

# Using Deep Learning Technique in an IoT Environment to Prevent Intrusions into Internet Networks

Rita Bhawalkar<sup>1</sup>, Shalini kumari<sup>2</sup>, Saurabh Vyas<sup>3</sup>, Pravin kulurkar<sup>4</sup> and Vishakha Akhare<sup>5</sup>

<sup>1</sup>Yeshwantrao Chavan College of Engineering/Information Technology, Nagpur, India and  
Email: bhawalkarrita1991@gmail.com

<sup>2-5</sup>GHRIET/Cyber Security, Nagpur, India

Email: {shalini.kumari@ghrua.edu.in, saurabh.vyas@ghru.edu.in, pravin.kulurkar@raisoni.net, vishuakhre@gmail.com}

**Abstract**—Every day, the Internet of Things (IoT) becomes more widespread and smarter by enabling data sharing among devices. By connecting the physical and digital realms, IoT is rapidly bringing intelligence to the globe; by 2024, it is anticipated that over 20 billion items will be connected. IoT attempts to simplify our lives, yet its environment is full of security holes and potential threats. Numerous research works offer machine learning and deep learning-based intrusion detection systems for Internet of Things environments. The solutions offered differ in terms of efficiency and precision. This study proposes an RNN deep learning approach to offer an intrusion detection model in an Internet of Things context. The suggested model is trained and tested using the NSL-KDD dataset. The proposed solution has an 87% accuracy rate, which is satisfactory. We intend to apply optimization strategies in subsequent work to raise our model's detection accuracy.

**Keyword:** IoT, Deep learning, Intrusion detection systems, Recurrent Neural Network, NSL-KDD dataset, Security.

## I. INTRODUCTION

In the past several years, the Internet of Things (IoT) has gained popularity across a number of industries, including smart metering, healthcare, environmental monitoring, and monitoring. The Internet of Things has risen and with it, so have concerns about cybersecurity. AI is at the forefront of cybersecurity as complex algorithms are developed to safeguard networks and systems, especially Internet of Things (IoT) technologies. But concerns over privacy and security have slowed the advancement of this ground-breaking technology. The exponential rise in connected devices is creating new security holes and attack vectors. Even worse, a lot of IoT devices lack proper security features and/or are not made with security in mind.

Even basic IoT devices may become attack vectors if they are not properly safeguarded, as the great majority of IoT devices in use today have serious security flaws and vulnerabilities. It is essential to design defense systems with the ability to recognize attacks.

Security defensive methods such as intrusion detection systems (IDS) are essential for sensitive IoT setups. Because of resource and computing limitations, traditional security solutions cannot be directly used to safeguard Internet of Things devices. Deep learning algorithms account for the majority of machine learning algorithms utilized in the Internet of Things context. These algorithms automatically generate and analyze vast volumes of data, then interpret and predict the behavior of the system.

The application of deep learning to IoT security holds great promise for identifying any irregularities in the system's regular operation. As a result, our suggested technique for identifying intrusions on the Internet of Things will be precise and efficient. We presented the RNN deep learning method in our research paper as a means of detecting intrusions in the Internet of Things.

## II. WORK RELATED TO THE INTRUSION DETECTION SYSTEM

### *IOT Challenges*

If the Internet of Things (IoT) is to become a reality, security is paramount. The security of information security and services is a major concern for users. Therefore, in order to improve the security of the IoT environment, it is necessary to ensure the properties of the entire IoT system, such as confidentiality, integrity, authentication, authorization, availability and privacy.

#### *A. Confidential*

This ensures that data can only be accessed and modified by authorized parties. Authorization is granted not only to individuals, but also to objects in the Internet of Things environment.

#### *B. Integrity*

Based on truth, honesty and trustworthiness. In IoT technologies, password protection is insufficient, and reliable computing solutions must be built to ensure data and machine integrity. An adversary cannot change data during an operation without any system noticing.

#### *C. Authentication*

is the process of verifying the authenticity of a person or entity participating in a connection. A technology or model must be developed to safely handle device scalability in an IoT environment.

#### *D. Authorization*

Anyone with a valid ID can access data in the IoT ecosystem. Permission is granted relative to a device or user ID. No one can access information or services from this environment without permission. Therefore, an effective authorization method is essential in an IoT environment.

#### *E. Denial*

In the IoT context, a router cannot deny an alert or information to another network or client.

#### *F. Availability*

Recoverability and reliability are important aspects of IoT availability. Once connected to the Internet, anyone, any device, can generate data and try to save it anywhere. An appropriate methodology must be developed to ensure the availability of data and services in the context of the Internet of Things.

#### *G. Privacy*

can become a big concern with anything related to IoT. Researchers should create a comprehensive framework for IoT privacy and creative enforcement mechanisms. A large amount of prescribed material can be assembled without the person's knowledge. Therefore, users of the IoT system must process their own data.

## III. LITERATURE REVIEW

To show how important our research was, we discussed what has been done before and what has been done recently in the field. Many machine learning and deep learning algorithms have been used to protect IoT networks. From the literature Researchers presented an intrusion detection system based on a machine learning algorithm, logistic regression (LR), to classify network traffic as normal or malicious. Their system was evaluated on the NSLKDD dataset. Their proposed algorithm achieved 78% accuracy. In researchers presented an intrusion detection system that artificial neural networks. A proposed neural network (ANN) model can detect many attacks. An artificial neural network (ANN) consists of hidden input and output layers. The effectiveness of the proposal was evaluated using the database UNSW-15. The average accuracy of the model was 84%. And the model achieved high accuracy. Another type of deep learning algorithm, Deep Neural Networks (DNN), was used. They developed an intelligent intrusion detection system (IDS) that combines network virtualization with a Deep Neural Network (DNN) deep learning algorithm to detect strange behavior in insecure IoT networks. In order to find the optimal solution for a deep learning-based IDS, they tested their technology against five

different attack scenarios, including wormhole, opportunistic service, DDoS, sinkhole, and wormhole attacks. Examining the accuracy recovery curves under different attack scenarios, they were able to achieve an average accuracy of 95 percent. In this paper, they proposed an intrusion detection system based on a deep neural network, which uses a mixed activation function to improve the classification accuracy and reduce the error rate. The proposed model achieved high accuracy.

In, researchers developed a deep detection algorithm to detect a botnet attack in the Internet of Things environment. The model shows a high accuracy of identification. Researchers presented an intrusion detection model based on a deep learning model. They used UNSW-15 to evaluate the performance of the algorithms. The proposed model can classify IoT network traffic with good accuracy. Researchers have proposed an effective anomaly detection solution for IoT network using a deep neural network. It is used to classify network traffic as normal or abnormal. They use IoT-Botnet2020 to evaluate the model. The results show that the model successfully detects.

Deep Believe Networks (DBN) has achieved good results in detecting attacks on IoT networks. Other deep learning techniques are also used, such as feedforward neural networks (FNN). The researchers proposed a model that uses a feedforward neural network (FNN).

In the IoT context, they used the BoT-IoT dataset. Denial of Service, Distributed Denial of Service, Intelligence and Data Theft are four types of cyber attacks in the IoT environment. They provide a neural network based framework for intrusion detection. The proposed model has high precision all other measures, including recall and F1 score. In this paper, they propose a deep multilayer classification strategy for intrusion detection that combines the two steps of intrusion presence and intrusion detection and to improve the resampling method. Classifier performance. They used SLFN (Single-Hidden Layer Feedforward Neural Network). Has a good result. They evaluated their model using the IoTID20 dataset.

#### IV. METHODOLOGY

This section contains a detailed description of the proposed system to detect intrusion processes in IoT networks. Figure 1 explains the stages of our work.

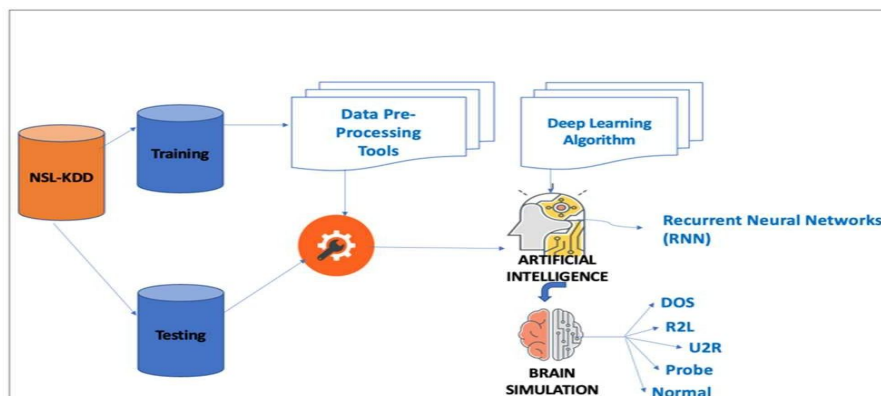


Fig.1 The proposed IDS Framework

##### A. Data set used

The DARPA98 IDS evaluation program provided the quantitative data that formed the KDD data set.

A new version of the KDD dataset has been created to fix several issues with the KDD cup dataset. The NSL-KDD dataset is proposed to correct and reduce duplicate entries in the KDD Cup dataset. This dataset contains a total of 125,973 training cases and 22,544 cases for testing.

Each instance of the NSL-KDD dataset has 41 features. Some of the features found in the NSL-KDD dataset are shown in Table 1.

TABLE I: LIST OF FEATURES OF NSL-KDD DATASET

| No | Features      | No | Features       |
|----|---------------|----|----------------|
| 1  | Duration      | 22 | is_guest_login |
| 2  | Protocol Type | 23 | Count          |
| 3  | Service       | 24 | srv_count      |
| 4  | Flag          | 25 | serror_rate    |

|    |                  |    |                        |
|----|------------------|----|------------------------|
| 5  | Src_Byte         | 26 | srv_error_rate         |
| 6  | dst_bytes        | 27 | error_rate             |
| 7  | Land             | 28 | srv_error_rate         |
| 8  | Wrong_Fragment   | 29 | same_srv_rate          |
| 9  | Urgent           | 30 | diff_srv_rate          |
| 10 | Hot              | 31 | srv_diff_host_rate     |
| 11 | Num_Failed_Login | 32 | dst_host_count         |
| 12 | Logged_In        | 33 | dst_host_srv_count     |
| 13 | Num_Compromised  | 34 | dst_host_same_srv_rate |

TABLE II: ATTACK TYPE

| Attack Type             | Attack                                                                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Denial of Service (Dos) | Back, Land, Neptune, Pod, Smurf, teardrop, Mailbomb, Processtable, Udpstorm, Apache2, Worm                                                    |
| Probe                   | Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint                                                                                                 |
| Remote to Local         | Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Xlock, Httpunnel, Sendmail, Named, WarezClient, SnmpGetAttack, Xsnoop, SnmpGuess |
| User to Root            | Buffer_overflow, Loadmodule, Httptuneel, Rootkit, Perl, Sqlattack, Xterm, Ps                                                                  |

The NSL-KDD dataset classifies data into common or specific forms of abuse. Denial of Service (DoS), Probing, Remote to Local (R2L) and User to Root (U2R) are the four main attack categories that consist of 39 different attack types. Table 2 shows the different attack types.

### B. Preprocessing Data

The data is preprocessed using the subsequent procedures :

- Transform all network and symbolic attributes.
- strings to represent a flag, protocols, services, and numerical properties.
- Seconds Normalization of all attributes using a Scaler basis.
- Reduce the number of attack types from 39 to four (DoS, U2R, R2L, and Probe), plus standard.

The experiment is carried out with TensorFlow and Keras. After the data has undergone preprocessing, the deep neural network is constructed. Ever since we developed the network attack detection method for multi-class classification based on autoencoders, the model consists of three layers of trained recurrent neural networks. This is also used to create a higher-level representation from the raw data.

### C. The Supposed Model of Classification

The input layer, the output layer, and the hidden layers are the three layers of recurrent neural networks. Figure 2 illustrates the one-way flow of information. where the direction is from the time masking unit that was used earlier to the one that is used now. The network's hidden units store data and retain information from beginning to end. We discover that RNN embodies deep learning when we investigate it.

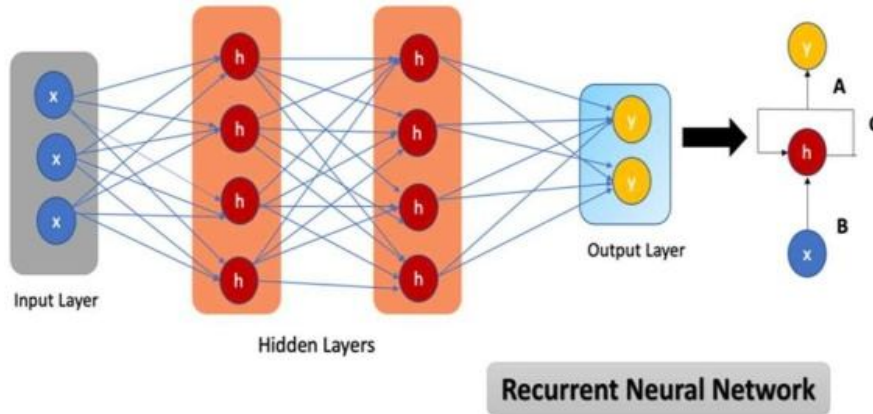


Fig. 2 Recurrent Neural Networks Architecture

## V. OUTCOMES AND COMMENTS

The results of applying the suggested method for intrusion detection in Internet of Things networks demonstrated how accurate the developed RNN model was. Tables and images below will provide a detailed display of the findings from the two training and testing phases.

TABLE III. MATRIX OF TRAINING STAGE

|                  |      |
|------------------|------|
| <b>Accuracy</b>  | 0.55 |
| <b>F1- score</b> | 0.55 |

TABLE IV. PRECISION, RECALL, F1-SCORE AND SUPPORT FOR TRAININGSTAGE

| <b>Attack</b> | <b>Precision</b> | <b>Recall</b> | <b>F1-Score</b> | <b>Support</b> |
|---------------|------------------|---------------|-----------------|----------------|
| <b>DOS</b>    | 0.55             | 0.46          | 0.49            | 45,927         |
| <b>PROBE</b>  | 0.63             | 0.62          | 0.62            | 11,656         |
| <b>R2L</b>    | 0.54             | 0.58          | 0.55            | 995            |
| <b>U2R</b>    | 0.52             | 0.58          | 0.55            | 52             |
| <b>NORMAL</b> | 0.55             | 0.64          | 0.58            | 67,343         |

TABLE V. MATRIC SCORE OF TESTING STAGE

|                  |      |
|------------------|------|
| <b>Accuracy</b>  | 0.87 |
| <b>F1- score</b> | 0.87 |

TABLE VI. PRECISION, RECALL, F1-SCORE AND SUPPORT FOR TESTING STAGE

| <b>Attack</b> | <b>Precision</b> | <b>Recall</b> | <b>F1-Score</b> | <b>Support</b> |
|---------------|------------------|---------------|-----------------|----------------|
| <b>DOS</b>    | 0.99             | 0.87          | 0.92            | 7460           |
| <b>PROBE</b>  | 0.91             | 0.96          | 0.93            | 2421           |
| <b>R2L</b>    | 0.69             | 0.94          | 0.79            | 2885           |
| <b>U2R</b>    | 1                | 0.97          | 0.98            | 67             |
| <b>NORMAL</b> | 0.87             | 0.88          | 0.86            | 9711           |

Our experience is shown in the table above. The suggested algorithm, RNN, demonstrated excellent performance in identifying the subsequent attack types: U2R and probe, with accuracy values of 100% and 0.99%, respectively. Still, it did a respectable job at identifying Dos, R2L, and Normal assaults. Overall, the findings show that the suggested technique is successful in detecting intrusions, which supports our observations about the significance and effectiveness of deep learning algorithms for network security. The accuracy and loss validation of the suggested (RNN) model are displayed in Figures 3 and 4.

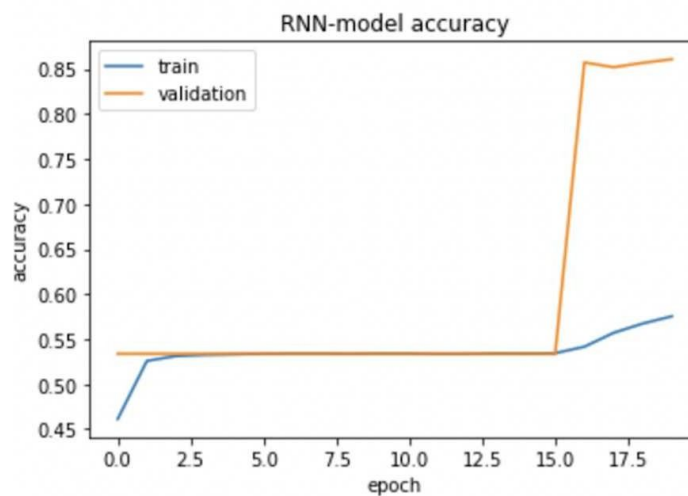


Fig.3 RNN Model Accuracy

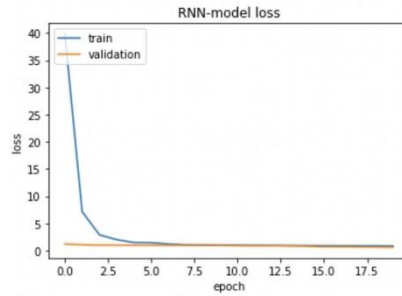


Fig.4 RNN Model Loss

We provided a comparison between the suggested algorithm and the machine learning algorithms examined in earlier works to show the effectiveness of our suggested work.

We can see from the above table that RNN, the suggested deep learning method, performs better than machine learning techniques.

TABLE III. COMPARISON RESULTS

| Classification Algorithm | Dataset Used | Accuracy      |
|--------------------------|--------------|---------------|
| LR [9]                   | NSL-KDD      | 0.78 %        |
| ANN [10]                 | UNSW-NB15    | 0.84 %        |
| PROPOSED RNN             | NSL-KDD      | <b>0.87 %</b> |

Up to 84% of the time, the ANN algorithm outperformed the LR method in terms of performance. It was demonstrated by our suggested study that the deep learning algorithm outperforms the machine learning algorithm in terms of accuracy and efficiency.

## VI. FUTURE WORK AND CONCLUDING REMARKS

Organizations are increasingly favoring IoT systems and the rise in assaults is a result of the interaction between law enforcement and ordinary citizens. Opposing IoT networks system based on machine learning algorithms is proposed for improving network security.

A system is suggested that utilizes a Recurrent Neural Network as the main learning algorithm. Artificial neural networks (ANNs). The suggested framework is composed of two phases:

The stage of data preprocessing, and the stage of classification.

This categorization decides if the data is accurate or not.

Whether they are in a normal state or under attack depends on the dataset utilized by NSL-KDD.

The system successfully detected attacks with an 87% accuracy rate.

Precision and showcased the capacity of deep learning to Enhance the security of IoT. In upcoming projects, We will evaluate different deep learning models. Additionally, our intention is to utilize optimization algorithms for enhancing the detection procedure.

## REFERENCES

- [1] Yahyaoui, A., Lakhdhari, H., Abdellatif, T., and Attia, R. (2021, January). Machine learning-based network intrusion detection for streaming data. IoT applications. In 2021, the 21st ACIS International Winter Conference on Software Design, Artificial Intelligence, Networks and Parallel/Distributed Computing (SNPD Winter) will be held (pages 51-56). IEEE.
- [2] Chiba, Z., Abghour, N., Moussaid, K. and Rida, M. (2019). An intelligent approach to create a deep neural network based IDS in a cloud environment using a combination of machine learning algorithms Computers and Security, 86, 291-317.
- [3] Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012). The Internet of Things: Vision, Applications and Research Challenges. Ad hoc Networks, 10(7), 1497-1516
- [4] Hossain, M. M., Fotouhi, M. and Hasan, R. (2015, June). Towards an Analysis of Internet Security Issues, Challenges and Open Issues. In 2015 IEEE World Congress on Services (pp. 21-28). IEEE.
- [5] Rajkumar, M.N., Chatrapathi, C. and Venkatesakumar, V. (2014). The Internet of Things: Visual Technical Issues for Applications and Information Security. IPASJ International Journal of Computer Science, 2(8), 20-27.

- [6] Abomhara, M. and Køien, G. M. (2014, May). Security and Privacy The Internet of Things: Current Status and Open Issues. In 2014, the International Conference on Privacy and Security for Mobile Systems (PRISMS) was held (p. 18). IEEE.
- [7] Kumar, J. S. kaj Patel, D. R. (2014). Exploring the Internet of Things: Security and Privacy Issues. International Journal of Computer Applications, 90(11).
- [8] Brech, B., Jamison, J., Shao, L. and Wightwick, G. (2013). Putting it all together. IBM Red Book.
- [9] Raghuvanshi, A., Singh, U. K., Sajja, G. S., Pallathadka, H., Asenso, E., Kamal, M., ... and Phasinam, K. (2022). Machine-assisted intrusion detection learning for risk mitigation in smart agriculture enabled by IoT. Journal of Food Quality, 2022.
- [10] Hanif, Sohaib, Tuba Ilyas, and Muhammad Zeeshan. "IoT Intrusion Detection Using Artificial Neural Networks on the UNSW-15 Dataset." IEEE 2019 16th International Conference on Smart Cities: Improving the Quality of Life Using ICT and the Internet of Things and Artificial Intelligence (HONET-ICT). IEEE, 2019.
- [11] Chiba, Z., Abghour, N., Moussaid, K. and Rida, M. (2019). An intelligent approach to create a deep neural network based IDS in a cloud environment using a combination of machine learning algorithms Computers and Security, 86, 291-317.
- [12] Roy, B. and Cheung, H. (2018, November). A deep learning method for intrusion detection in the Internet of Things using a bidirectional long-short-term memory recurrent neural network. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) (pp.1-6). IEEE.
- [13] Ramadan, R.A. and Yadav, K. (2020). A new hybrid intrusion detection system (IDS) to detect Internet of Things (IoT) network attacks. Annals of Emerging Technologies in Computing (AETiC), print ISSN,2516-0281.
- [14] Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., ... and Cui, L. (2020). Efficient Intrusion Detection of Industrial Internet of Things Network Based on MultiCNN Fusion. Dimensions, 154, 107450.
- [15] Keserwani, P. K., Govil, M. C., Pilli, E. S. and Govil, P. (2021). A smart anoia-based intrusion detection system for Internet of Things (IoT) network using the GWO-PSO-RF model. Journal of Reliable Intelligent Environments, 7(1), 3–21.
- [16] Thamilarasu, G. and Chawla, S. (2019). Towards deep learning-based intrusion detection in the Internet of Things. Sensors, 19(9), 1977.
- [17] Manimurugan, S., Al-Mutairi, S., Aborokbah, M.M., Chilamkurti, N., Ganesan, S. and Patan, R. (2020). Effective attack detection in an intelligent environment in the Internet of Medical Things using a deep belief neural network. IEEE Access, 8, 77396-77404.
- [18] Manimurugan, S., Al-Mutairi, S., Aborokbah, M.M., Chilamkurti, N., Ganesan, S. and Patan, R. (2020). Effective attack detection in an intelligent environment in the Internet of Medical Things using a deep belief neural network. IEEE Access, 8, 77396-77404.
- [19] Stiawan, D. (2021). Intrusion Detection and Deep Learning on the Internet Heterogeneous Network. International Journal of Artificial Intelligence (IJ-AI).
- [20] Shareena, J., Ramdas, A. and AP, H. (2021). An intrusion detection system for iot botnet attacks using deep learning. SN Computing, 2(3), 1-8.
- [21] Aleesa, A.M., Younis, M. O. H. A. M. M. E. D., Mohammed, A. A. ja Sahar, N. M. (2021). Deep detection system with improved UNSW-NB15 dataset based on deep learning techniques. Journal of Engineering Science and Technology, 16(1), 711-727.
- [22] Li, P. and Zhang, Y. (2019, June). A New Intrusion Detection Method Internet of Things. In 2019, the Chinese Control and Decision Conference (CCDC) was held (p. 4761-4765). IEEE.
- [23] Zhang, Y., Li, P. and Wang, X. (2019). IoT intrusion detection is based on advanced genetic algorithm and deep belief networks. IEEE Access, 7, 31711-31722.
- [24] Sahu, A.K., Sharma, S., Tanveer, M. and Raja, R. (2021). Internet of Things attack detection using a hybrid deep learning model. Computer Communications, 176, 146–154.
- [25] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., and Robles-Kelly, A. (2019, December). Intrusion detection in deep learning in IoT networks. In 2019 IEEE 24th Pacific Rim International Symposium on Trusted Computing (PRDC) (p. 256-25609). IEEE.
- [26] Ahmad, Z., Shahid Khan, A., Nisar, K., Haider, I., Hassan, R., Haque, M.R., ... ja Rodrigues, J. J. (2021). Anomaly detection using deep neural network for IoT architecture. Applied Sciences, 11(15), 7050.