International Journal of Computer Networks and Communications Security

VOL. 8, NO. 8, August 2020, 67–73
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Threat Detection using Machine/Deep Learning in IOT Environments

Danish Javeed[1], Umar MohammedBadamasi[2], Tahir Iqbal[3], Aliyu Umar[4] and Cosmas Obiora Ndubuisi[5]

[1, 3] Northeastern University, Shenyang, Liaoning province, China

[2, 5] Changchun University of Science and Technology, China

[4] Jigawa State Institute of Information Technology Kazaure, Nigeria

[1]*thedanishkhn@gmail.com*

ABSTRACT

The quality of human life is improving day by day and IOT plays a very important role in this improvement. Everything related to internet have some security concerns. This paper aims to improve the security in IOT environments. In any of the IOT networks the unknown and knows flaws can be a backdoor for any adversary. The increase use of such environment results in the increase of zero day cyber-attacks. This paper aims to focus on different models of DL in order to predict the attacks in IOT environments. The main aim of this research is to provide a very best solution for the detection of threats in order to improve the infrastructures of IOT. In this paper different experiments has been conducted and its results has been discussed in order to provide an effective solution.

Keywords: *IOT, Machine Learning, Threat Detection, Deep Learning*.

1 INTRODUCTION

Internet of things plays a very important role in this modern world. It empowers the world with smart homes, smart cars and plenty of other things. The IOT have different pros i.e. communication, automation, control, monitor and the most important it is cost effective as well as time saving. The IOT makes the communication possible in between devices and the most important is M2M communication which is famously knows as machine to machine communication. Due to such communication all of the physical devices have the ability to be connected together which provides the transparency with far greater quality and lesser problems [1]. While making any decision the information we have the more better decision we can make, whether we are buying something in any mall or grocery store or whether we want to check how much supplies and widgets our company supplies locally or globally. Knowledge gives power and the more power a person have the more better it is. As IOT provides the connectivity of physical devices, it provides an opportunity to control these devices using wireless communications. Without human intervention it was impossible for the machines to communicate with each other and after IOT infrastructure it became possible and it results in a very faster and efficient output [2]. Using smart homes which are one of the best inventions of IOT. It became easy to monitor the quality of air in our homes as well as to monitor the refrigerator in our homes in order to check where we have enough food supplies.

As shown in the above figure IOT provides lots of services to the world. Which starts from a smart watch and end with home appliances [3].While aiding the world with its incredible benefits, at the same time it ended up with new cyber-attacks. In order to improve the security of IOT environments different researchers provided different solutions. Some of them are to keep the data private and provides the access control for the purposes of authentication but IOT networks are still accessible to cyber threats even after adopting to these new security techniques. So it became more essential to provide and develop more security techniques to an IOT environment. Presently the intrusion detection system are incomplete for any IOT network, though it at is having mature technology for outdated networks. The reason behind it is that they are lacking the flexibility because IOT environment are having a complex ecosystem. There are some of the features of IOT which needs the necessity of development of intrusion detecting system. IOT environments are vulnerable to multiple cyber-attacks and the most common attack is DOS attacks. Such attack can deeply affect the environment as well as its applications. DoS incidences have perceived the development in DoS attacks from single flooding to multi – vector attacks. In Fog-to-Things, the unavailability of critical infrastructure as well as businesses that are held by the smart IoT objects, supported as primary target of DoS attacks. The transmission of undersized packets is called injection attacks in huge amounts. An SQL injection attack is one of the attacks which will be used in our dataset and it is used to poison dynamic statements of SQL for appending a true condition that won't be false. This attack is used to execute malicious SQL code for exploiting SQL statements in poorly intended web applications. Brute force attack is one of the attacks seen from our dataset because this type of attacks are very collective adjacent to networks in case of weak username as well as password combinations, they incline to break into accounts. The Infiltration attack, which we have used to select from inside the network in our dataset, is carried out in such a way that an attacker sends a malicious file to the target through an email for the manipulation of application susceptibility. A backdoor will be implemented on the victim's computer after the successful manipulation and then the attacker uses target computer for scanning the whole internal network and search for other weak holes and attempts possible manipulations. This paper classified the attack in to three different categories and this classification make it possible for numerous is researches to have a depth analysis of the smart environments. As shown in the figure 1below the attacks has been categorized in two three types.

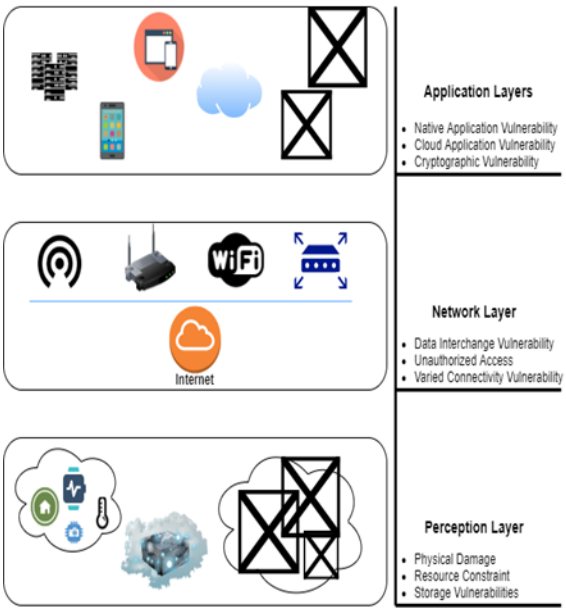

Fig. 1. Attacks on IOT Environments

There are different types of attacks which are known as (DOS) attacks, probing attacks, (R2L) attacks and (U2R) attacks.

- ***Probing Attacks:***

Any attack which creases evidence about the target.

- ***DOS attacks:***

An attempt which is used to hold the valid user to access the system.

- ***R2L Attacks:***

A type of attack which is used to gain access to an authorized system of a user account on the system in knows as remote to lacal (R2L) attacks.

- ***U2R Attacks:***

It is the most destructive type of an attack, it arises when the access of the system or user account has already been achieved by the attacker, and furthermore the attacker tries to access the administrative privileges of the user. Such attacks are known as User to root (U2R) attacks.

2 RELATED WORK

In [1] the author used artificial neural network and offered threat detection but the supervised ANN was used to trace the packet instead of detecting the DDOS attacks. The key objective for using this

method is to detect the DDOS attacks but the classification of this design save bandwidth and resources which leads to the consumption of such attacks. In [2], the author addresses an intrusion detecting system for SDN defined IOT environments using IA techniques. The assessment of more accuracy and low overhead in the presence of the current solutions is the main objective of this technique. IOT provides logical data which is of a very high capacity authorizes nearly every field of normal life. [5,7] IOT is facing a key problem which contains privacy as well as security. [8] In order to prevent diverse attacks some of the techniques of data mining can be used in smart grid.

2.1 Comparison of IDS in IOTs

The model performance has been improved by the methods of deep learning. A huge variety of fields are using the architecture of deep learning such as natural language processing, voice recognition and computer vision. A huge number of the approaches of deep learning have been used in order to prevent the DDOS attacks [8]. In [11] the author introduced a detection system for the DDOS attacks based on multi-level deep learning technology. In [13] the author proposed a model of MC-CNN in order to enhance the feature information to expect a better recognition. The performance metric has been used by the n-fold cross validation evaluation. In order to maintain a high rate of detection, the results show the potential of deep learning. The whole process is similar as LSTM training, although the study used CNN. Under some studies the memory requirements and the detection system of DL is found to be far better than the machine learning. There are multiple researches in the area of cyber security but there is hardly a promising one in cyber security using deep learning. With the advancement in the area of computer security, the research work in DL has been emerged in areas like image processing and pattern recognition. In [9] the author used a dataset named NSL-KDD, which is an application of deep learning in the area of computer security. In his work unsupervised feature learning has been employed on training of data which used an encoder named as sparse-auto encoder by the application of a self-taught deep learning scheme. For the division of attacks and normal activities, the application of learnt features to the labeled set dataset has been used. For the performance evaluation the author used n-fold cross validation technique and the desired outcome seems to be reasonable. Though this paper aims to consider the centralized system. [19] The knowledge for the identification of an infected script code from a normal code was acquired by the application of denoising Auto Encoder for deeper features. The outcome has provided desired accuracy in the best-case scenario. This can be scarcely applied to distribute IOT systems, although the method is found to be operative in web applications. By using the approach of deep learning in the area of IOT, the detection of intrusions has been achieved. LSTM network for intrusion detection has been used to obtain the accuracy in networks which shows the capability of the deep learning in order to extract patterns from a raw data. But it has been clearer from some evidences that for any intrusion detection the LSTM shows a better performance than classical machine learning because of its long memory. In order to model normal and anomalous pattern another research was conducted on this detection showing the effectiveness of LSTM. The performance of the model is another indicator to show the efficiency of deep learning in intrusion detection. [10] LSTM outclassed the n-gram approach which was the demonstration of the (AUC). This technique is having a great efficiency as well as importance in the detection of injected malwares using URLs. In order to detect phishing links LSTM was used in [11]. The comparison of different experimental results has been done on random basis and LSTM model has been found as the most accurate one.

Table 1: Comparison of proposed model with existing work

Methodology	Dataset	Algorithim	Relevance to topic	Standard parameters	Outcome
Deep learning (DL)	KDD99	Restricted Boltzman n Machines (RBM)	8%	Accuracy higher than 94%. Accuracy slightly higher than 85%	Improved Accuracy rate
Ensemble of classifiers Ensemble of Deep Belief Network (DBN)	SCADA network data set	Deep Belief Network(DBN) and SVM	7%	SVM: 93.88 Ensemble SVMs: 94.41 Ensemble of DBNs: 95.60	Ensemble Approach of DBN for large dataset
Artificial intelligence (AI)	Some Unbalanced Dataset	BAT algorithm For feature selection, random forest (RF) for classification	9%	Accuracy: 96.42 Precision :99.51 Recall :95.17 F-score: 97.29 FPR: 0.98302	Done classification on unbalanced data
Ensemble Methods and Deep Learning Models.	Self-generated Dataset using IOT protocols	XGB oost, LST M, GRU RNN	10%	Cross Entropy 0.128 Accuracy DOS: 0.99377 MitM: 0.953 F-Beta Score 0.95777	Collaborative method Enhanced the Overall Accuracy as match to the Deep learning models
DEEP Learning	NSL-KDD	SGD	7%	Accuracy : increased from 96 to 99 False Alarm rate: decreased from 6.97 to 0.85. Recall: improved from 97.50 to 99.27	Proved that even simple deep learning algorithms can outperform efficient machine learning algorithms
Machine learning and Network Function Virtualization	Self-Generated dataset using Scapy and Wireshark	Rand om Forest and SVM	8%	Accuracy: 96%	Examined the traffic on the IoT security network edge for detection of Attacks.
Deep Learning	NSL-KDD and UNSW-NB15.	Unsupervised Deep Auto-Encoder (DAE)- DFF NN	10%	Accuracy: 99% FP rate: 1.8%	In an IIoT situation, system can notice normal and attack conduct with the usage of unsupervised learning.

3 IMPLEMENTATION

This part of the paper aims to conduct different experiments of three algorithms which have been used for the implementation of our module. First of all the data has been prepared in order to make it understandable for the machine. The machine will use the data for training. At the later stage the evaluation of every model will be tested after the completion of training phase and will be mapped accordingly. Step by step procedure has been followed of each of the selected scheme of deep learning.

3.1 Predictions of CNN Architecture

The figure used frequently for presenting the model of classification on the test data set, according to which values of true predictions are recognized, this is what we called confusion matrix. It allows the presentation of an algorithm to be envisioned. The confusion matrix can also be clarified to condense the result of predictions over a problem related to classification. The sum for summarizing predictions as the correct and as an incorrect, computational power is used and it can also be achieved by breaking each class. It's very crucial for confusion matrix. This figure exemplifies the resources by which the classification model is muddled when it makes calculations. It provides us with the understanding

about the inaccuracies made by the classifier but also the kinds of inaccuracies being made. As shown in the Fig – 3.1, the confusion matrix provides correct number of predictions alongside each class. The model accurateness is clearly proven.

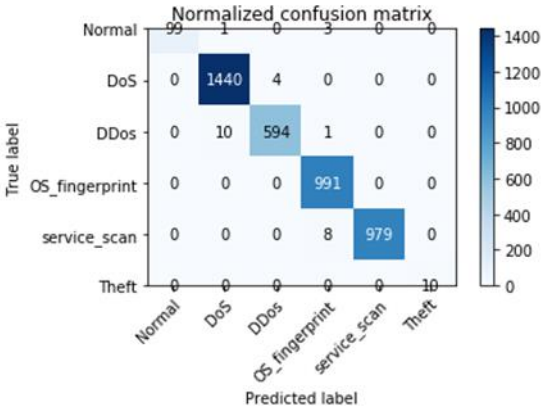

Fig. 3.1. confusion matrix provides correct number of predictions alongside each class.

3.2 Check Loss and Accuracy

At this stage of the implementation phase the loss check and accuracy of the train and tested data has been shown in the figure 3.2. As shown in the figure below the percentage of accuracy has been different in test data and train data. Its almost 0.8 on the train data but if we see the test data it is almost 0.9. Initially the loss was high for both of the data but it was decreased gradually. As the number of epochs as well as the size of dataset has been increased it had a sever effect on the result and the result was totally changed. The accuracy and loss shares a direct proportionality in between each other, if model is exposed to a huge data as well as more times, the model will learn more and will have the ability to differentiate in between the targets and non-target matters. But the model has performed very well overall and not a single mistake has been found in fuse detection.

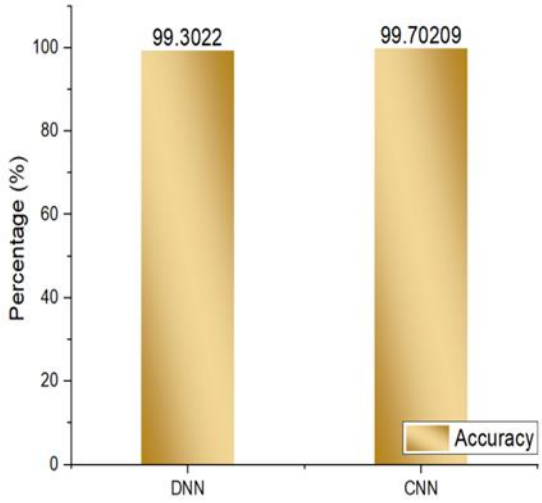

Fig. 3.2 Model Accuracy.

3.3 Algorithm Structure

The structure of the algorithm has been used for testing and training the proposed model of this research. There are total seven layers of DNN is used. 39 input dimensions as well as 300 neurons were present in the first dense layer of the model. The second layer had 200 neurons, third layer had 150 neurons, fourth layer had 100 neurons, and fifth layer had 50 neurons. While sixth layer had 20 neurons and finally the last layer had only 6 neurons respectively. Last year consist of softmax which is used for the detection of multi class as well as it is used as an activation function, while RELU is sued in the hidden layers.

3.4 Predictions of DNN Architecture

As in the figure 3.1 it is clearly shown that against every class, a correct number of predictions are provided by the confusion matrix. The accuracy of the model has been proven evidently as shown in figure 3.3.

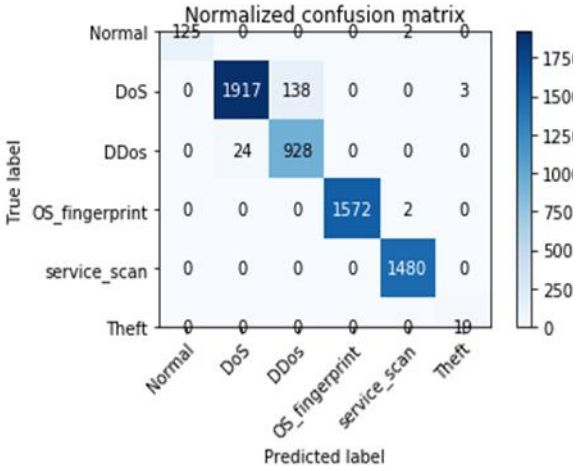

Fig. 3.3 Confusion Matrix DNN

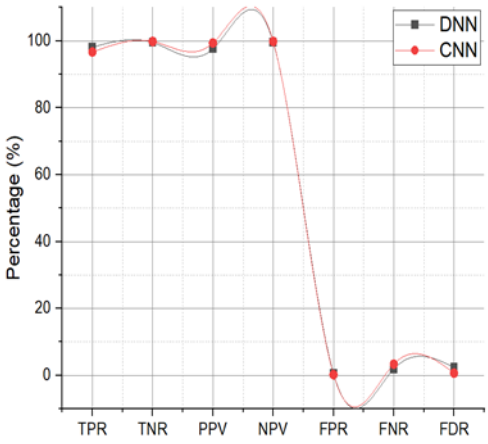

Fig. 3.5. T & F positives & Negatives

3.5 Precision and recall of DNN and CNN

The precision and the recall results which are based on the perfect results shown are shown in the figure 3.4.

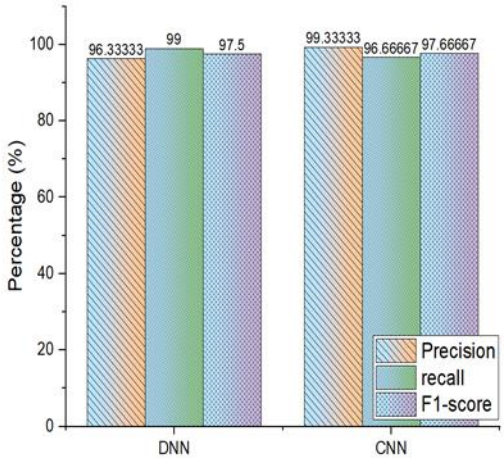

Fig. 3.4. P & R of the models

3.6 True and False Positives and Negatives

False positive rate shows the extent to which the prediction of proposed module is accurate. True positive rate confirms the ratio of system responded accurately same as the False negatives which tells the ratio of accurate predictions as shown in fig-3.5 in next column. The true negative rate tells the system predicts attack when there is no attack in actual.

4 CONCLUSION

A significant attention has been gained by deep learning with advancement in it. In this paper two states of art algorithms has been compared from advancement of machine learning known as DNN and CNN. In order to make the system to detect different attacks and classify different attacks in IOT, CNN and DNN models are used. It has been concluded from the results in this paper It has been concluded that the DNN model is totally outperformed by CNN model because it consistently shows accuracy up to 99 percent with small incorrect negative as well as positive rates. Furthermore, for the experimentation purposes both the CPU and GPU has been used. It has been noticed that the CNN GPU utilization was much higher with the comparison to CPU. The testing and the training times of the GPU were much faster, about more than 15 times faster than the CPU. The future work of this research aims to test these models with various and updated datasets in order to find a best model and to deploy that model in order to detect anomalies in IOT environments. On the same dataset various deep learning algorithms will be applied such as RNN as well as LSTM is some types of algorithms for future work.

5 REFERENCES

[1] Elrawy, Mohamed Faisal, Ali Ismail Awad, and Hesham FA Hamed. "Intrusion detection systems for IoT-based smart environments: a survey." Journal of Cloud Computing 7.1 (2018): 21.

[2] IoT Bots Cause Massive Internet Outage. https://www.beyondtrust.com/blog/iot-bots-cause-october-21st-2016-massive-internet-outage/. Accessed 22 Oct 2016.

[3] Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90
[4] Javeed, Danish, et al. "An Efficient Approach of Threat Hunting Using Memory Forensics." International Journal of Computer Networks and Communications Security 8.5 (2020): 37-45.
[5] Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computers to the Internet of Things". Informatik-Spektrum. 33 (2): 107–121.
[6] B r o w n , Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com.
[7] Saha, Himadri Nath, Abhilasha Mandal, and Abhirup Sinha. "Recent trends in the Internet of Things." 2017 IEEE 7th annual computing and communication workshop and conference (CCWC). IEEE, 2017
[8] Khan, Tahir Ullah. "Internet of Things (IOT) Systems and its Security Challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 8.12 (2019).
[9] Viegas, E. K., Santin, A. O., & Oliveira, L. S. (2017). Toward a reliable anomaly-based intrusion detection in real-world environments. Computer Networks, 127, 200-216
[10] Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 32-37). IEEE.
[11] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.
[12] Liu, H., Lang, B., Liu, M., & Yan, H. (2019). CNN and RNN based payload classification methods for attack detection. Knowledge-Based Systems, 163, 332-341
[13] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.
[14] Abeshu, A., & Chilamkurti, N. (2018). Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169-175
[15] J. Li, Z. Zhao, R. Li, and H. Zhang, “AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks,” IEEE Internet Things Journal, vol. 6, no. 2, pp. 2093–2102, 2019.
[16] S. Sukode, and S. Gite, “Vehicle Traffic Congestion Control & Monitoring System in IoT,” International Journal of Engineering Research, vol 10, pp 19513-19523.
[17] A. Dunkels, J. Eriksson, and N. Tsiftes, “Low-power interoperability for the IPv6-based Internet of Things,” in Proc. 10th Scandinavian Workshop Wireless ADHOC, Stockholm, Sweden, 2011, pp. 10–11.