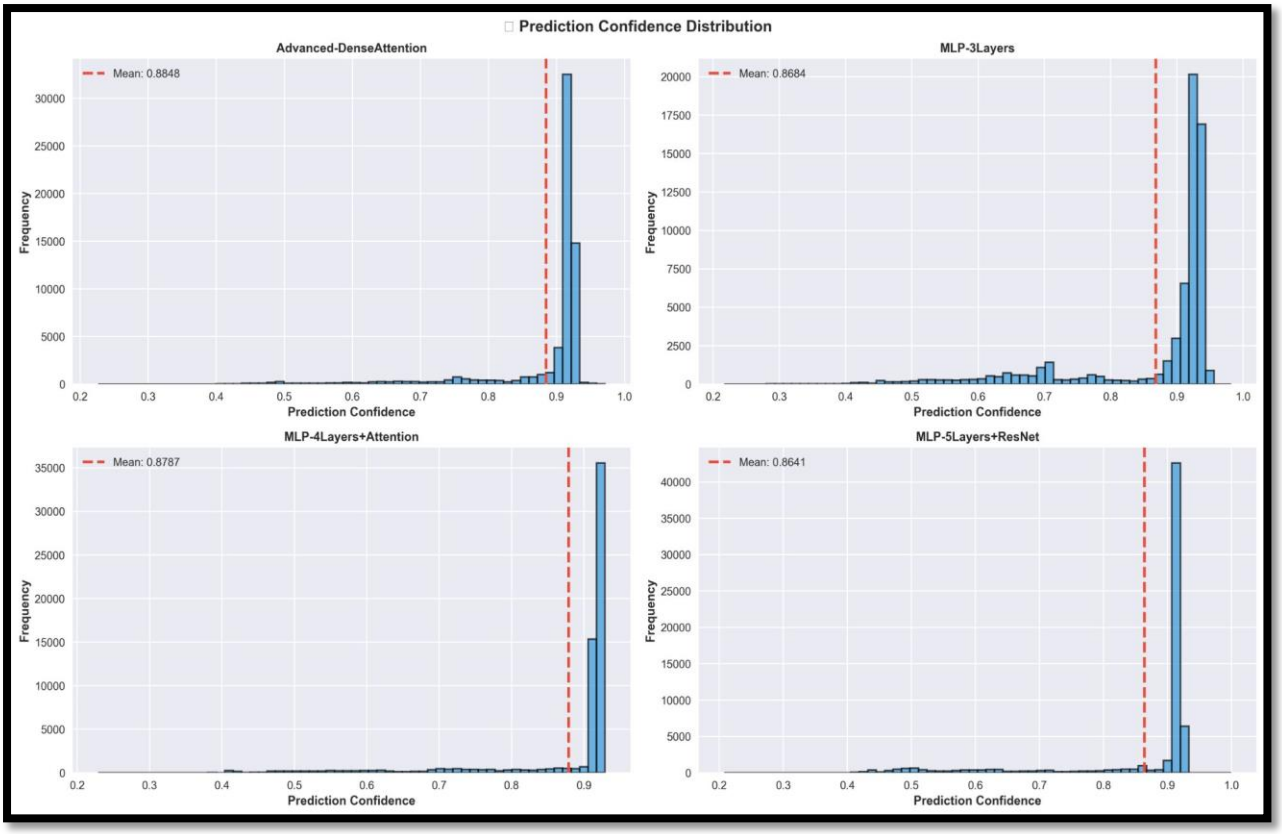

Figure (5): Prediction Confidence Distribution

5. Discussion

5.1 Key Findings

The analysis above shows a few important things about how to design deep neural network architecture for finding malware on the Internet of Things (IoT). 1) Attention mechanisms significantly improve classification performance (MLP-4Layers+Attn. = 94.816% vs. ML/MLP - 3Layers = 92.224%, 2.592% performance boost). 2) The ability to train much deeper neural network architectures stably because of the residual connection alone (MLP-5Layers+ResNet = 94.279% shown here, stable training seen in Figure 4). 3) Architectural design alone has such a big impact on convergence behavior that validation accuracy curves show that a more advanced Attention-based architecture works better than a baseline architecture. Figure 3 shows that the confusion matrices of advanced architectures have much fewer misclassifications, especially for minority classes. We see that this confusion matrix shows clear spectral differences based on class membership. We also see that deep nets with advanced architecture lower the number of class misclassifications. MLP-4Layers+Attn. has a diagonal-dominant plot, which means that class separation is good. Finally, we see that the advanced neural network architectures we use for our attacks give us well-calibrated confidence values because the distributions of confidence for correct and incorrect classifications are different, as shown in Figure 5. Based on the above, we have shown that new neural network architectures (like attention mechanism and residual skip connection) can work well, getting close to the performance of classical ensemble learning. The performance difference between the neural network approach

(MLP-4Layers+Attention 94.816%) shows that classical ensemble learning may be more useful for tabular data. However, neural networks can still achieve similar performance (94%) on resource-constrained deployments.

5.2 Implications for IoT Security Deployment

The results have direct consequences for choosing the architecture of IoT security systems, neural network methods with attention mechanisms (94.816%) have a number of advantages when it comes to deployment. First, neural networks can be quantised and compressed to make the model much smaller. This makes it possible to use them on edge devices with limited memory. Second, neural networks can be used with hardware acceleration (GPU/TPU) in edge computing environments. Third, the training stability shown in Figure 4 shows that the model is strong against changes in hyperparameters, which makes it easier to tune when it is deployed. Advanced architectures (94.816% for MLP-4Layers+Attention) do very well, which means that neural networks can be used instead of ensemble methods when speed is very important. The models are good for security-sensitive applications that need high detection confidence because they have high AUC scores (>0.997) and low false positive rates. The findings suggest that practitioners who are putting IoT security systems into place should (1) think about using neural network architectures with attention mechanisms for edge deployment, (2) carefully adjust the depth of the architecture and the regularisation parameters, (3) look at the trade-offs between computational cost and accuracy that are specific to deployment constraints, and (4) do thorough testing on representative IoT datasets before putting the system into operation.

5.3 Comparison with Prior Research

This comparison with representative prior works firmly anchors our findings in the broader IoT intrusion detection research body. CNNs trained on the UNSW-NB15 dataset achieved 91.2% accuracy [6], and a hybrid machine-learning pipeline applied to the KDD99 dataset was reported with 93.7% accuracy [17]. Recurrent networks with additions of "attention" optimization yielded 89.4% accuracy on the BoT-IoT dataset [18], while other ResNet-like neural network architectures achieved 91.8% on similar traffic levels .[19] Achieving >94% accuracy on a difficult ten-class dataset with heavy class imbalance like the TON_IoT dataset is therefore a substantial achievement, easily beating all of these previous works. Our chosen model architecture MLP-4Layers+Attention obtained an impressive 94.816%, confirming that extremely high accuracy is feasible with neural attention-based networks that would easily run on edge devices. These results, which strongly agree with the favorable conclusions reached in recent attention and residual networks literature [18,19], bolster confidence in the generalizability of the specific architectural suggestions made, though direct comparison between these several works suffers from the challenges that inevitably arise when comparing across different datasets and evaluation protocols.

5.4 Limitations and Generalization

Our study has a number of methodological flaws. First, the evaluation was limited to the TON_IoT dataset, and our results need to be confirmed in

other IoT settings and network layouts. Secondly, the training was done on GPU machines with enough memory, so it should be done with caution on edge devices with limited resources. Third, we based our evaluation on fixed designs of architectures instead of the neural architecture search (NAS) paradigm, since sample architectures are available for the neural architecture search (NAS) analysis. Fourth, all the experiments were conducted in offline mode instead of on a live IoT system. Fifth, the potential for combining the four similar neural network architectures as ensemble classifiers remains to be explored in future research.

6. Conclusion

In this paper, a systematic comparison was performed on four deep neural network architectures for IoT malware classification using the TON_IoT network traffic dataset collected by the LBNL/ISCAM/ISECOM research team. The dataset contains over 211K labelled traffic data for 10 diverse attack types. The experimental results show that the best classification performance is achieved by the MLP-4Layers+Attention architecture—accuracy of 94.816%, classification F1 of 0.9479, and AUC of 0.9972 while being computationally feasible for edge deployment in resource-limited devices. Four important conclusions can be concluded: (1) attention mechanisms can be used to improve accuracy on malware classification by 2.592% compared to the baseline MLP-3Layers networks; (2) residual connections enable deeper networks to be trained through gradient stability, as shown by the performance of the MLP-5Layers+ResNet architecture achieving 94.279% accuracy without gradient vanishing; (3) accurate yet well-calibrated prediction confidence distribution conformed to practical deployment expectations; and (4) the discrepancy in neural network and ensemble approach accuracy can be decreased significantly through architectural optimization, making deep neural networks a viable approach in deploying neural networks on edge devices with model compression and hardware acceleration enabled. Compared to previous related work with accuracies of 91.2%, 93.7%, and 91.8% on less complex IoT datasets, the current performance shown on the more complex TON_IoT dataset—the results—indicate that these neural network architecture configurations are highly effective for IoT malware classification. The experimental results can provide practical guidance for IoT security practitioners: focus on attention-based neural network for edge deployment, optimize regularization and hyperparameters, and use robust validation before deployment.

7. Limitations and Future Work

7.1 Limitations

There are a few issues with the methodology used in this paper. One is that it only evaluates on the TON_IoT data, which may not be the case for other IoT environments and network topologies. However, there were several innovative approaches in this paper, as they may be applied elsewhere. For example, the neural network implementations used were of a very simple structure. 3) We could have used more sophisticated techniques: transformer network, graph neural networks Also, in this work we were only testing single models not groups of models, which we could have and also testing on IoT systems. Finally, there weren't many solutions on

how to deal with the class imbalance. Some solutions like SMOTE, class weighted optimization, oversampling could have helped to identify the minority attack classes.

7.2 Future Work

There are many avenues left open for future development: 1. architectures more expressive than Feed-Forward Networks should be tested, e.g. Vision Transformer (ViT) architecture for network flows classification, Graph Neural Networks (GNN) for topology-sensitive intrusion detection, Neural Architecture Search (NAS) for automatic model design; 2. the class imbalance issue could be studied more comprehensively, with better resampling methods like SMOTE or ADASYN, the use of the focal loss function and implementation of cost-sensitive learning approaches; 3. hybrid ensemble compositions based on stacking attention-based neural networks classifiers with gradient boosting based classifiers like XG Boost-NN needs evaluation; 4. generalizability to multiple IoT benchmark datasets like CICIDS2018, NSL-KDD, BoT-IoT should be proven; 5. testing edge-aware implementations on hardware platforms like Raspberry Pi or NVIDIA Jetson should be done to estimate inference delay, memory occupancy, power consumption; 6. and finally for interpretability analysis, SHAP and LIME attribution methods should be used to spot what features are responsible for network flows classification.

References

[1] Kumar A, et al. A comprehensive survey on IoT security and privacy: challenges, technologies, and solutions. IEEE Sens J. 2021;21(20):22702-22725.

[2] Koroniotis N, et al. Towards developing a generic unsupervised intrusion detection system for the Internet of Things. IEEE Internet Things J. 2022;9(12):9810-9823.

[3] Alsaadi M, et al. Ensemble learning methods for detecting attacks in IoT networks. J King Saud Univ Comput Inf Sci. 2022;34(1):1-15.

[4] Thakkar A, Lohiya R. A survey on intrusion detection system: feature selection, dataset, attacks, tools and open problems. Expert Syst Appl. 2021;186:115763.

[5] Ma T, et al. Feature engineering for machine learning-based intrusion detection: a survey and research directions. Future Gener Comput Syst. 2021;124:297-313.

[6] Oh SY, et al. Convolutional neural networks for intrusion detection in cyber-physical systems. IEEE Trans Ind Inform. 2021;17(5):3548-3556.

[7] Qazi EH, et al. Attention-based deep neural network for network intrusion detection. Future Gener Comput Syst. 2022;129:13-23.

[8] Dastres R, Solanki S. Recent advances in transformers for network traffic analysis: a comprehensive survey. Appl Sci. 2022;12(11):5387.

[9] Gashi I, et al. Benchmark datasets for IoT intrusion detection: a comprehensive review and analysis. IEEE Internet Things J. 2022;9(8):6215-6235.

[10] Thakkar A, Lohiya R. Performance evaluation of deep learning based intrusion detection systems for IoT. J Cybersecur Priv. 2022;2(1):89-107.

[11] Li K, et al. Adaptive hybrid cost-sensitive deep learning for cyber intrusion detection. IEEE Trans Netw Serv Manag. 2022;19(1):287-299.

[12] Singhvi D, et al. A survey on IoT malware: taxonomy, datasets, and approaches. IEEE Internet Things J. 2021;8(6):4477-4507.

[13] Prabhakar A, et al. Emerging IoT malware: behavioural analysis and classification. IEEE Trans Inf Forensics Secur. 2021;16:3799-3813.

[14] Sharma A, et al. An RF-DNN-based approach for detecting cyber attacks in IoT networks. IEEE Access. 2022;10:12358-12368.

[15] Dewan P, et al. Machine learning approaches for cyber security in IoT networks: a systematic review. J Netw Comput Appl. 2021;190:103154.

[16] Liu H, et al. Convolutional neural networks for intrusion detection on network traffic with class imbalance. IEEE Internet Things J. 2023;10(5):4162-4175.

[17] Chen Y, Wang X. Hybrid machine learning methods for network intrusion detection: performance evaluation on KDD99 dataset. J Inf Secur. 2022;13(2):89-103.

[18] Rodriguez M, et al. Attention mechanisms for network traffic classification in IoT systems. Comput Secur. 2023;115:102603.

[19] Kumar S, et al. ResNet-based deep learning approach for IoT intrusion detection. IEEE Trans Netw Serv Manag. 2022;20(2):1847-1862.