2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) | 978-1-6654-4058-5/20/$31.00 ©2021 IEEE | DOI: 10.1109/HORA52670.2021.9461285

A new Deep Learning Based Intrusion Detection System for Cloud Security

Selman HIZAL
Distance Education Research and
Application Center
Sakarya University,
Sakarya, TURKEY
shizal@sakarya.edu.tr

Ünal ÇAVUŞOĞLU
Software Engineering
Sakarya University
Sakarya, TURKEY
unalc@sakarya.edu.tr

Devrim AKGÜN
Software Engineering
Sakarya University
Sakarya,TURKEY
dakgun@sakarya.edu.tr

Abstract*—Cloud computing is used in many different research areas thanks to its high computing power and network capacity. Data security, cost-effectiveness, and flexibility of working options for remote workers have made this technology even more attractive today. Today, servers in cloud computing should protect themselves from threats more intelligently and provide security by preventing a new threat. A new deep learning model based on convolutional neural networks and recurrent neural networks for intrusion detection has been developed for cloud security in this study. The proposed model was trained and tested using NSL-KDD train dataset. With our deep learning model, any detected and not approved traffic is prevented from reaching the server in the cloud. The proposed system has 99.86% accuracy for five-class classification, which is the best result comparative to studies in the literature.

***Keywords*—Cloud Computing, Security, Deep Learning, NSL-KDD**

I. Introduction

Most of the communication of people in the world takes place over the internet. The internet has become an indispensable part of our lives in the military, health, public institutions, private organizations, industry, education, and many other fields. Moreover, smart devices called the internet of things (IoT) is also included in this mass communication network. Therefore, the need for cloud computing technology is increasing day by day to provide more efficient and secure big data created with this communication network. Especially in the global pandemic of COVID-19 in world, this need is felt more by all countries. Instead of service provider companies such as Microsoft Azure, Amazon Web Services, Google Cloud, and Oracle Cloud, which invest heavily in cloud computing, different countries want to create cloud systems. The biggest concern here is to ensure the security of its national data. In the globalizing world, it is inevitable to commercially use cloud computing infrastructures in different countries of the world. However, the quality of cloud computing service providers is achieved mainly by the sophistication of security systems.

The attackers carry out different types of cyber-attacks on the servers and network infrastructure in cloud computing. DoS attacks are the most common type of attacks constantly sent to the server from different IP addresses, preventing the servers from serving or even shutting them down.

"Fig. 1" shows a malicious attack on a data center belonging to cloud computing service providers and the detection of this attack by deep learning methods in real-time. The attacker usually changes the IP address to hide or perform the attack on the victim's computer or servers he has acquired. Although the firewall on the network that first responded to the attack performed an attack filtering process, unfortunately, this security measure alone is not sufficient today. Attacks that can bypass the firewall are then sent to the deep learning-based intrusion detection system (IDS) through an intermediate router. Many different classes of attacks or new attacks can be detected here. If an abnormal situation is seen, this is reported to the management system center instantly. This center usually notifies this situation via SMS or e-mail notifications to the system officers immediately to their mobile phones. It informs that the attack has been detected and then blocks this attack automatically.

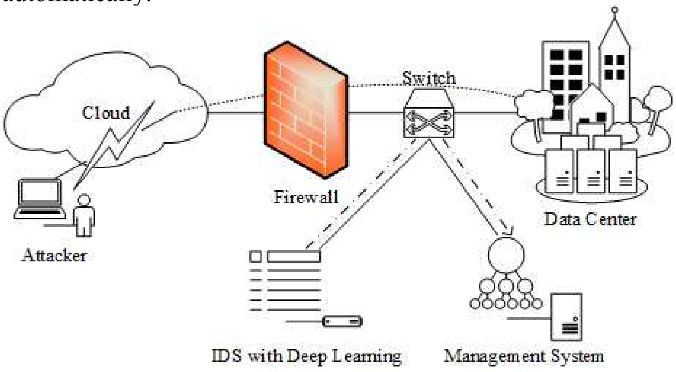

Fig. 1. An intrusion detection and management system using deep learning for cloud security.

Nowadays, it is necessary to propose a more accurate and efficient attack detection method to detect new attacks on networks and servers within cloud computing. Detection approaches don't usually utilize explicit programming due to the complexity of the problem. Instead, they typically use Machine learning methods that can significantly be successful in decision problems like IDS as long as enough features are provided about the problem. In deep learning, a sub-branch of Machine Learning, necessary features are also extracted by training particular layers such as Convolutional Neural Networks (CNNs) or recurrent Neural Networks (RNN). The success of a developed deep learning network depends heavily on the type of feature extraction layers in addition to a training set large enough. Also, organization and preprocessing of the input data may have a significant impact on the success. Therefore, the search for better models in various areas, including IDS is an ongoing issue studied by researchers.

This paper is interested in finding a suitable deep learning model for Cloud security. We are especially interested in

978-1-6654-4058-5/21/$31.00 ©2021 IEEE

multiclass and binary classification tasks. We proposed a lightweight model based on convolutional and recurrent layers for binary and five-class classification using the NSL-KDD dataset. According to experimental evaluations, our five-class classification achieves 99.86% accuracy, which is the best result compared with the previous studies.

The remainder of this study was organized as follows: Section II provides the literature review. The proposed deep learning model is described in Section III. Comparative experimental results were presented in Section IV. Finally, a brief conclusion about the study was given in Section V.

II. LITERATURE REVIEW

In the literature, there are various studies about IDS using machine learning methods. We gave the most recent deep learning-based articles. Zhang et al. [1] proposed a combined approach based on Deep Belief Networks (DBN) and Probability Neural Networks (PNN). They dealt with a class imbalance on NSL-KDD using SMOTE for increasing minority classes and NCL for under-sampling majority classes. Yan et al. [2] proposed a feature extraction technique, using the stacked sparse autoencoder (SSAE), an instance of a deep learning strategy to select attributes with higher representation. The proposed system is compared with previous feature extraction methods. The classification process is accelerated and a better learning process is achieved, an efficient and applicable system for use in intrusion detection systems has been developed. Xin et al. [3] presented a literature review for machine learning and deep learning applications in network intrusion detection, and they evaluated various datasets, methods, problems, and approaches for intrusion detection. Elmasry et al. [4] proposed algorithms based on Particle Swarm Optimization (PSO) for feature selection and hyperparameter selection. They evaluated various deep learning models such as Long Short Term Memory (LSTM), and DBN. Aldweesh et al. [5] presented a survey study on deep learning in IDS and investigated open studies and future directions. They also gave a background for deep learning architectures, IDS types, and datasets. Gamage et al. [6] presented a classification of deep learning models in intrusion detection systems and a detailed literature study in their study. Training and testing operations were carried out on four different datasets (KDD 99, NSL-KDD, CIC-IDS2017, CIC-IDS2018) using four other deep learning methods. The obtained test results were compared with the studies in the literature, and evaluations were given for future studies on deep learning-based intrusion detection systems. The author proposed a deep learning-based attack detection system for proposed DDOS attacks. The proposed system has been tested on the CICIDS dataset and virtually generated DDOS traffic. It has been stated that the proposed system performs better than many previous studies in detecting DDOS attacks [7]. Shone et al. [8] presented a stacked nonsymmetric deep autoencoder (NDAE) classification model for unsupervised feature learning. The presented system is tested on the GPU using KDD-CUP99 and NSL-KDD datasets. The results obtained were compared and evaluated with the studies in the literature. Xu et al. [9] developed a deep network model consisting of recurrent neural networks with gated recurrent units (GRU), multilayer perceptron (MLP), and softmax modules to increase the performance of intrusion detection systems. The tests of the proposed system have been carried out on the KDD-99 and NSL-KDD datasets. According to the test results, it has been shown that the GRU system has better results than LSTM for intrusion detection systems. Al-Qatf et al. [10] developed self-taught learning (STL)-IDS based on the STL framework to provide better network security than traditional network defense technologies. Their experiments on the NSL-KDD dataset increase the accuracy in the binary and five-class classification and reduce the training and testing times. Parampottupadam et al. [11] proposed a cloud-based system for real-time network intrusion detection using binomial and five-class deep learning models together on the H2O framework. In case of an attack, they can automatically send a mobile notification to the system authorities thanks to a web page in the cloud-based architecture they designed. Zhang et al. [12] presented an IDS based on improved DBN with genetic algorithms for the Internet of Things (IoT). The optimal network structure is determined with GA using multiple iterations. Vinayakumar et al. [13] examined a DNN model with various layers, and they used NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017 for HIDS and NIDS. According to detailed experiments, their model can be monitored in real-time and has better results when compared to the classical machine learning algorithms. Yang et al. [14] developed a DBN-based model with a 4-layer and SVM classification layer. They experimented with various kernels such as Rbf, linear, polynomial, and sigmoid. According to experimental results on the NSL-KDD dataset, they achieve the best results using the RBF kernel.

III. PROPOSED SYSTEM

In this study, the NSL-KDD dataset, widely used in the literature to detect attacks with deep learning methods, was used. This data set consists of five classes: Normal, Denial of Service (DoS), User To Root (U2R), Root To Local (R2L), and Probe. Table I give the distribution of these classes in the NSL-KDD training and test data set.

TABLE I. NSL-KDD DATA SET TRAFFIC DISTRIBUTION

Main Class	Training	Test
Normal	67343	9711
DoS	45927	7458
U2R	52	200
R2L	995	2421
Probe	11656	2754
Total	125973	22544

- DoS: It is the most common attack class in the NSL-KDD data set. Hackers generally attack the servers to make them entirely out of service or prevent normal users from accessing the servers.
- U2R: Attacks made by hackers to gain unauthorized access to servers through methods such as malware infection or stolen credentials.
- R2L: Attacks by hackers to gain remote access to a victim machine by mimicking existing local users. This machine at the target chosen as the victim can usually be a server or a computer authorized to access the server.

- Probe: Attacks made by hackers to learn the IP address or active ports of the network or target server, the operating system on which it is running, and other similar important information.

The accuracy, which generally explains how the model performs in all classes, was calculated in the proposed method. It is calculated as the ratio of the number of correct predictions to the total number of predictions. The proposed model consists of one-dimensional convolution (Conv1D) layers and a Gated Recurrent Unit (GRU) layer, as given in "Fig. 2." The first layer of the model contains three parallel Conv1D layers with kernel sizes of 1, 3 and 5. The features extracted with different kernel sizes are summed together and transferred to the second Conv1D layer, where kernel sizes are set to 5. The final Conv1D layer contains kernels that have the size of 9 so that a more extensive set of features can be evaluated together to form better features. Following Conv1D layers, a GRU layer was used to extract features according to the order of input feature sequence using recursive operations. It takes 122 elaborated feature tensors from the convolutional layer as input layer and produces an output. After various experiments, the size of the GRU layer was set to 128, which also determines the number of inputs for the following classification layer. Due to the number of classes, there is only one fully connected layer employed as a classifier. Since multiclass classification involves five-class, the number of units was set to 5, and the softmax activation function was selected to produce probabilistic output. A single sigmoid function to produce the binary output was used during experiments in the Binary classification case.

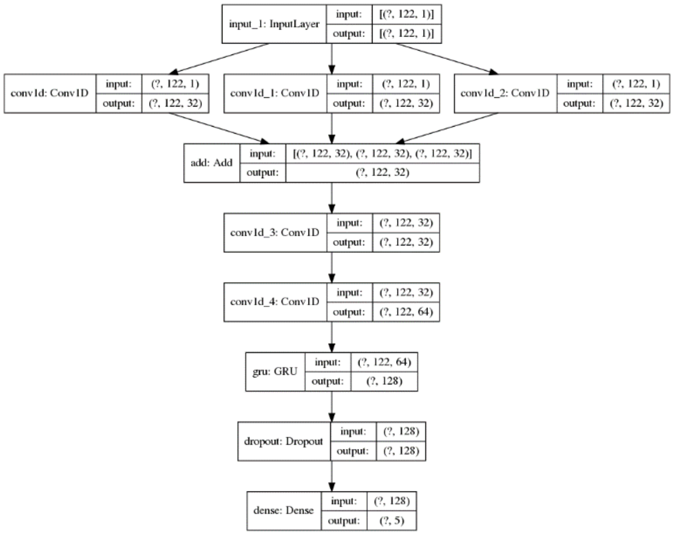

Fig. 2. The proposed deep learning model structure.

IV. EXPERIMENTAL RESULTS

The experimental computer consists of an AMD Ryzen 2700 eight-core processor, NVIDIA GeForce® GTX 1080 8 GB video card, and 16 GB of main memory. The experimental programs were implemented on Ubuntu 18.04 operating system using Python 3.7 with Keras 2.4.3 framework installed for deep learning utilities. Both models for multiclass and binary class classifications were trained with the RMSprop algorithm where learning rate and batch size were selected as 1e-4 and 128, respectively. The number of epochs is set to 200 for both experiments, and the best models according to validation values were saved using *ModelCheckpoint* class. Table II represents the confusion matrix for the binary classification model tested using 20% of the NSL KDD training dataset, which amounts to 25195 samples. The model can be able to classify 25166 samples correctly as an attack or not attack. Table III represents the case of five-class classification where the number of correctly classified samples is found to be 25161. Though the increased number of classes, the model still provides close results to binary classification. When the classes are examined, the worst-performing detection was found to be U2R, which has relatively few training samples compared to others.

In Table III, the results obtained with the proposed system are compared with other studies in the literature. The table contains the binary and multiclass results obtained with the NSL-KDD dataset. When Table IV is examined, it is seen that the accuracy rate of the proposed system in binary classification is 99.88%. When this value is compared with the recent studies in the literature, it is the best result in Table III only after the study of Santosh et al. [11]. The accuracy value for the recommended system for multiclass classification is 99.86%. When looking at the multiclass results in Table III, it is seen that it is the best and highest result. According to evaluations, the success of the proposed system was found to be better for five-class classification. The binary classification result of this study is also very close to the best work according to comparative studies.

TABLE II. CONFUSION MATRIX FOR BINARY CLASSIFICATION

	Normal	**Attack**
Normal	13458	11
Attack	18	11708

TABLE III. CONFUSION MATRIX FOR FIVE CLASS CLASSIFICATION

	Normal	**DoS**	**U2R**	**R2L**	**Probe**
Normal	**13442**	5	2	15	5
DoS	1	**9185**	0	0	0
U2R	2	0	**8**	0	0
R2L	0	0	0	**199**	0
Probe	2	1	1	0	**2327**

TABLE IV. THE PERFORMANCE COMPARISONS WITH RELATED WORKS ON NSL-KDD DATASET

Binary Classification			**Multiclass Classification**	
References	**Accuracy**		**References**	**Accuracy**
Diro-2018b-[15]	98.27		Wang-2018-[16]	86.35
Jiang-2019-[17]	98.94		Xu-2018-[9]	99.24
Abeshu-2018-[18]	99.20		Yin-2017-[19]	81.29
M. Al-Qatf-2018-[10]	99.41		Wisam-2020-[4]	98.77
Ömer-2020-[7]	99.50		Nathan Shone-2018-[8]	85.42
Wisam-2020-[4]	99.83		Binghao Yan-2018-[2]	99.35
Santhosh-2018-2-[11]	**99.91**		Yang-2019-[14]	97.45
Proposed Model	99.88		Proposed Model	**99.86**

V. CONCLUSIONS

This paper proposed a deep neural network model based on 1D convolutions and the GRU layer to process the input sequences in arrays for intrusion detection. The raw features obtained from the network packages in the form of arrays with 41 elements were converted to arrays with 122 attributes by one hot coding of some flags to process the input features better. Though the imbalanced nature of the dataset used in this study, the designed model can detect intrusions successfully after training the model using the class balancing parameter in Keras. The high success rate of the model was achieved with multiple convolutional layers and a recurrent layer for feature extraction. According to the test results, the model's accuracy for binary and five class classification reaches 99.88% and 99.86%, respectively. Although our model is lightweight and can detect intrusion detections successfully, our focus will be the faster and more accurate models on different datasets for future studies.

REFERENCES

[1] Y. Zhang, H. Zhang, X. Zhang, and D. Qi, "Deep Learning Intrusion Detection Model Based on Optimized Imbalanced Network Data," in 2018 IEEE 18th International Conference on Communication Technology (ICCT), 2018, vol. 2019-Octob, pp. 1128–1132.

[2] B. Yan and G. Han, "Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System," IEEE Access, vol. 6, pp. 41238–41248, 2018.

[3] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, 2018.

[4] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," Comput. Networks, vol. 168, 2020.

[5] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Syst., vol. 189, 2020.

[6] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," J. Netw. Comput. Appl., vol. 169, p. 102767, Nov. 2020.

[7] Ö. KASIM, "An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks," Comput. Networks, vol. 180, p. 107390, Oct. 2020.

[8] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[9] C. Xu, J. Shen, X. Du, and F. Zhang, "An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units," IEEE Access, vol. 6, pp. 48697–48707, 2018.

[10] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," IEEE Access, vol. 6, pp. 52843–52856, 2018.

[11] S. Parampottupadam and A.-N. Moldovann, "Cloud-based Real-time Network Intrusion Detection Using Deep Learning," in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018, pp. 1–8.

[12] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," IEEE Access, vol. 7, 2019.

[13] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[14] H. Yang, G. Qin, and L. Ye, "Combined Wireless Network Intrusion Detection Model Based on Deep Learning," IEEE Access, vol. 7, 2019.

[15] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," Futur. Gener. Comput. Syst., vol. 82, pp. 761–768, May 2018.

[16] Z. Wang, "Deep Learning-Based Intrusion Detection With Adversaries," IEEE Access, vol. 6, pp. 38367–38384, 2018.

[17] F. Jiang et al., "Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security," IEEE Trans. Sustain. Comput., vol. 5, no. 2, pp. 204–212, Apr. 2020.

[18] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," IEEE Commun. Mag., vol. 56, no. 2, pp. 169–175, Feb. 2018.

[19] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.