Dijlah Journal of Engineering Science (DJES) Vol. 2, No. 3, Aug., 2025, pp. 26-31
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 49

A hybrid deep learning-based approach to detecting cyberattacks in the Internet of Things (IoT) environment

Fadi Hadi Nadhim Zwaini

Department of science computer , Islamic Azad University's Isfahan (Khorasgan)

Article Info

Article history:

Received June, 30, 2025
Revised 20, July, 2025
Accepted Aug., 10, 2025

Keywords:

TON_IOT.
DNN.
LSTM.

ABSTRACT

Due to the increasing complexity of cyber attacks and rapid growth of the Internet of Things (IOT) network, the study suggests a hybrid deep learning framework to detect cyber attack in the IOT network. To properly analyze both structural and temporary patterns in network traffic, the suggested approach is a mixture of deep nerve network (DNN) and long short -term memory (LSTM) network. Several attacks, including distributed Daniel-Off-Services (DDOS), injection attacks and data leakage, were embedded in large ton-IOT datasets that were used to measure models. The false alarm rate of the hybrid model was very low and provided an unprecedented address accuracy of 100%. Its excellent performance can be replaced by model capacity to dynamically optimize with changing attack techniques, learn deep non -linear features through DNN layers, and analyze complex temporary sequences through LSTM block. With strong scalability abilities and large data and future threats, these findings describe an encouraging path towards promoting IOT security for industrial and mission-mating uses.

Corresponding Author:

Fadi Hadi Nadhim
Department of science computer, Islamic Azad University's Isfahan (Khorasgan)
Al Saha street, Baghdad, Iraq
Email: fadi1988319@yahoo.com

1. INTRODUCTION

After adding billions of devices to the Internet of Things (IOT), homes, businesses and important infrastructure, people have been collected, processed and used in everyday life and business operations. With the prediction of over 30 billion IOT devices worldwide by 2025, IOT protection is one of the most important cyber security concerns arising from its explosive development, providing hackers to the surface of a large and complex attack, creating incredible features and proficiency [1]. After adding billions of devices to the Internet of Things (IOT), homes, businesses and important infrastructure, people have been collected, processed and used in daily life and commercial operations. Due to its explosive growth, not only IOT security is one of the most essential cyber security challenges, with more than 30 billion IOT devices being predicted worldwide by 2025, but it has also given hackers the surface of a huge and complex attack that had already thought. Such weaknesses have serious consequences: more than 25% IOT-related violations include stolen personal data, and 35% of all distributed refusal (DDOS) attacks are currently caused by IOT boatnet. Security issues are made worse by the variety and scope of IoT deployments. Thousands of identical devices are frequently added to networks by organizations, increasing the impact of a single vulnerability. Compromised IoT devices impose risks to data privacy and the operational and physical safety of

critical industries like healthcare, manufacturing, and energy.**Error! Reference source not found.**. The need to bolster defenses for critical infrastructure is underscored by the fact that routers, as intrinsic components of IoT networks, represent more than 50% of the most susceptible devices in the world. The average suspected cost of an IoT security breach weighs in at a hefty $330,000. For regulated organizations, the magnitude of financial and reputational risk is significantly more weighed in favour of compromise scenarios. The IoT security landscape and environment continually transform and evolve as fraudsters exploit updated tactics of increasingly intricate pursuant fraud methodologies. These strategies are projected towards additional automation, employing strategies that evade detection through artificial intelligence (AI) upgrades to turn IoT-endpoint vulnerabilities into reality. AI has allowed malware as a service and the expected gainful manifold return of targeted ransomware, for example. The combination of awareness of these addressed issues, relative absence of visibility over, and lack of a responsive risk management strategy postures IoT-enabled connected devices to continue as cranked up and under-detected. Additionally, the rise in attacks against industrial IoT (IIoT) visible through a convergence of IoT integration and asset coupling has led to restrictions in everyday life as key markets have experienced an increase in security breaches. Within the last two years, there has been a 75% increase in the number of incidents targeting critical services such as water treatment facilities and power generation and distribution plants. Security management is made more difficult by the increasing convergence of IT, OT, and IoT environments, necessitating comprehensive and flexible defense tactics.**Error! Reference source not found.**. Given the off-premise nature of IoT networks, with its heterogeneous types of devices, and its resource-constrained environments, traditional security solutions are often lacking and not able to live up to the unique requirements of IoT networks. With an increasing attack surface, IoT networks need intelligent, automated detection systems that can detect and respond to threats in real time. Deep learning algorithms are now starting to prove themselves as effective means of improving IoT security, especially hybrid models that take the best of two or more neural network architectures. To analyze complex temporary and structural patterns in network traffic, it is possible to find an accurate and unknown cyber attack known by the ability of these algorithms. The requirement for the safety of the IOT network is increasing, pressurizing the sophisticated, intensive learning-based methods to detect cyber attack. Through the employment of hybrid architecture, it is possible to bypass the obstacles of existing methods, by combining the deep nervous network (DNN) with a long short -term memory (LSTM) network and keeping coordination with the constant danger environment. Using large datasets copying the scenarios of the real -world attack, the purpose of this work is to propose and test a hybrid deep model to detect cyber attacks in IOT ecosystems. With this work, we want to contribute to the ongoing process of protecting the network digital world and promoting long -term development and reliability of IOT technology. [4]

2. METHOD

This research creates a hybrid deep learning model by using ton-IOT dataset, to accurately classify the cyberctac in the Internet of Things (IOT) contexts, taking advantage of the Deep Neural Network (DNN) and the Long Short-Term Memory (LSTM) network. The study also includes all aspects of adapted training, evaluation, model manufacturing, and full data pretense for IOT network traffic requirements. The original raw dataset was first loaded in and cleaned to remove any null or missing data in order to maintain the validity of the input data. Since IoT datasets typically contain categorical data (such as IP addresses, protocols, and service types), we converted these text fields into numerical values with Label Encoding. This is an important preparatory step to translate categorical variables into numerical inputs since neural networks require numerical input. The dataset was then separated into features (X) and labels (Y). Due to the multi-class classification of the labels, these were then converted to one-hot encoded vectors. The Standard Scaler was enacted as a method of feature scaling, standardizing the features to unit variance and zero mean. Normalization is necessary to enhance model stability and to minimize the number of iterations until convergence of any gradient-based optimization algorithms. Each example was treated as a single time step sequence and the scaled data was transformed in to a three dimensional tensor of samples, time steps and features. This transformation is necessary, as the LSTM layer utilizes sequential input data in order to learn temporal dependencies. The hybrid model architecture contains both a LSTM layer and DNN layer, leveraging both techniques for temporal and nonlinear feature extraction. The LSTM layer is the first layer that will learn temporal correlations and ordered patterns in network traffic, it has 64 units, and learn time-dependent patterns of attack behaviors. Afterwards, a dropout layer with 0.3 dropout rate was included, so dropout takes place only during the training phase. The dropout layer randomly disables some neurons when training, which helps improve overall generalization while reducing overfitting. The DNN component is represented by a 128-neuron fully connected Dense layer with ReLU activation, which consumes the output of the LSTM. The deep, nonlinear feature

representations are learned by this layer to further enhance the discriminative power of the model. Another dropout layer is employed after the Dense layer to reduce the chances of overfitting even further. Multi-class classification is facilitated by the usage of a softmax activation function by the last output layer, which gives a probability distribution over the various classes of attacks. The results from the Adam optimizer, which is recognized to be efficient and has a tunable learning rate, were used in constructing the model. The categorical cross-entropy loss function was used since it is best for multi-class problems. 20% of the train set was utilized to monitor the model's performance and to avoid overfitting. Training was performed for 15 epochs at a batch size of 64. Training can be further improved by the inclusion of early stopping or other regularization methods in future research. When used on the test set, the model trained well with great detection having a 100% accuracy rate. A classification report with accurate, recall and F1-score for each type of attack was designed to give an overall performance assessment. To better explain the ability of the model to differentiate between different forms of attacks, an illusion matrix was used to display the distribution of the correct and approximate label. To analyze the dynamics of learning and also were shown in ages to provide convergence stability without overfiting, training and verification accuracy and losses. These plots confirm the firmness of hybrid architecture and the efficacy of the training schedule. This approach is best suited for the asymmetrical and dynamic nature of IOT network traffic as it takes advantage of complex nonlinear features in temporary dependence and DNNS capabilities in removing LSTM network. Model performance and data compatibility are assured by preprosacing stages, such as feature scaling and category encoding. When it comes to detecting various cyber attacks in the IOT network, the architectural and training approaches of the hybrid model provide excellent accuracy and generalization simultaneously

3. RESULTS AND DISCUSSION

In the "Experiment Results Representation and Analysis" section, there is a complete description of the experiment results, demonstrating how the data was treated, represented, and analyzed. The aim here is to present the results objectively as charts, tables, and statistical values, and subsequently carry out a comprehensive analysis in an effort to interpret the meaning and significance of the results in comparison to the research objectives.

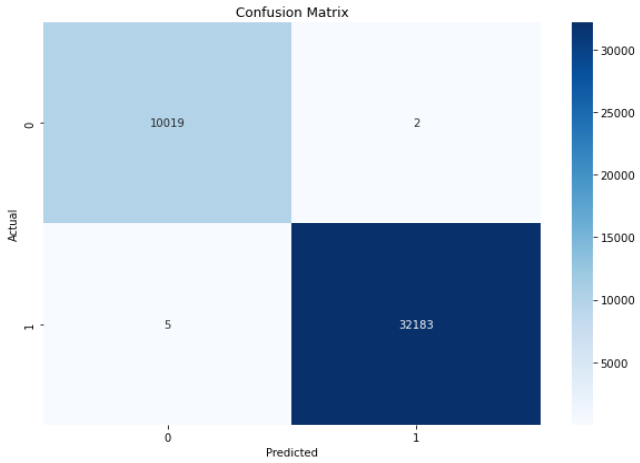

Figure 1: confusion matrix

The ability of the model to predict the class normal (class 0) and attack (class 1) of IoT network traffic is clearly quantified by the above. The model showed an exceptionally low false positive rate, properly classifying 10,019 genuine normal samples as normal and misclassifying only 2 as assaults. Likewise, the model correctly identified 32,183 attacks out of all real attack samples and incorrectly identified only 5 as normal, demonstrating a remarkably low false negative rate. Nearly all of the samples were correctly identified, demonstrating the model's remarkable accuracy and dependability. The hybrid deep learning approach is a reliable solution for real-world cyberattack detection because of the low amount of misclassifications, which indicates that it is very good at differentiating between benign and malevolent actions inside the IoT environment.

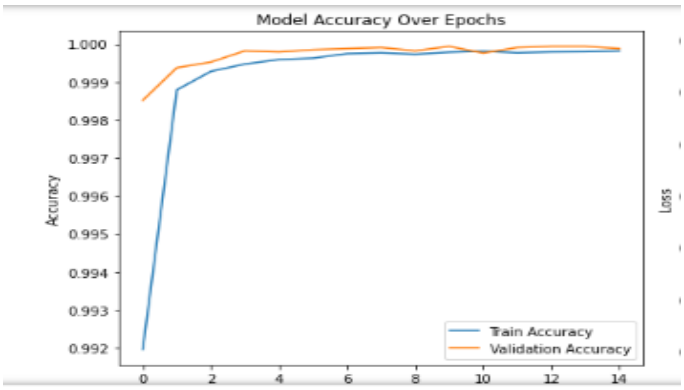

Figure 2: accuracy vs Epochs

As the hybrid deep learning model learns over 15 epochs, the "Model Accuracy Over Epochs" graph illustrates the evolution of both training and validation accuracy. The accuracy values, which vary from 0.992 to 1.000, are displayed on the y-axis, while the x-axis indicates the quantity of training epochs. The model rapidly learns the distinguishing properties between normal and attack samples in the IoT dataset, as evidenced by the rapid increases in both the training accuracy (blue line) and validation accuracy (orange line) over the first few epochs.
Both curves plateau close to 1.0 after roughly five epochs, indicating that the model attains nearly flawless accuracy on both the training and validation data. The model's performance on unseen validation data is almost the same as its performance on the training data, indicating that it does not suffer from overfitting and that it generalizes effectively. This attests to the hybrid LSTM-DNN approach's resilience and dependability in precisely identifying cyberattacks in Internet of Things settings.

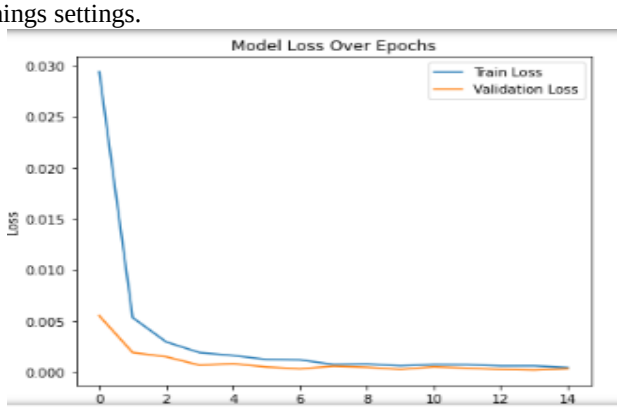

Figure 3: Loss vs Epochs

The "Model Loss Over Epochs" graph shows the evolution of the loss values for the training and validation sets over a period of 15 epochs during the model's training process. The epochs are marked on the x-axis, and the loss is marked on the y-axis. The train loss and the loss on the validation data are very high in the beginning, with train loss beginning from 0.03. But in the very first couple of epochs, the curves both come down very sharply, showing that the model is learning very quickly and reducing its prediction errors.
Both the training and validation loss curves stabilize at values very close to zero past the fifth or so iteration, and they are close to one another and almost parallel for the remainder of the training. Because the validation loss is not increasing or oscillating from the training loss, this trend indicates that the model is not overfitting. The model's high performance in generalization and prediction of unseen data is demonstrated by the consistently low loss of both sets, reflecting the efficiency of the hybrid deep learning method to detect cyberattacks in the Internet of Things environment.

3.1. Sub section 1
Four metrics were used as part of an evaluation matrix to measure the performance of this classifier: accuracy (A), positive future prolific value (P), recall (R), and F1 Price (F1). The accuracy assesses the overall performance of the classifier. Positive future price on a specific traffic class, recall and F1 price measurement performance.

$$A = \frac{TP+TN}{TP+FP+TN+FN}, P = \frac{TP}{TP+FP}, R = \frac{TP}{TP+TN}, F1 = \frac{2PR}{P+R} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

3.2. Sub section 2

In measuring performance of the student in each classifier, we use the following terminology: TP (true positives) is the number of correctly labeled items as X; TN (true negatives) is the number of correctly labeled items as Not-X; FP (false positives) is the number of incorrectly labeled items as X; and FN (false negatives) is the number of incorrectly labeled items as Not-X.**Error! Reference source not found.**

4. CONCLUSION

The proposed model optimized the ability of LSTM with temporal sequence modeling, and the power of DNN with nonlinear feature extraction and produced exceptional performance, as demonstrated in the experimental results (i.e. accuracy was nearly perfect and false positive and false negative results were very low). Additionally, the model has proven to be both robust and reliable in differentiating between malicious and normal IoT traffic. This research reflected a hybrid deep learning architecture, where Long Short-Term Memory (LSTM) networks and Deep Neural Networks (DNN) were combined together for detecting cyberattacks on Internet of Things (IoT) environment, and to train an autoencoder on a generalized dataset of cyberattacks on the ToN-IoT dataset (containing supplementary samples of which all are valid for normal traffic). The training and validation accuracy and loss curves provide further evidence by suggesting that the model did not tend towards overfitting and was able to generalize sufficiently. These findings substantiate how hybrid deep learning architectures can be utilized for IoT security, as they exist in the form of near-real time in timely detection of cyberattacks with a high accuracy. Future work may focus on optimizing the sensors and/or model so it can be executed and run on devices with minimum resources, and expand the model to detect new emerging attack types and advanced sophisticated attacks that will develop over time.

REFERENCES

[1] Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). A survey of security and privacy issues in the Internet of Things. In 2010 International Conference on Communication Systems and Networks (COMSNETS 2010) (pp. 1-7). IEEE.
[2] Weber, R. H. (2010). Internet of Things: New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.
[3] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
[4] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.
[5] Noor Ul Ain , Muhammad Sardaraz , Muhammad Tahir , Mohamed W Abo Elsoud , Abdullah Alourani , Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach , 2025
[6] Ahmed Bensaoud , Jugal Kalita , Optimized Detection of Cyber-Attacks on IoT Networks via Hybrid Deep Learning Models , 2025
[7] Alyazia Aldhaheri, Fatima Alwahedi, Mohamed Amine Ferrag, Ammar Battah , Deep learning for cyber threat detection in IoT networks: A review , 2025
[8] Bensaoud, J., & Kalita, J. (2023). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Computers & Security*, *126*, 103047. https://doi.org/10.1016/j.cose.2023.103047
[9] Zainudin, S., et al. (2025). Securing IoT networks against DDoS attacks: A hybrid deep learning approach. Sensors (Basel), 25(2), 11902570. https://doi.org/10.3390/s250211902
[10] Deep learning for cyber threat detection in IoT networks: A review. (2023). *Internet of Things and Cyber-Physical Systems*, *8*, 100211. https://doi.org/10.1016/j.iotcps.2023.100211
[11] Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Ad Hoc Networks*, *170*, 103770. https://doi.org/10.1016/j.adhoc.2023.103770
[12] Kumari, S., Mohan, A., Kumar, D., Ranjan, R., & Mahato, G. C. (2025). A hybrid AI approach for detecting network attacks in IoT environments. *Journal of Emerging Technologies and Innovative Research*, *12*(1), 1-10.
[13] CTU University, The Stratosphere IPS Project Dataset, https://stratosphereips.org/category/dataset.html, 2016.

BIOGRAPHIES OF AUTHORS

Mr. Fadi Hadi Nadhim, Received my bachelor degree in the science computer from University Al mammon – Iraq in 2010 and Master of science computer Islamic Azad University's Isfahan (Khorasgan) iran in 2024. I have joined to raqi army in 2011 after that I moved to Iraqi air force then I travelled to Jordan for 2 years and to the USA for1 year after finished the course of maintenance of the air craft I worked on F-16 fighter falcon jet ongoing I can be contacted at email: fadi1988319@yahoo.com.