Available online at http://scik.org
J. Math. Comput. Sci. 11 (2021), No. 5, 5278-5295
https://doi.org/10.28919/jmcs/5921
ISSN: 1927-5307

INTRUSION DETECTION SYSTEM USING DEEP LEARNING METHODOLOGIES

AYUSH CHOUBEY, ADDAPALLI VN KRISHNA*

Department of Computer Science and Engineering, CHRIST University, Bengaluru, Karnataka 560074, India

Abstract: Intrusion Detection Systems (IDS) are the backbone that helps secure organizations and individuals from malicious internet traffic. Deep-Learning is another field of computer science that enables us to build productive Artificial Intelligence (AI) models that can be applied in a variety of fields. In this paper, we discuss the CSE-CIC-IDS2018 dataset for internet intrusion detection and provide a detailed study and analysis of various deep learning approaches that could be used to make a secure intrusion detection system. We test the accuracy of these algorithms and their effectiveness in detecting the malicious traffic for multiclass classification of the traffic in 14 different classes including benign traffic and malicious traffic. The outcome of which is to obtain a model framework based upon deep learning to build a usable model for an intelligent IDS that could potentially be used for real time data traffic security.

Keywords: deep learning; cyber security; intrusion detection system; ids2018.

2010 AMS Subject Classification: 00A71.

*Corresponding author:
E-mail address: adapalli.krishna@christuniversity.in

Received May 21, 2021

1. INTRODUCTION

With the advancement of various technologies in the past 10 years and rapid expansion of digital mediums such as handheld smart phones and Internet of Things (IOT), cyber-crime is more explosive than ever. With the people unaware of most of the daily exploits conducted upon them, it becomes a concerning situation. The targets for most of these exploits and attacks are critical infrastructures and organizations apart from individuals.

Cyber Security is the vast field of computer science that deals with the study of various technologies, processes, workflows, algorithms and networking with data to provide authenticity, reliability and security to the data while maintaining data integrity and provide recovery solutions. It encompasses a collection of mechanisms such as Access Control Lists (ACL), Authentication Systems, Secure Socket Layer (SSL) and Secure Shell (SSH).

Intrusion Detection Systems (IDS) provide us with a way to deal with these attacks by serving as an added layer of security against threat. IDS are a very intuitive way to deal with this issue as they are seamless and could be paired up with similar technologies such as access control methods and high grade encryption and authentication mechanisms such as AES.

The sheer number of threats are increasing on a daily basis and studying the network traffic data, one can get insights upon the malicious intent of the attacker by identifying the patterns of the data from existing attacks thus helping classify a benign data packet from a malicious one.

With the technological growth in the field of data science and massive parallel computing systems using arrays of GPUs to process thousands of data points in an instant, deep learning has become the new way to advance the field of Artificial Intelligence for its use in various applications. Deep Learning technologies enable us to improve the IDS models using trained algorithms to sniff out malicious packets and classify them on the basis of attack types. Many attacks that are classified as Zero- day attacks, which are the ones never seen before, usually are a variation on previously conducted attacks and thus could potentially be identified as a threat. Artificial Intelligence combined with the existing cyber security measures could pave a new way of securing ourselves from malicious intent on a network.

The problem encountered by most of the problems such as the one discussed above, is lack of abundant data. Data proves to be useful when it is present in an abundant quantity, is of the right format and contains important information. Since AI algorithms need abundant quantities of data to learn patterns in data for the problem in hand. The dataset discussed in this paper and used for training is the CSE-CIC-IDS2018 dataset. This is an intrusion detection dataset that contains real time internet traffic data that has been categorized into 14 different classes. One of them being benign traffic data and 13 others being various kinds of exploits. There are 80 columns that represent various fields such as port number of the data packet and so on. The Literature Survey section of the paper discusses further on the breakdown of the data set.

This paper is an in-depth analysis of deep learning algorithms such as Convolutional Neural Networks (CNNs). The Literature survey section of the paper discusses deep learning algorithms for an in-depth understanding. The Methodology section of the paper deals with how the models are applied with respect to the dataset in hand.

The paper also discusses a possible framework for a Deep learning based Intrusion Detection System to be used. This paper is aimed at beginners who are new to the field of artificial intelligence and plan to learn more applications of such. Also at professionals working on deep learning and cyber security applications for a deep insight on what to use and how to apply the concepts.

2. LITERATURE REVIEW

The studies in this paper can be categorized as follows:

Study of CSE-CIC-IDS2018 dataset.

In depth workings of Deep-Learning Algorithms.

Applications of AI in cyber security as well as its application in future relevance.

2.1. DATASET DESCRIPTION

CSE or the Communications Security Establishment and Canadian Institute of Cybersecurity Intrusion Detection Systems Dataset from 2018 contains network traffic data organized into 10 different files. With more than 60 crore data points and 80 columns.

2.2. STUDY OF DEEP LEARNING APPROACHES

Deep Learning is a subfield of Artificial Intelligence. The backbone of deep learning and the key differentiator between deep learning and traditional machine learning is the artificial neuron. Deep learning algorithms are made by constructing networks of these artificial neurons called an artificial neural network (ANN) or simply neural networks. Some of the networks discussed below are:

- **DNN:** Deep neural networks are a model that consists of multiple layers of perceptron (MLP) where each perceptron in the current layer is connected to each other perceptron on the other layer. The number of layers should exceed three. Feed forward neural networks (FFN) are the DNNs that can contain different activation functions other than the perceptron model.

  A layer L in a DNN can be defined as $D_L\ (a_L, f_L, g_L)$with w_L, b_L where:

  a_L: number of neurons present in the layer L;

  f_L:represents the transformation with the help of weight matrix $w_L$and bias matrix b_L;

  g_L: the transformation function between layer $L - 1$and L.

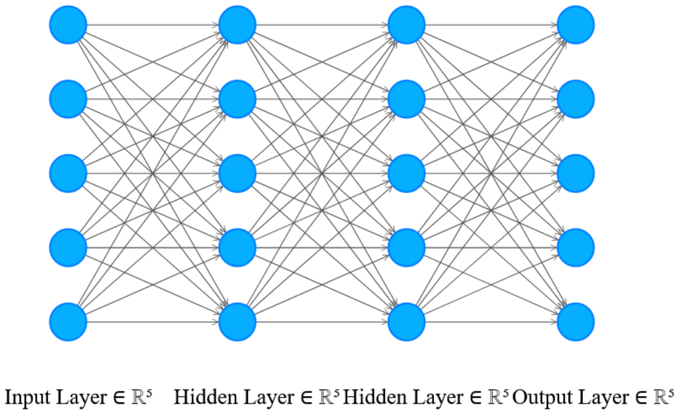

Figure 1. DNN Architecture

- **RNN:** A Recurrent Neural Network (RNN) is different from a regular feed forward neural network as the outputs from the calculation of the neurons are provided as a feedback to the neuron. There are various kinds of RNNs. The most popular one being used currently is LSTM-RNN. Long Short Term Memory (LSTM) consists of long sets of neurons that have short term memory of the feedback provided by the previous iterations of calculations.

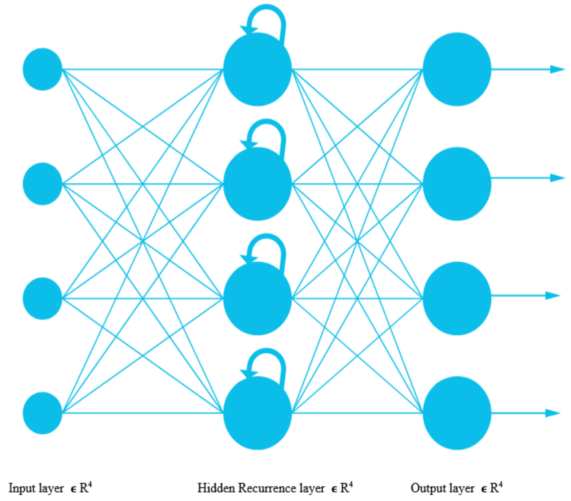
Input layer ϵ R^4
Hidden Recurrence layer ϵ R^4
Output layer ϵ R^4

Figure 2. RNN Architecture

- **RBM:** Restricted Boltzmann Machine (RBM) consists of two layers of Neural Networks. One is the visible layer and other is the hidden layer. This is an example of a generative neural network kind. The two layers are fully connected but the hidden cells are not aware of other hidden cells in the network. The visible neurons are connected to all other hidden neurons through weights, biases and constants.

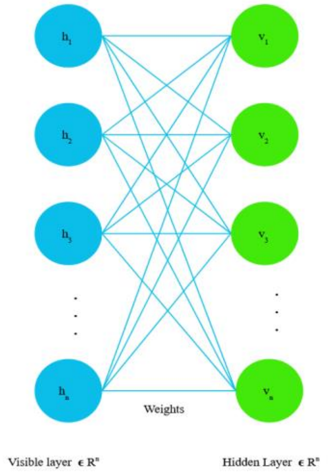

Figure 3. RBM Architecture

- **DBN:** Deep Belief Networks (DBN) consists of multiple layers of RBMs. The job of the visible layers is to present the data to the network and hidden layers learn the patterns in the data.

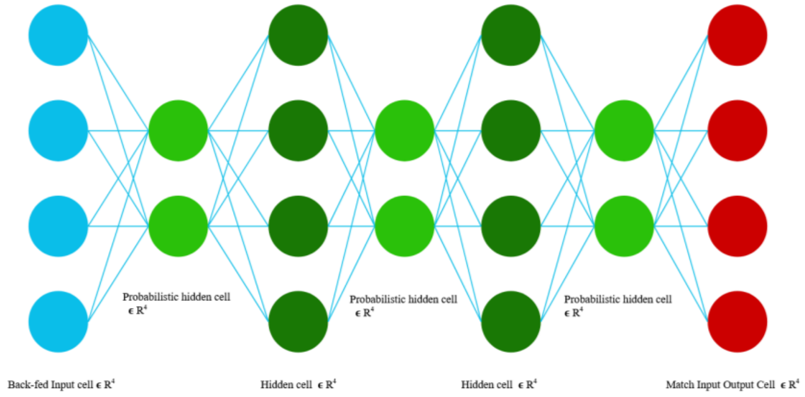
Probabilistic hidden cell $\in R^4$
Probabilistic hidden cell $\in R^4$
Probabilistic hidden cell $\in R^4$
Back-fed Input cell $\in R^4$
Hidden cell $\in R^4$
Hidden cell $\in R^4$
Match Input Output Cell $\in R^4$

Figure 4. DBN Architecture

- **DAE:** Deep Auto Encoder (DAE) are a set of two kinds of neuron layers. One layer is known as the encoder layer and the other is called the decoder layer.

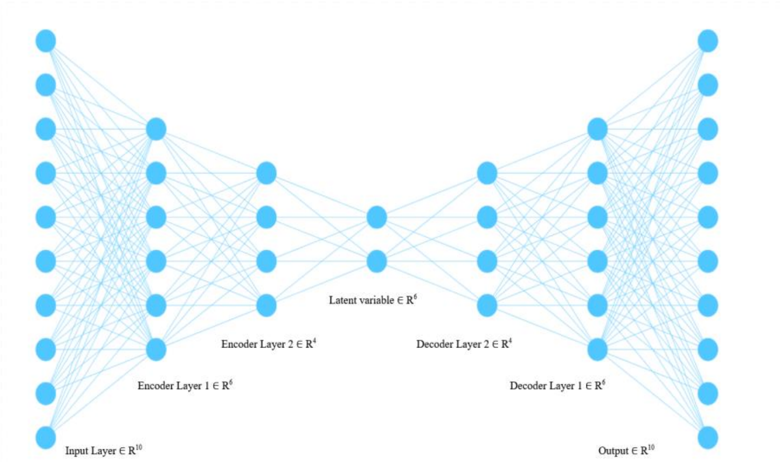
Latent variable $\in R^6$
Encoder Layer 2 $\in R^4$
Decoder Layer 2 $\in R^4$
Encoder Layer 1 $\in R^6$
Decoder Layer 1 $\in R^6$
Input Layer $\in R^{10}$
Output $\in R^{10}$

Figure 5. DAE Architecture

- **CNN:** A CNN or a Convolution Neural Network is popularly used for image recognition in general use. The Neural network itself is very similar to a normal feed-forward neural network except it has special layers known as convolutional layers. The job of convoluted layers is to pass the input through a matrix of ‘n x n’ defined for that particular layer and it changes the input for further segmentation. The filters are used to detect features in the input provided. At the start of the layers, the initial filters may detect something trivial as an ‘edge’, but as the network grows deeper, the filters are successfully able to detect whole objects. The process of passing every ‘n x n’ successive pixel to the filters is called convolution. The pooling layers reduce the images in size by performing various operations such as max-pooling and average-pooling.

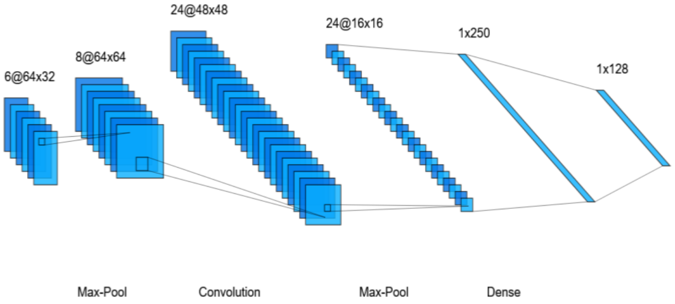

Figure 6. CNN Architecture

2.3. RELATED WORK

Ferrag et al. in [1], presents a similar study using CSE-CIC-IDS2018 dataset and Bot-IOT based dataset using generative deep learning approaches to test how the algorithms hold up in regards to the datasets. They present seven algorithms and test their efficiency, accuracy and false alarm rate. These algorithms are pitched against each other to obtain which ones prove to be more stable. The CNN model proposed here gives a 97% accuracy rate as compared to the 96% by the RNN-LSTM model and 82-97% of the DNN model.

The study conducted by Berman et al. in [2], provides an insightful look upon the workings of various deep learning neural networks such as general adversarial networks, deep auto-encoders and restricted Boltzmann machines. Their paper also discusses the various kinds of attacks such as spams, malware based attacks, bot based attacks and SQL injection. Their work provides a basis for other researchers to advance the cyber security field using deep learning as its core.

Xin et al. in [3], provide a study on the challenges faced by deep learning and machine learning to be applied in the field of cyber security. They work upon the NSL-KDD dataset and DARPA

IDS dataset to provide a detailed study of machine learning algorithms such as Support Vector Machines, K-Nearest Neighbor, Decision trees and some deep learning methods such as CNN, RNN and DBN. Their work provides a summary and culmination of other similar works and studies conducted over a period of three years in the field of artificial intelligence and cyber security. This literature review also provides information on other important datasets used and their success rates on various algorithms discussed above.

Tuor et al., in [4], work on insider threat detection for the benefit of organizations. They work upon the CERT insider threat dataset and use a novel deep recurrent neural network model to achieve 95.53% accuracy on detecting insider threats. Their work guides through the process of deep learning and its application. They propose an online architecture for deep learning that goes through the streaming logs and detects insider threats. This outperforms standard techniques such as SVMs and PCA.

Roopak et al. in [6] propose various deep learning models for cybersecurity threat detection in IOT based networks. They work upon the CSE-CIC-IDS2017 dataset and with an accuracy of 97.16%, predict DDOS attacks. The model they proposed was based upon CNN + LSTM networks. They also show a brief comparative study with regards to machine learning algorithms.

Alom et al. presented an approach to build IDS using KDD-99 dataset in [7]. Using auto encoders and restricted Boltzmann machines, they reached 91.86% and 92.12% accuracy which is significantly greater than unsupervised extreme machine learning algorithms. Pairing K-Means clustering and deep learning approaches proved to be a success as presented here.

In their paper [8] Geluvaraj et al. state that with the advancement of cybersecurity and machine learning, so come newer kinds of attack which may prove to be fatal. These attacks will be difficult to detect using the traditional models of machine learning. Cybersecurity will be aided by smart AI to build better infrastructure for security.

Jian-hua in [9], discusses the intersection of the two fields of cybersecurity and artificial intelligence. The work consists of studying the areas of research that is going on regarding how cyber threats could be detected using AI aided models, the attacks that could be conducted on those AI models themselves and provide insights on some defense mechanisms. Using this work, they propose a way to build encrypted neural networks that are secure themselves and could be used for cybersecurity threat detection.

Vinaykumar et al. propose Scalable-Hybrid-IDS-AlertNet(SHIA) that could be used in real time to effectively monitor the traffic and detect threats if any. They work in [10] upon the KDD-99 dataset, CIC-IDS2017, NSL-KDD with 1000 epochs on each model with varying learning rates to benchmark and test their proposed model. They achieve an average of 97% accuracy on different models on the KDD-99 dataset.

Farhan et al. used the dataset collected from Google Code Jam to perform cyber security threats detection on IOT systems in [5]. The deep neural network is used to detect software piracy and malware infection of files.

3. METHODOLOGY

Every Artificial Intelligence (AI) problem has a singular starting point, i.e. the dataset. CSE-CIC-IDS2018 dataset, initially created by University of New Brunswick to conduct a study on various kinds of DDOS attacks, contains about 16 million data points and is available for public use. We use Google colab environment and python-pytorch library to make our model.

3.1. TYPES OF ATTACKS

DDOS attacks-HOIC: High Orbit Ion Cannon (HOIC) is an open source tool which can hide the perpetrator’s geolocation once the attack is complete. Using this, even a small group of hackers can conduct a massive-scale DDOS attack.

DOS Attacks-LOIC-UDP: Low Orbit Ion Cannon (LOIC), unlike HOIC is not capable of obstructing the attacker’s geolocation by hiding the IP address, but this stress testing tool can use UDP, ICMP and TCP protocols to successfully conduct a DOS attack.4

DOS Attacks-Goldeneye: Golden eye uses HTTP to conduct a denial of service attack. This uses a technology called KeepAlive which forces the http connection to remain online and can easily take control of the cache.

DOS Attacks-Hulk: This type of DOS attack is capable of penetrating through the server’s cache and attacking its base resources such as memory. This uses an exorbitant volume of corrupt traffic to create a successful attack.

DOS attacks-SlowHTTPTest: These are low bandwidth attacks that target application layers to create a denial of service. The main objective behind these attacks is to use up all of a server's cpu resources.

DOS attacks-Slowloris: This attack allows a single penetrator to carry on a DOS attack on a server by opening a large number of connections with the server and sending incomplete bits of http requests periodically.

SQL Injection: This is a direct attack on the database of a server. Attackers ask users of the victim system to provide an input and then make them run a SQL script that compromises their database, giving the penetrator access to all the privileges of that user in that database.

SSH-Bruteforce attack: This attack is one of the most primitive types of attacks where an attacker would try to penetrate the system by keeping dictionaries of usernames and passwords and then trying them one by one once a ssh connection is established.

FTP-Bruteforce attack: This is a very similar attack to SSH-BF attack. Here the attacks are conducted to gain FTP credentials and server access.

Web-Bruteforce attack: This attack is conducted in various ways but the underlying factor being the hacker sending requests using some known values and then analyzing the response by the server to get new information. This is done repeatedly until one gains access to the server.

XSS-Bruteforce attack: This is an attack conducted on a victim's browser. Known as Cross Site Scripting (XSS), the hacker runs special javascript code in the http packet received by the victim. The victim's display is controlled by the hacker.

Infiltration: This is a large scale attack. Once the hacker gets into one of an organization's systems, he tries to learn of other devices and slowly corrupts them all.

Bot based attacks: Networks of infected devices are controlled by the hacker on the web to send out malwares to the victims. These systems are programmed to do so, hence they become the bots on the web. The network itself is called Botnet.

3.2. Preparation of Data

The data contains more than 16 million data points. This big data needs to be shortened to a usable amount. Since there are 10 different files of datasets, we iterate through each file and take 10 thousand samples from each attack kind of attack. Since each file contains benign data as well, we only take 2 thousand data points from the benign category. After combining the resultant data-frames and removing redundant rows, rows with missing data and improper values such as infinity and NAN, we further reduce the data-frame to contain 170 thousand data points.

After some manual feature selection, the data-frame consisted of 170 thousand rows and 78 columns. Using a min-max-scaler, we normalize the data between the feature range of 0-1. The data-frame is then split into training and testing data with 0.3 test-split constant. This means 30% of the data is kept for testing purposes and the remaining is kept for training purposes.

3.3. Deep Learning and IDS Framework Model

Intrusion detection is done in two steps. First the model, after training and learning the various parameters, tries to detect whether the traffic passing through is benign or not. If the traffic is detected to be benign, it is successfully passed to the next layer. In the case of traffic being malicious, it is passed to the next step of identifying the attack type. This is done by another model that does the classification for the attack types.

This proposes two kinds of classification problems. Once being binary classification and the other, multi-class classification.

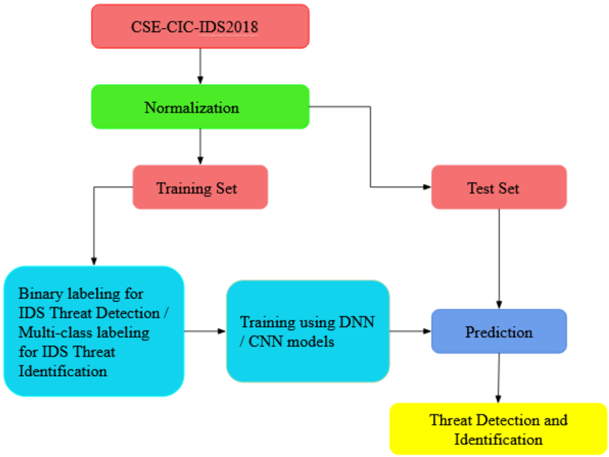
CSE-CIC-IDS2018
Normalization
Training Set
Test Set
Binary labeling for IDS Threat Detection / Multi-class labeling for IDS Threat Identification
Training using DNN / CNN models
Prediction
Threat Detection and Identification

Figure 7. IDS Framework Architecture

Deep Neural Network model.

The deep neural network model consists of multiple layers of neurons that take the traffic data with 78 input features as an input vector and then give out the required number of outputs based upon the problem at hand, whether it being binary or multi-class.

The activation function used in this case is ReLU activation which is coupled with Batch-Normalization to counter the zero effect ReLU can produce as well as help to reduce overfitting in the training process. The learning optimizer used is Adamax, a variant of Adam optimizer, with a learning rate of 0.0001. We learnt that the model performs best when the training is done in batches of 64 data points and if the model is stopped early or if it keeps checkpoints on the weights and biases.

Convolutional Neural Network model.

The Convolutional Neural Network (CNN) model provided many challenges, the primary of which being that the data is not spatially arranged. This means that although there is a deep resemblance and connection between many columns, they are not aligned completely. This also means we need to convert the input vectors to an image vector with multiple input channels to provide with the best learning.

After converting the input vector into an image like format, we create a convolutional neural network architecture. This architecture was built using GoogLeNet as the backbone, modifying it till it produced a viable result. The activation function used in the fully connected layers is ReLU. Batch normalization is done to reduce overfitting. The training optimizer used is Adamax with a learning rate of 0.0001.

4. RESULTS

4.1. TESTING PARAMETERS

The testing parameters for the model are as follows:

Precision

$$precision = \frac{TP}{(TP + FP)}$$

Recall

$$recall = \frac{TP}{(TP + FN)}$$

F1-Score

$$f1\ score = \frac{2 * precision * recall}{(precision + recall)}$$

Accuracy

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

4. DNN MODELS

DNN-Threat Identification.

The model achieved an accuracy score of 94.83 % on the training dataset and 94.58% on the testing dataset.

Table 1 shows the results of DNN-threat identification model

Threat	**Precision**	**Recall**	**f1-score**
No	0.85	0.82	0.84
Yes	0.95	0.96	0.96

DNN-Threat Classification.

The model achieved an accuracy score of 87.99 % on the training dataset and 88.2% on the resting dataset.

Table 2 shows the results of DNN-threat classification model

Classification	**Precision**	**Recall**	**f1-score**
Benign	0.85	0.83	0.84
Bot	0.63	0.84	0.72
Web-BF	0.98	0.99	0.99
XSS-BF	1.00	1.00	1.00
DDOS-HOIC	0.99	0.99	0.99
DDOS-LOIC-UDP	0.51	0.51	0.51
DOS-Goldeneye	0.99	0.99	0.99
DOS-Hulk	0.51	0.51	0.51
DOS-SlowHTTPTest	0.51	0.51	0.51
DOS-Slowloris	0.76	0.51	0.61
FTP-BF	0.76	0.86	0.81
Infiltration	0.99	0.98	0.99
SQL-Injection	0.99	1.00	1.00
SSH-BF	1.00	0.99	0.99

4.3. CNN MODELS

CNN-Threat Identification.

The model achieved an accuracy score of 94.2 % on the training dataset and 95% on the testing dataset.

Table 3 shows the results of CNN-threat identification model

Threat	Precision	Recall	f1-score
No	0.85	0.90	0.87
Yes	0.97	0.96	0.97

CNN-Threat Classification.

The model achieved an accuracy score of 90.01 % on the training dataset and 89.29% on the testing dataset.

Table 4 shows the results of CNN-thread classification model

Classification	Precision	Recall	f1-score
DOS-Slowloris	1.00	1.00	1.00
Infiltration	0.84	0.84	0.84
SSH-BF	1.00	1.00	1.00
DOS-SlowHTTPTest	0.72	0.55	0.63
DDOS-LOIC-UDP	1.00	1.00	1.00
SQL-Injection	0.88	0.38	0.53
Benign	0.87	0.88	0.87
DOS-Hulk	1.00	1.00	1.00
Bot	1.00	1.00	1.00
DDOS-HOIC	1.00	1.00	1.00
DOS-Goldeneye	1.00	1.00	1.00
Web-BF	0.71	0.76	0.74
XSS-BF	1.00	0.46	0.63
FTP-BF	0.64	0.79	0.71

5. Conclusion

In this paper, we conducted a study in the field of cyber security and artificial intelligence and various areas of research that include Intrusion Detection systems and Deep Learning. We learnt about the CSE-CIC-IDS2018 dataset and the types, methodologies, and technologies behind the attacks. We learnt about some deep learning models and how neural networks are used to construct them. Using this knowledge, we proposed two different deep learning architectures and models to make a two-step IDS with intrusion detection and threat classification. We then performed a comparative study based upon the results achieved by these two architectures and four models using standard benchmarks such as accuracy, precision, recall, and f1-score. This helped us conclude a generalized framework for an IDS that could be built using deep learning methodologies.

Conflict of Interests

The author(s) declare that there is no conflict of interests.

References

[1] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, J. Inform. Security Appl. 50 (2020), 102419.

[2] D. S. Berman, A. L. Buczak, J. S. Chavis, C. L. Corbett, A survey of deep learning methods for cyber security, Information, 10(4) (2019), 122.

[3] Y. Xin, L. Kong, Z. Liu, et al. Machine learning and deep learning methods for cybersecurity. IEEE Access, 6 (2018), 35365-35381.

[4] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, S. Robinson, Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams, ArXiv:1710.00811 [Cs, Stat]. (2017).

[5] F. Ullah, H. Naeem, S. Jabbar, et al. Cyber security threats detection in internet of things using deep learning approach. IEEE Access, 7 (2019), 124379-124389.

[6] M. Roopak, G. Yun Tian, J. Chambers, Deep Learning Models for Cyber Security in IoT Networks, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Las Vegas, NV, USA, 2019: pp. 0452–0457.

[7] M. Z. Alom, T. M. Taha, Network intrusion detection for cyber security using unsupervised deep learning approaches, in: 2017 IEEE National Aerospace and Electronics Conference (NAECON), IEEE, Dayton, OH, 2017: pp. 63–69.

[8] B. Geluvaraj, P. M. Satwik, T. A. Ashok Kumar, The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace, in: S. Smys, R. Bestak, J.I.-Z. Chen, I. Kotuliak (Eds.), International Conference on Computer Networks and Communication Technologies, Springer Singapore, Singapore, 2019: pp. 739–747.

[9] J. H. Li, Cyber security meets artificial intelligence: a survey, Front. Inform. Technol. Electronic Eng. 19(12) (2018), 1462-1474.

[10] R. Vinayakumar, M. Alazab, K. P. Soman, et al. Deep learning approach for intelligent intrusion detection system. IEEE Access, 7 (2019), 41525-41550.

[11] A. Javaid, Q. Niyaz, W. Sun, M. Alam, A deep learning approach for network intrusion detection system, in: Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS), ACM, New York City, United States, 2016.

[12] Z. Wang, Deep learning-based intrusion detection with adversaries. IEEE Access, 6 (2018), 38367-38384.

[13] S.S. Roy, A. Mallik, R. Gulati, M.S. Obaidat, P.V. Krishna, A Deep Learning Based Artificial Neural Network Approach for Intrusion Detection, in: D. Giri, R.N. Mohapatra, H. Begehr, M.S. Obaidat (Eds.), Mathematics and Computing, Springer Singapore, Singapore, 2017: pp. 44–53.

[14] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, M. Marchetti, On the effectiveness of machine and deep learning for cyber security, in: 2018 10th International Conference on Cyber Conflict (CyCon), IEEE, Tallinn, 2018: pp. 371–390.

[15] S. Mahdavifar, A. A. Ghorbani, Application of deep learning to cybersecurity: A survey. Neurocomputing, 347 (2019), 149-176

[16] A. Sharma, E. Vans, D. Shigemizu, K.A. Boroevich, T. Tsunoda, DeepInsight: A methodology to transform a non-image data to an image for convolution neural network architecture, Sci. Rep. 9 (2019), 11399.