IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

Deep Learning Latent Representation for IOT Anomaly Detection

Shreya Balaraman[1], Joshua Geoffery Ebenezer[2], G. Paavai Anand[3]
Department of Computer Science and Engineering[1,2,3]
SRM Institute of Science and Technology, Vadapalani Chennai, India

Abstract: *The Internet of Things (IoT) refers to huge network of intelligent device able to gathering, storing, analyzing, and communicating data. Intrusion detection for the IOT is a swiftly advancing. The IoT ecosystem is more challenging to defend than traditional information technology systems due to limited resources and huge amount of smart devices. Unknown IoT-based attacks are significantly more harmful since they have the ability to outperform the bulk of recent security solutions and require time to detect and remediate. In this section, we will demonstrate how representation learning, namely CNN and LSTM-based anomaly detection approaches, may be utilised to accurately identify unknown threats*

Keywords: IOT; Anomaly Detection; Botnet; CNN; LSTM; Autoencoder.

I. INTRODUCTION

The quick advancement of the Internet of Things, brings huge advantages to everyday modern life. IOT has helped a variety of applications in recent years, including those in healthcare, finance, agriculture, the industrial sector, transportation, detecting systems, etc. Also, IOT has had a significant influence on daily life, which motivates developers to create new techniques. It keeps expanding as more devices are connected and more data are produced, providing fresh perspectives and chances for breakthroughs.

Yet, if more data are floating, they become more susceptible to environmental changes. IOT data protection is crucial for the technological advancements of today. In today's IOT world, cyber security plays a critical role in the information management system. Attacks like Denial of Service and many similar hacking tactics are frequently utilized in penetrating the sensitive data as IOT and web frameworks have grown easily accessible [8].

The intrusion detection systems are crucial to protect the network from malware [9]. The detection system that is being introduced is a deep learning on which three types of autoencoders are used.

Hybrid CNN-LSTM is an effective deep learning algorithm to evaluate, prepare and determine the accurate information in the given data. The evaluation of accuracy, precision, recall and F1score show a high performance rate compared to other deep learning models [5]. The purposed of Hybrid CNN-LSTM is that, this algorithm can handle massive amount of data and given a mixture of unknown, anomalous and normal data, a complex algorithm is required to detect quickly and effectively to attain best results.

Autoencoders are a type of artificial neural network which reduces the dimensionality of input data. There are two parts in autoencoder, encoder - this compresses or reduce noise of input data and decoding - revive the input data. Deep Autoencoder, Sparse Deep Autoencoder, Sparse Deep Denoising Autoencoder are the three types of autoencoder used in this experiment . These methods will support the data from segregation to give a comprehensible detected data . The greatest advantage of autoencoders is that, they can reduce the noise of the input data which help the models to work efficiently and give robust response. As in [12] autoencoders and Principle Component Analysis are effective methods for dimensionality reduction. Some study show that classification of binary and multinomial variables are productively used to reduce dimensionality.

But compared to PCA, autoencoders give more accurate results.

II. RELATED WORK

A new representation learning method for supervised machine learning anomaly detection created several auto encoders for building a representation learning from the input data. The data categorization methods, as well as

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

additional attributes collected from well- known IOT dangers. were applied. Numerous tests on nine current IoT datasets show that a new latent representation may improve the effectiveness of supervised learning algorithms for identifying unknown IoT attacks [1], [13]. A research which combines CNN and LSTM to develop an effective Intrusion Detection System capable of tracking geographical and time- varying network traffic characteristics. Regularisation algorithms improve zero-day intrusion detection performance. Regularisation techniques improve the efficacy of CNN algorithms in detecting new invasions [5]. To detect irregularities in an Internet of Things network, this research suggests leveraging mutual information and a deep neural network. Experiment findings reveal that the DNN-based Network Intrusion Detection System model outperforms well-known deep learning models in terms of model accuracy, with a 0.57-2.6% increase and a 0.23-7.98% reduction. Furthermore, it was revealed that utilising only the 16- 35 top features determined via MI, rather of the 80 features in the dataset, resulted in nearly no performance reduction but did aid to reduce overall model complexity [4]. A deep learning-based technique for specialised intrusion detection to assure the network's high security. [6]—fulfil the goals of feature categorization and harmful data detection, a CNN- based technique is used. After comparing the results of the algorithm to that of competing algorithms in space, comparison findings are made. These findings demonstrate the practicality of the proposed study for detecting data packet assaults, as well as the usage of the suggested network security approaches. Another approach, DNN model and a Deep Learning enabled LSTM Autoencoder were developed and tested to be much better in terms of accuracy.Built NIDS models based on stacked LSTM and bidirectional LSTM LSTM variations of LSTMs and evaluated their effectiveness on the datasets [10]. A deep learning intrusion system for the Internet of Things (IoT) that can learn and gather reliable and practical characteristics that aren't greatly impacted by unstable conditions. The classifier then employs these characteristics to increase the accuracy with which it can detect untrue IoT data. In order to get features that are resistant to the varied IoT environment, the suggested deep learning model employs a noise reduction autoencoder [6]. Convolutional neural networks are used in this study because they are an excellent choice for detecting and categorising anomalies since they can automatically identify significant attributes in incoming data and execute faster computations[7]. [3]—proposed convolution technique is validated by using multiple detection datasets. On the subject of accuracy, in the matter of precision, respecting recall, and F1 the proposed binary and multiple-class classification models beat previous deep learning implementations. A sequencing monitoring architecture, and machine learning attack detection system. To create a compact detection system with great performance, a powerful feature selection approach is applied. The findings show that the suggested architecture is capable of identifying botnet- based assaults efficiently. Other sub-engines for the detector can be created to accommodate totally new types of assaults. Various machine learning techniques were studied to get an overall detection rate [2], [11]. In an article, at first it examines the security of IoT systems using an analytics approach, categorising using a machine learning approach and recognizing IoT
dangers. Assess the performance of machine trying to learn-trained models for forecasting using data gathered over a nine-month period as our testbed, and give design guidelines and a general framework for designing secure IoT systems [8]. A proof of concept using blockchain technology to protect home networks, Internet of Things devices, and Internet service providers . The findings support the idea of a distributed network for exchanging data on cyberthreat data and safeguarding various stakeholders. Despite the fact that the experimental analysis outlined in these study is only successful for known IoT attacks, it will be unsuccessful in dealing with modern IoT threats [9].

III. METHODOLOGY

A new method is implemented to improve the performance of anomaly detection algorithms. To distinguish between normal and abnormal samples in the latent space, given a novel variable to the loss function of these autoencoders. This latent representation is subsequently introduced into filters to detect unanticipated information. To put our theories to the test, we conduct extensive experiments with IoT botnet datasets. The experimental findings demonstrate that incorporating latent features considerably enhances the performance of basic classifiers when compared to learning from the primary characteristics. Following an extensive assessment of the latent representation's properties in distinguishing novel assaults, running the intersect-dataset test, and verifying its durability with different hyperparameter values. The study discusses how the proposed models might be used in real-world scenarios. The latent

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

feature space is separated into two discrete, limited sections, one for known attacks and the other for standard data. To create such a latent representation, we modified three autoencoder versions, yielding three regularised models.

Classification:

The classifiers in the deep learning models namely the input layer, hidden layer, dropout layer and output layer are intended to be the most important layers of neural network.

Auto Encoders:

In order to detect abnormalities in time series data produced by IoT devices, autoencoders may learn complicated patterns in the data, including temporal relationships. In IoT devices with limited resources, they can develop an effective representation of the data, which can lower the computational cost of anomaly detection. Last but not least, autoencoders have the ability to spot both local and global irregularities in data, making them useful for spotting both broad-scale assaults and focused attacks on particular IoT devices

Convolutional Neural Network (CNN):

The CNN network is trained on a dataset of typical network traffic before being used to categorise fresh network traffic data as normal or abnormal in IoT networks. As compared to typical network traffic, anomalies in the network traffic data will provide various feature representations. As a result, using the collected characteristics, CNN may learn to differentiate between regular and abnormal network data. Using CNNs for anomaly detection in IoT networks has significant drawbacks, though. One drawback is that CNNs could need a lot of training data to develop an accurate model of typical network traffic. As a result, gathering and categorising a large enough set of training data can be difficult and time-consuming. Another drawback is that CNNs might not be good at spotting abnormalities that differ considerably from typical network data.

Long Short-Term Memory (LSTM):

By employing the network to identify new network traffic data as either normal or anomalous after training it on a dataset of typical network traffic, LSTM is used for anomaly detection in IoT networks. As compared to typical network traffic, anomalies in the data will produce unusual patterns in the sequence. They are useful for spotting abnormalities in time series data produced by IoT devices because they may capture long-term dependencies in the sequence. Second, since LSTMs may be trained end-to-end, the network can learn to automatically extract the characteristics that are most pertinent to anomaly detection from the data. Lastly, depending on the availability of labeled training data, LSTMs may be applied to supervised and unsupervised anomaly detection. Nevertheless, just with CNN, employing LSTMs for anomaly detection in IoT networks has significant restrictions. One drawback is that LSTMs could need a lot of training data to develop an accurate model of typical network traffic. As a result, gathering and categorising a large enough set of training data can be difficult and time-consuming. Another drawback is that LSTMs might not be good at spotting abnormalities that differ considerably from typical network traffic.

Hybrid CNN-LSTM Model:

Convolutional Neural Network and Long Short-Term Memory, two potent deep learning architectures, are combined in the hybrid LSTM-CNN model, which has been demonstrated to be successful for anomaly detection in IoT networks. The hybrid model's LSTM component detects temporal connections in the sequence while the CNN component extracts spatial characteristics from the input data. In order to detect abnormalities in IoT networks, it is critical for the

model to be able to collect both geographical and temporal data. There are various benefits to adopting the hybrid LSTM-CNN model over using either architecture by itself. Initially, pre-processing the input data with the CNN component can make the LSTM model less complicated and perform better. Second, the LSTM component is useful for identifying abnormalities in time series data because it can capture long-term relationships in the sequence. The hybrid model may also learn to recognise intricate patterns in the data, which makes it useful for spotting abnormalities that could be hard to spot using more conventional techniques. The hybrid LSTM-CNN model has been used to analyse

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

video data, network traffic data, sensor data, and other IoT data sources. The hybrid model has been demonstrated to be successful in spotting data abnormalities in each instance.

In conclusion, the hybrid LSTM-CNN model offers a quick and accurate way to find anomalies in IoT networks. It is ideal for identifying both known and unidentified anomalies because to its capacity to collect both geographical and temporal characteristics, manage changing data durations, and spot complicated patterns in the data.

IV. ARCHITECTURE

The architecture of this project consist of four segments. The data from the dataset is derived and preprocessed. After preprocessing further the data are cleaned, trained and tested and a new set of data are derived from the process of canonicalization.

Normalization basically calculates the total data and number of noisy data and its percentage. These trained data are put into the process included in hybrid CNN - LSTM. Here the data are trained again going through numerous layers of deep neural network. The three types of autoencoders are used as a part of this process. Finally, the given results are evaluated and showed as graphs. Figure 1 shows the architecture diagram of the project. Finally, the given results are evaluated and showed as graphs. Figure 1 shows the architecture diagram of the project.

V. DATASET

The KDD Cup 99 dataset is popular for assessing intrusion detection systems. DARPA (Defence Advanced Research Projects Agency) established it to support research in the field of network intrusion detection. The dataset connection records that have been labeled as normal or attack comprises a significant number of network connection records that have been labeled as normal or attack. The dataset contains 24 different types of assaults with varied degrees of Over the course of nine weeks, the attacks were simulated in a military network environment [14].

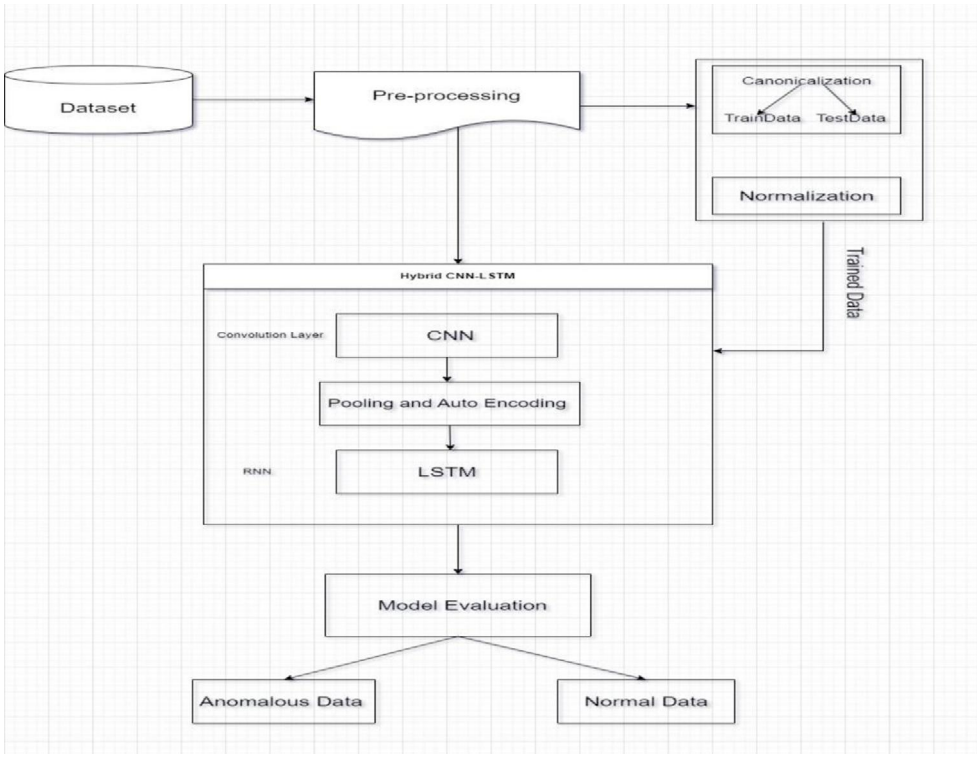

Figure 1: Architecture diagram and Modules

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

VI. MODULES

A) Preprocessing:

It imports the relevant libraries, defines the lists of column names to be eliminated, and sets up some basic data cleaning procedures to handle missing and infinite values in specific columns during preparation.

B) Canonicalization:

The Local Outlier Factor (LOF) method is used to detect abnormalities in network traffic data. The train() function loads the training dataset, runs the LOF algorithm on it, and provides the preprocessed dataset, as well as the top 10% highest outlier scores and column names. Each instance is scored by the LOF algorithm based on its distance from its k-nearest neighbours. In the LOF method, the contamination parameter determines the fraction of outliers in the dataset. The test() function imports a test dataset, adds each instance to the preprocessed dataset, runs the LOF algorithm on the revised dataset, and outputs a list of binary labels depending on the cutline score (1 for inliers, -1 for outliers). The lowest score of the top 10% of occurrences in the training dataset is used as the cutline score.

C) Normalization:

Here, we use the DBSCAN method to conduct clustering on a dataset imported using the Preprocessing.load_data function. The dataset is initially scaled using the scikit-learn library's StandardScaler. The DBSCAN algorithm is then applied to the scaled dataset through the eps and min_samples parameters. The total amount of data, noise data, and noise percentage from total data are then computed and printed.

D) Hybrid CNN-LSTM model:

It reads a network intrusion detection dataset, preprocesses it, then uses MinMaxScaler to scale continuous features. This scales the characteristics from 0 to 1. It also creates a function that categorises the attack types into five distinct groups based on the type of attack, and assigns a new label to each sample as a result. "Normal", "Dos", "PortScan", "DDoS", and "Probe" are the new designations. Then it shows how a denoising autoencoder is utilised to detect anomalies in network intrusion detection. Keras is used to build the autoencoder, which has an input layer, output layer, two dense layers with ReLU activation function and L2 regularisation, an encoder layer, another concentration layer activation function and L2 regularisation, an encoder layer, another concentration layer with the activation function, and a decoder layer with activation function.After the denoising the data, the implementation of three types of autoencoder is performed to detect the anomalies using.

E) Deep Autoencoder:

A hidden layer of 64 neurons, followed by a layer with 8 neurons, and then another layer with 64 neurons, and a final output layer with the same number of features as the input.

The model is trained using mean squared error loss and the adam optimizer. Regularization is applied to the first layer using L2 regularization with a strength of 10e-3.

Sparse Deep Autoencoder:

This is similar to Deep Autoencoder architecture but without regularization. This model is also trained with mean squared error loss and the adam optimizer.

Sparse Deep Denoising Autoencoder:

To reduce the noise in the input data, a dropout layer is introduced before the input layer. The rest of the architecture has similarities to that of the Sparse Deep Autoencoder.

This model is also trained with “mean square error loss” and an optimizer called “Adam”.

After training each model, the code predicts the anomalies in the testing set by applying a threshold to the loss calculated between the input and the output of the autoencoder. If the loss is above the threshold, the data point is classified as an anomaly. Finally, it prints the performance of each model on the testing set, including accuracy, recall, precision, and F1 score and the detection rate of anomalies for each class.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

VII. RESULTS

The graph (Figure 2) shows the plots of the loss distribution of Normal Data and Attacked data against the predicted label; that is, of where the red line represents the threshold value. The confusion matrix show the concentration of each data at the between 2000 to 12000. The maximum threshold reached for any given data is upto 8000.

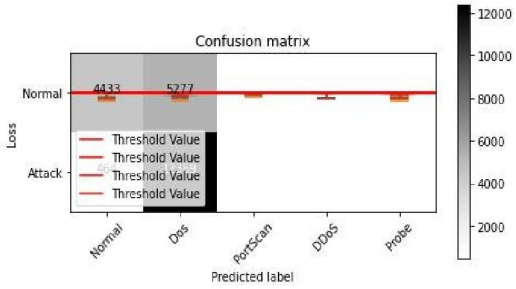

Figure2: Confusion matrix of Loss distribution.

To evaluate the data, Exploratory Data Analysis is performed to understand the different types of DOS attacks in the dataset and plot a bar chart. All the data given in the bar chart are compared with DOS Attack.

The bar chart(Figure 3) titled Saturation by types of DOS attack depict the number of records present in different types of DOS attacks where the neptune attack seem to be the heighest followed by smurf. Neptune has a record of 40000 and smurf is comparatively low around 5000.

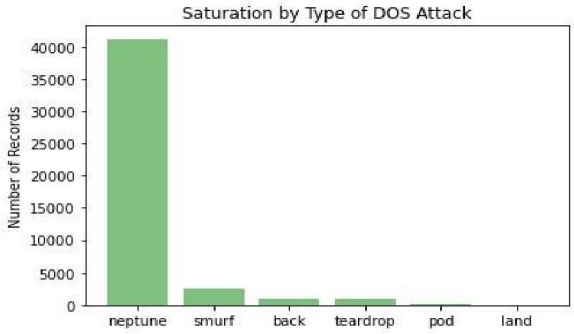

Figure 3: Types of Dos Attack

The bar chart (Figure 4) compares the records of non-attacks that is the unaffected data and the DOS attacks, the data which are attacked by DOS. After training and testing the model for the given dataset the results shows that the DOS attack seem to be low in numbers.

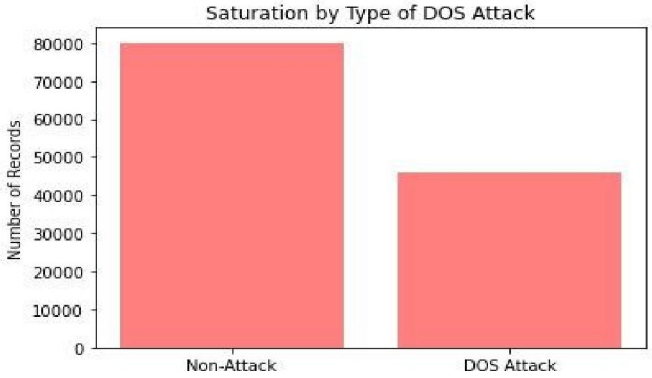

Figure 4: Non-Attack vs Dos Attack

The Saturation of DOS Attack bar chart (Figure 5) compares the total network interaction with DOS attack. This graph infer the amount of DOS Attacks intruded into the network flow and it is shown that the network interaction record falls to 40000 and the DOS attack encroach to 12000

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

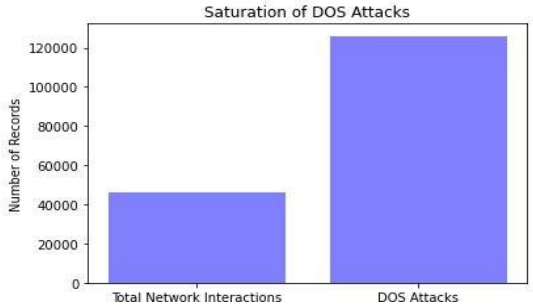

Figure 5: Comparison of Dos attacks to total network

VIII. CONCLUSION

To test the models, a significant experiment is run utilizing IoT botnet datasets. The experimental results illustrate that when compared with training from the original attributes or hidden representations developed by other autoencoders, training from latent representations is superior. These learning representation models significantly enhance the effectiveness of basic classifiers. The characteristics of the representation learning in comprehending unexpected assaults, executing the intersect-dataset test, and its resistance to diverse values are fully investigated. The research provides information on the practical applicability of the principles given.

REFERENCES

[1] Ly Vu, Van Loi Cao, Quang Uy Nguyen, Diep N. Nguyen, Dinh Thai Hoang, and Eryk Dutkiewicz, "Learning Latent Representation for IOT Anomaly Detection", IEEE Transactions on Cybernetics, Volume 52 Issue 5, 2022.
[2] Yan Naung Soe,Yaokai Feng,Paulus Insap Santosa,Rudy Hartanto and Kouichi Sakurai, "Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture", MDPI, Journal, Sensors, Volume 20 Issue 16, 2020.
[3] Imtiaz Ullah and Qusay H. Mahmoud,"Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks", Journals & Magazines, IEEE Access, Volume 9, 2021
[4] Zeeshan Ahmad, Adnan Shahid Khan 1, Kashif Nisar, Iram Haider, Rosilah Hassan, Muhammad Reazul Haque, Seleviawati Tarmizi and Joel J. P. C. Rodrigues, "Anomaly Detection Using Deep Neural Network for IoT Architecture", Journals Applied Sciences Volume 11 Issue 15, 2021
[5] Mahmoud Abdallah, Nhien An Le Khac, Hamed Jahromi, Anca Delia Jurcut, "A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs", Association of Computing Machinery, Digital Library, ARES 21, Proceedings of the 16th International Conference on Availability, Reliability and Security, Article, 2021.
[6] Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, Benjamin C.M. Fung, Saja Al Mamoori, "Deep learning-enabled anomaly detection for IoT systems", ScienceDirect, Internet of Things Volume 21, 2023.
[7] Zhiwei Gu, Shah Nazir, Cheng Hong, and Sulaiman Khan, "Convolution Neural Network-Based Higher Accurate Intrusion Identification System for the Network Security and Communication", Hindawi, Volume 2020, 2020.
[8] Charles Wheelus and Xingquan Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework", IoT, Journals, IoT, Volume 1, Issue 2, 2020.
[9]Diego Mendez Mena and Baijian Yang, "Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things", MDPI, Journals, IoT, Volume 2, Issue 1, 2020.
[9] Kumar Saurabh, Saksham Sood, P. Aditya Kumar, Uphar Singh, Ranjana Vyas, O.P. Vyas, Rahamatullah Khondoker, "LSTM-Based Deep Learning Model for Intrusion Detection Systems for IoT Networks", ADVANCED SEARCH Conferences, 2022 IEEE
World AI IoT Congress, 2022.
[10] Abebe Diro, Naveen Chilamkurti, Van-Doan Nguyen and Will Heyne, "A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms", MDPI, Journals, Sensors, Volume 21, Issue 24, 2021.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

[11] Lerina Aversano, Mario Luca Bernardi,Marta Cimitile, Riccardo Pecori and Luca Veltri, "Effective Anomaly Detection Using Deep Learning in IoT Systems", Hindawi, Volume 2021, 2021.

[12] Ramzi Snoussi, Habib Yousse, "VAE‐Based Latent Representations Learning for Botnet Detection in IoT Networks", Journal of Network and Systems Management, Article number: 4 (2023) , 2023

[14]Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, Ali
A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", Conferences, 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009