JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

COLLABORATIVE INTRUSION DETECTION SYSTEM FOR IOT DEVICES USING DEEP LEARNING TECHNIQUES

1Biju A, **1**Suganya Jerlin SL

1Department of Computer Science and Engineering

1Maria College of Engineering And Technology, Attoor, India

Abstract: Numerous researchers are deeply focused in the Internet of Things (IoT) and its applications because they render life become simple. Based on its widespread recognition, attacks targeting those devices including denial of service attacks as well as sybil attacks, have increased dramatically, potentially causing the system to become unavailable. Thus, it has become mandatory that the technique for identification of malware in the IoT is essential. This research proposes CNN-IoT a collaborative intrusion detection system (IDS) that monitors IoT devices regarding malicious activity. The NSW-NB15 dataset was utilised to evaluate the proposed system. An accuracy of 98.54% has been achieved with lower type II error rate around 0.01. The performance evaluations show that the proposed method outperforms the other existing techniques available in the literatures.

Keywords: IoT; edge computing; collaborative; malware

I. Introduction

By integrating the Internet towards physical objects (such as equipment as well as people) and transmitting data among them, the IoT enables the integration of the real world and indeed the data world [1] and making lives smarter and more fashionable [2]. Smart metering, smart hospitals,smart cities smart transportation and smart agriculture are some of the most prominent IoT applications presently [2].

IoT as well as social networking applications were expanding at an unsustainable rate, leading in an exponential surge in data produced at the network's edge [3]. Traditional centralised cloud computing platforms could previously offered centralised remote solutions by centralising all data upon a single server [4]. Regard to problem which including network bandwidth constrictions as well as data privacy [5], it is unrealistic and always inappropriate to continue sending overall data towards the remote cloud in the similiar manner [3], although this process requires enormous data transmission expenditures and thus would not satisfy the real requirements of certain lower latency applications and services [4]. As a direct consequence, edge computing must have grown rapidly as a cutting-edge strategy [5]. Edge computing extends different networking services as well as data processing closer to the end user to the edge of the network, until they would previously performed in the core network [6], emerging in edge-assisted IoT. Edge computing has already been mentioned as a feasible alternative for overcoming cloud

computing's shortcomings in addressing IoT applications [7, 8]. Edge computing, as contrast to cloud computing, permits consumers to access effective network communication services featuring decreased latency, higher flexible access, including data privacy protection [7, 9].

Intrusion detection seems to be a powerful active defensive mechanism with a variety of detection methodologies [10]. Intrusion detection strategies could indeed be categorised into two communities relying on the data source: network relied intrusion detection as well as host relied intrusion detection [11]. These are some of the methods for slightly earlier detection of network threats is a network based intrusion detection system [12]. Todays modern network data, on the other extreme, possesses more complex, but also multidimensional properties. Traditional machine learning algorithms must manually retrieve a significant number of features whenever dealing with high-dimensional data characteristics. The procedure is complex and difficult, and the calculation demanded is huge, making it impossible to fulfill the precision and requirements in real time of IDS [13].

Athough this theory has been suggested deep learning, as a fundamental field of machine learning, has gotten more consideration. The deep learning model specialises at handling with difficult data and thus can generate aspects of enhanced representation from massive datasets automatically. Feedforward neural networks, particularly convolutional neural networks (CNN), have attained well-recognized advanced outcomes in image classification. Recurrent neural networks (RNN), particularly LSTM, had even produced excellent performance for language modelling applications [14].

DBN, CNN, RNN, GAN, and other techniques are applied extensively in DL-based IoT intrusion detection [15, 16, 17]. Most depth models, on the other extreme, have a comprehensive network topology with training process, as well as a larger number of model parameters, which maximises the complexity as well as energy consumption of training. Stahl et al. [18] recommended using numerous collaborative edge devices to conduct CNN model identification attacks in a distributed sort of way. Their approach was based on partitioning the CNN layer, here the dominating weight lies, distributing the data weight and calculation load uniformly over all accessible devices, and decreasing time of task execution.

Researchers would have increasingly undertaken researching whether collaborative IDS [19] might become a mainstream alternative for detecting attacks in massive as well as complex networks likely to be the IoT[20]. By effectively and efficiently analyzing realistic worm datasets,

Researchers have proposed a variety of ways for detecting malicious activity in IoT devices, ranging from edge computing tools towards cloud computing. The software is intended to retrieve the characteristics of the traffic on the network Deep learning algorithms are often used to evaluate the data. Requests are characterized as either malicious or benign. Some of these technologies, on the other contrary, have a lot of delay.Fog computing is being used to capture and analyse requests. Furthermore, some of the current research takes into consideration a few categories of attacks present in IoT in their IDS.

The paper was organized as follows: Section 2 specifies the proposed methodology. Section 3 explains the outcome of the proposed system and. Finally, Section 4 addresses the conclusion as well as the future work.

II. PROPOSED METHODOLOGY

This section expains the components of the CNN learning model. Finally, use attention processes in an innovative way to establish a CNN-based intrusion detection technique.

2.1. CNN for Intrusion Detection

The study of visual cortex cells influenced CNN, which is a variety of artificial neural network (ANN). Its important component is that it seems to be using local connections as well as shared weight to start reducing the quantity of parameters throughout the network and actually accomplish several degree of affine invariance.

When implementing a NN model towards tasks detection, the network architecture provides a considerable influence on the detection outcomes. Most edge devices, on the other extreme, are restricted by memory and computational capacities, and therefore are still unable store and run complicated CNN models. As a result, when configuring the hierarchical framework of the CNN model begin by modifying parameters as well as optimising the structure. The CNN framework construction is fairly simpler, as depicted in the Figure 1, while ensuring accuracy.

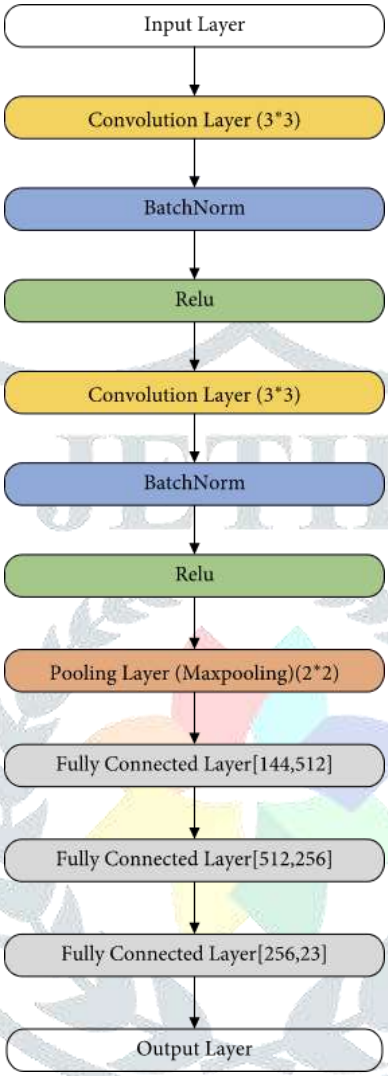

Fig.1 Structure of the proposed CNN Architecture

The convolution layer, pooling layer as well as the full connection layer comprise the majority of the CNN model framework. The data input layer is indeed the initial layer. The data distribution would modify even during training phase, providing complexity in learning the succeeding network. To force the data after the convolution layer, employ batch normalisation.

Returning to the normal distribution with the variance 1 and mean 0; on the one extreme, this ensures that the data distribution is coherent, and it prohibits gradient disappearance. Researchers are using the ReLU function as the nonlinear activation function for supplement the tanh or Sigmoid functions commonly utilized throughout classic NN, which can dramatically accelerates network convergence as well as training. The pooling process decreases the convolution layer's output size, minimizing calculation expenditures and eliminating overfitting. The mean-pooling as well as max-pooling methods constitute the most regularly deployed pooling methods, and the max-pooling methodology is explored in this paper. The fully linked layers are the ninth through eleventh layers; the overall neurons in every layer. The network's output layer was the final layer, which were mostly exploited for classification

estimation. As the function of decision, implement Softmax which develops a fractional vector towards every class as well as provides the maximal index to be the predicted class.

Algorithm: CNN-IoT Detection Procedures
Input: Network Traffic *NT* captured;
Output: 0-Normal; 1-Malicious
Step 1: *C = load Model*()
Step 2: **for** *Each Captured Traffic*
do
Step 3: *C.predict*(*NT*);
Step 4**: if** *Result* = 0 **then**
Step *5:Allow Traffic*;
else
Step *7: Block Traffic*;
Step *8: Inform Other Nodes*;

III. EXPERIMENTAL RESULTS AND DISCUSSION

To set up the design to the test, researchers utilise the NSL-KDD dataset. The number of clients in these investigations may indeed be continuously determined, and that each client trains their model utilizing local data prior uploading new parameters on model to the server for aggregate. The operating system on the server in this investigation is Windows 10, as well as the processor is an Intel(R) Core (TM) i5-10210U CPU@2.11 GHz. To develop CNN, utilise Pytorch, a Python deep learning framework.

3.1. Performance Metrics

The following indicators of performance were employed to assess the detection model's performance:

3.1.1 Accuracy: The proportion of correctly identified samples to the total number of samples. Equation (1) is being used to evaluate accuracy:

$$\boldsymbol{Accuracy = TP + TN / TP + TN + FP + FN} \quad \textbf{(1)}$$

True positive is symbolized by the TP. This implies that the sample accurately recognizes harmful samples as. True negative signifies that the model was incapable to characterize a benign sample to be benign. The FN continues to stand for false negative,that further suggests that this design would have been inadequate to distinguish a malicious sample consequently.

3.1.2 Type II Error or FN Rate: In comparison to the maximum number of malicious samples, the overall number of malicious samples that are incorrectly classified.

The proposed approach realised the best accuracy of 98.35 % when these were trained on the great aspects determined by F-test methodology, as demonstrated in Table 1. The rate of type II errors remained 0.01 %. As reported in Table in Table 1, CNN-IoT has been examined towards other present state-of-the-art tools. C ompared CNN-IoT to some of the current tools suggested by Moustafa and Slay [15], I determined that CoLL-IoT outperforms latter. Through using UNSW-NB15 dataset, Moustafa as well as Slay [21] evaluated machine learning techniques. Employing DT algorithm, they were able to acquire an accuracy of 85.56 %, with either a type II error rate of 15.78 %. Using decision tree algorithms, Dimitrios et al. [22] recommended a network IDS regime. Users assessed the suggested system on the UNSW-NB15 dataset as well as observed that it would having accuracy about 84.33 % and also type II error rate of 2.61 %. Using the SVM methodology, the suggested system performed two detection phases to categorize malicious behaviour and acquired an accuracy of 82.11 %. Furthermore, Ferhat and Ahmet [23] presents a methodology that attained 97.44 % combining a deep neural network as well as an autoencoder.

Table.1: Comparative Analysis

Author	Accuracy (%)	Type – II Error (%)
Moustafa and Clay[21]	85.56	15.78
Dimitrios et al. [22]	84.33	2.61
Ferhat and Ahmet [23]	97.44	2.01
Proposed	98.54	0.01

IV.CONCLUSION

CNN-IoT, a collaborative detection procedure for recognizing malicious activities in the IoT devices, has been proposed in this investigation. The layers cooperated collaboratively to evaluate network traffic to discover malicious behaviour. With a low type II error rate, CNN-IOT was being used to diagnose malicious activities. The recommended approach was examined on the UNSW-NB15 dataset, including IoT threats like shellcode, DoS, exploits, fuzzers and analysis. The simulation outcomes shows that proposed CNN-IoT achieves an accuracy of 98.54% with a minimum type II error rate around 0.01%. dataset. As a future work, other deep learning algorithms can be used to improve accuracy and more types of attacks can be deployed, that would employ to construct a model to detect most popular attacks.

REFERENCES

[1] S. S. Swarna and R. Ratna, "Investigation of machine learning techniques in intrusion detection system for IoT network," in Proceeding of the 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1164–1167, IEEE, *oothukudi, India, December 2020.

[2] S. Anand and A. Sharma, "Assessment of security threats on IoT based applications," Materials Today: Proceedings, 2020, In press.

[3] D. Wu, J. Yan, H. Wang, and R. Wang, "Multiattack intrusion detection algorithm for edge-assisted internet of *ings," in Proceeding of the International Conference on Industrial Internet (ICII), pp. 210–218, IEEE, OL, USA, November 2019.

[4] S. Wang, T. Tuor, T. Salonidis et al., "Adaptive federated learning in resource constrained edge computing systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205–1221, 2019.

[5] A. Alwarafy, K. A. A. *elaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edgecomputing-assisted internet of *ings," IEEE Internet of @ings Journal, vol. 8, no. 6, pp. 4004–4022, 2021.

[6] W. Y. B. Lim, C. Luong, T. Hoang, Y. Jiao, and C. Liang, "Federated learning in mobile edge networks: a comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2031–2063, 2020.

[7] F. Lin, Y. Zhou, X. An, I. You, and K. R. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of internet of *ings devices," IEEE Consumer Electronics Magazine, vol. 7, no. 6, pp. 45–50, 2018.

[8] G. W. Cassales, H. Senger, E. R. de Faria, and A. Bifet, "IDSAIoT: an intrusion detection system Architecture for IoT networks," in Proceeding of the Symposium on Computers and Communications (ISCC), pp. 1–7, IEEE, 2019.

[9] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacypreserving user authentication scheme with forward secrecy for industry 4.0," SCIENCE CHINA: Information Sciences, vol. 64, 2020.

[10] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques," Mobile Networks and Management (MONAMI), vol. 235, pp. 30–44, 2017.

[11] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," Physical Communication, vol. 42, 2020.

[12] S. Hosseini, "A new machine learning method consisting of GA-LR and ANN for attack detection," Wireless Networks, vol. 26, no. 6, pp. 4149–4162, 2020.

[13] A. P. D. C. Kelton, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. D. Albuquerque, "Internet of *ings: a survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147–157, 2019.

[14] B. McMahan, E. Moore, D. Ramage et al., "Communicationefficient learning of deep networks from decentralized data," in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, vol. 54, pp. 1273–1282, Ft. Lauderdale, FL, USA, April 2017.

[15] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, 2020.

[16] X. Yuan, C. Li, and X. Li, "DeepDefense: identifying DDoS attack via deep learning," in Proceeding of the International Conference on Smart Computing (SMARTCOMP), pp. 1–8, IEEE, Hong Kong, China, May 2017.

[17] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," IEEE Access, vol. 7, Article ID 64366, 2019.

[18] R. Stahl, A. Hoffman, D. M. Gritschneder et al., "Deeper*ings: fully distributed CNN inference on resourceconstrained edge devices," International Journal of Parallel Programming, vol. 49, 2021.

[19] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained IoT devices," Mechanical Systems and Signal Processing, vol. 136, 2020.

[20] X. An, X. Zhou, X. L¨u, F. Lin, and L. Yang, "Sample selected extreme learning machine based intrusion detection in fog computing and MEC," Wireless Communications and Mobile Computing, vol. 2018, Article ID 7472095, 2018

[21] Moustafa, N.; Slay, J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Inf. Secur. J. Glob. Perspect. 2016, 25, 18–31.

[22] Papamartzivanos, D.; Mármol, F.G.; Kambourakis, G. Dendron: Genetic trees driven rule induction for network intrusion detection systems. Future Gener. Comput. Syst. 2018, 79, 558–574.

[23] Catak, F.O.; Mustacoglu, A.F. Distributed denial of service attack detection using autoencoder and deep neural networks. J. Intell. Fuzzy Syst. 2019, 37, 3969–3979.