Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7670219

CLASSIFICATION OF ATTACKS IN IoT NETWORK USING DENSE NEURAL NETWORK

Dr. Sumathy S
MCA.,M.Phil.,Ph.D.,SLET Assistant Professor and Head, Department of Computer Science, Sir Theagaraya College, Shift II, Chennai, Tamil Nadu, India
sumathymurugan@gmail.com

Ms.D.Radha
MCA.,M.E.,NET.,SET., Assistant Professor Department of Computer Science, Shri Krishnaswamy College for Women, Chennai, Tamil Nadu, India radha.aasc@gmail.com

Abstract:
With increasing applications in Internet of Things (IoT) increased the productivity of individuals and organisation, and further it simplified the daily activities of humans. These technologies are prone to attacks due to multiple attacks by the intruders in large-scale IT systems. Such attacks pose severe threats to the user in terms of their confidential data and privacy. Hence, a strong intrusion system is required to improve the detection ability in IoT networks. In this paper, we develop a classifier enabled with dense neural network (DenseNet) that classifies the input data from the given datasets. The steps of the classification contain a series of processing involving pre-processing and feature extraction, which boosts the process of classification. The simulation is conducted on IoT environment to test the efficacy of DenseNetsability to classify the threats. The simulation results show that the proposed method is efficient in improving the rate of classification than other existing deep learning architectures.
Keywords: Deep Neural Network, Threats, IoT Network, Intrusion Detection, Internet of Things

1. Introduction

The importance of security cannot be overstated in recent digital era. Using the internet of things (IoT), objects around us can be connected to make our daily lives more effective and, as a result, give more comfort and productivity in both our professional and personal lives [1] [2]. These links, however, also make private information public. Clearly, there is an unquestionable need for security. When it comes to the IoT, users will face new difficulties [3]-[5]. Because of the growing number of connected devices in our life and the increasing amount of data that is being collected every day, security is becoming more and more important [6].

Security has emerged as a hot study topic due to the increase in network attack that try to access confidential data without authorisation or to render computer systems unreliable or unusable. While most research has focused on standard TCP/IP networks, the IoT has unique security issues that must be addressed [7] [8].

MQTT protocol goal is to provide an easy-to-use internet of things communication protocol. Several security methods are indicated by the protocol itself. The intrusion detection system (IDS) detects and protects our IoT systems at the network level [9] [10]. To improve network security in power-constrained devices that employ the lightweight MQTT protocol, researchers are using deep learning techniques.

Various deep learning approaches [11] – [15] are being tested to see if they may help with intrusion detection systems. data containing frames labelled with different sorts of attacks and normal frames are submitted to the multiclass classification models. The resulting model can be used to identify and thereby prevent attacks or intrusions in the IoT system using the pertained model.

In this paper, we develop a classifier enabled with dense neural network (DenseNet) that classifies the input data from the given datasets. The steps of the classification contain a series of processing involving pre-processing and feature extraction, which boosts the process of classification.

2. Background

There may be dozens or even hundreds of sensors and actuators for regulating systems like the heating, ventilation, and air conditioning system (HVAC) in an IoT-connected home. Most of these devices fails to make a direct connection to the Internet because of the various communication protocols that each of them uses. IoT gateways are significant because they can aggregate and process sensor data before transmitting it to Internet servers for further processing. They are devices capable of doing this [16].

IoT gateways are vulnerable to both standard IP attacks and attacks on wireless sensor networks because they reside at the convergence of edge devices and the Internet. Both forms of attacks are taken into account. To keep things simple, the study look at some of the most popular and harmful computer and network attack tactics [17].

- Denial-of-Service Attacks: An attempt to overwhelm systems and prevent some or all valid requests from being fulfilled is the primary method used in a denial-of-service (DoS) attack. It is impossible to detect a distributed denial-of-service (DDoS) attack by blocking a single source when the incoming traffic overwhelming the target originates from several separate places [18] [19].
- Denial-of-Sleep attacks: As a result of the Internet of Things, low-rate wireless personal area networks are a common way for objects to communicate. Because of the restrictions on hardware costs, memory utilisation, and power consumption, a number of security vulnerabilities have emerged, including traffic eavesdropping, packet replay, and collision attacks, all of which are simple to carry out in real time. Depleting the energy available to operate the wireless sensor nodes is a straightforward attack method [20] [21].

No question, information security is a must in our day-to-day lives. But when it comes to IoT, which demands high usability, we confront a lot of implementation issues. It is no secret that security has always been a trade-off between insurance and usability. Because of the Internet of Things, this trade-off becomes a lot more interesting to contemplate. It is not uncommon for Internet of Things (IoT) devices to have extremely small memory capacities and CPU capabilities. A lot more resources are needed for high-security cryptographic methods than

small IoT devices have. As a result, until we discover the Holy Grail of compact energy sources, we must look for new, lightweight methods of securing our IoT devices, which are little but vital to our daily lives.

Encryption-heavy security approaches are not a good fit for these restricted gadgets since they cannot conduct complex encryption and decryption quickly enough for secure real-time transmission of data [22-25]. To compensate for these device limitations, IoT framework systems should deploy various layers of protection and defence. Detecting, identifying, and mitigating threats as they occur is an IoT security challenge that requires the use of security intelligence.

Multiclass categorization of frames utilising typical deep learning algorithms to associate frame features with frame type is one method the study employed in our research. Longer- term objectives could include anticipating evolving threats using artificial intelligence to predict adaptively updated security methods, which are then implemented based on the viability of earlier activities and actions that have already been taken.

Each level component has a distinct purpose. The intermediary node collects data from the sensors and appliances, and sends it to the base units. It is the intermediary node that aggregates all of the data it receives from the many leaf nodes. The MQTT protocol is used to transmit it to the server. Every intermediary node sends data to the server, which collects, processes, and analyses it.

In fact, MQTT is a transport layer protocol, whereas at the application layer, TCP is employed to improve communication dependability. Sensors operate at the data link layer, while IP resides at the network layer, and binary data was once sent from the physical layer to the network layer. However, as the study identifies, IoT architecture lacks a security component, thus we'll need strategies to safeguard the IoT network. To solve this issue, the IoT architecture's application layer contains a built-in deep learning algorithm.

Constrained devices do not fit well with security approaches that heavily depend on encryption because they lack the processing power to quickly perform complex encryption and decryption so that they may safely transmit information in real-time. To compensate for these device limitations, IoT framework systems should deploy various layers of protection and defence.

Multiclass categorization of frames utilising standard DenseNet to connect frame features with frame type is one way the study utilised in our research. A more long-term goal may be to anticipate evolving threats by using DenseNet to predict how security methods will change based on historical performance and actions

3. Proposed Method

Using DenseNet, we created a classifier that can sort input data from different datasets. Pre-processing and feature extraction are included in the classification processes, which speeds up the classification process.

3.1. Attack Models

Target objects created by assaults with their own profile can have their recommendations changed using the suggested system. The attack model can be identified based on assumptions about the attacker intent and understanding.

An average, random, and segment attack model are all to be used in the proposed research. There are three categories of rating for an attack profile: target, selected, and filler.

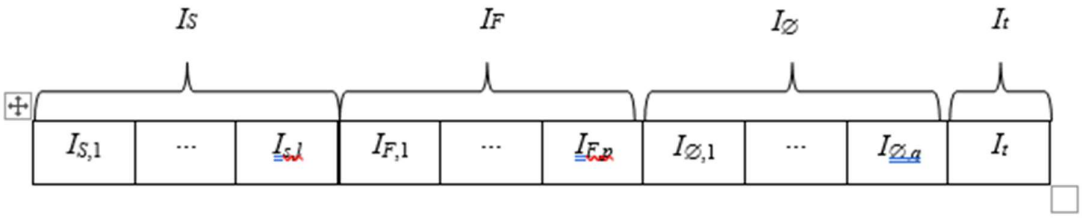

Fig. 1. Structure of attack profiles

Figure 1 depicts the attack profile's overall structure. Depending on the type of attack, one or more objects are selected and given a maximum or minimum rating value for each attack profile. The selected set is made up of a selection of things, each of which has a unique set of characteristics. Some assault models don't require IS, but IF is the collection of filler objects that is normally chosen at random. An attack profile's filler elements are components that make the profile appear authentic.

The quality of the filler items is determined by the recommender system's prior knowledge. Any attack that is launched becomes more complex as time goes on. When comparing attack models, the most significant distinction is between how the ratings of filler and selected items are derived. The variable rating distribution of filler items and the selected items varies among attack models.

3.2. Profile AttributeExtraction

Using the profile attributes, we can tell an attack from a legitimate profile in the dataset. Using an attack model, the profile attributes are split up into generic and specific to the attack model attributes. The generic qualities separate the attack from the true profile by using descriptive statistics to obtain the profile traits. The collaborative recommender system's rating matrix has a large dimensionality and sparsity, making it impossible to use the shilling attack model on it. With the use of supervised detection methods on an extracted attribute set (A), the extraction and dimensionality reduction of big datasets are simplified. In Eq.(1), you'll see a schematic diagram for obtaining the profile attributes. The extraction method in the proposed system incorporates the extraction of q attributes as an optional step.

(1)

Attack profiles and user profiles are mixed together to make up the training set. Users' profiles are generated using a dataset's rating matrix and an attack model. Depending on our findings, the user profile is classified as either a legitimate user or an attack profile. However, for the

sake of testing, all user profiles were taken as authentic. DenseNet is a binary classifier that can be generated based on the attributes of a training set.

3.3. Shilling Attack Detectionusing DenseNet

This section addresses the attack profile group characteristics and DenseNet's classifier. An adapted pruning model is used in the first phase of the two-phased method to handle the unbalanced class problem during the classification process of DenseNet. After achieving an unusual detection result in the first step, the fine tuning is carried out in the second phase, which examines the attack profile set's target people.

There are three sections to the full phase. The first step involves extracting attributes from the collaborative recommender system using a rating matrix to provide a score to each item. The rating matrix has a row for each item rated by users, and a column for each item rated by users in the recommender system.

In Collaborative Filtering, this assumes the user-item rating through n×m matrix with user vote (i) on an item (j), which is supplied by Dij, and plays a significant role. Users rate the matrix data to create a user profile, which has its own set of traits that can be used in the extraction process later on.

Adapted pruning models are used to build the proposed DenseNet classifier in the intermediate phase. When using a classifier, you'll get an inaccurate but still usable detection result. The coarse detection result is fine-tuned in the attack profile using GMM in the final step. During this stage, false positives are weeded out in favour of attack profiles. As you can see in Figure 1, the DenseNet Shilling Attack Detection procedure works as follows:

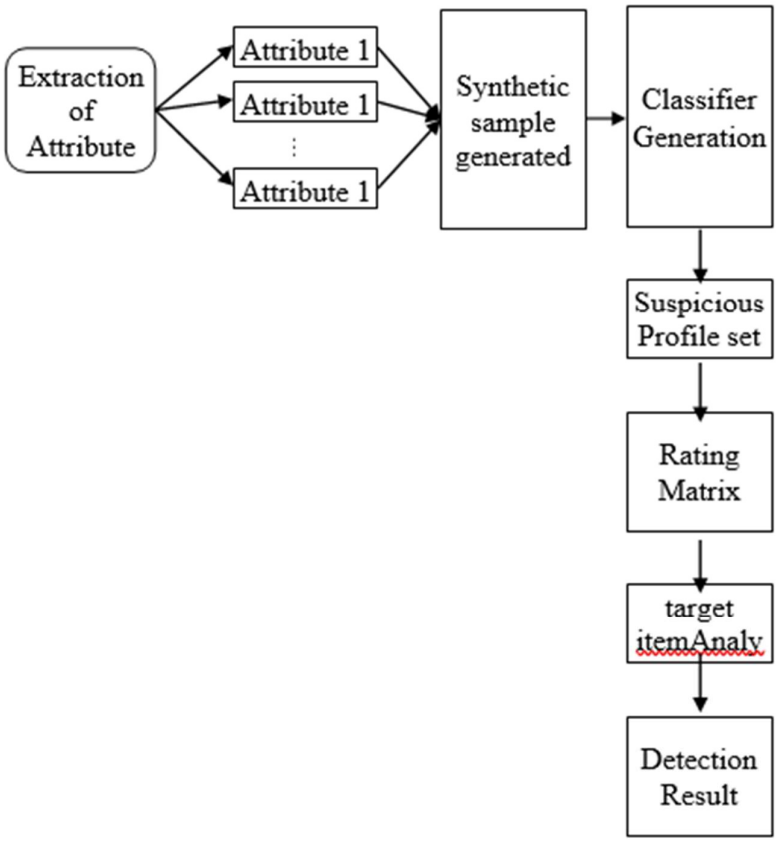

Figure 1: Detection Model

3.4. DenseNet

As soon as the feature identification operations are complete, Softmax converts the neural network's output into an estimate of the likelihood of an error occurring. The weight of the link is calculated and then updated after these processes have been completed.

The convolutional layer contains the features from the network logs. Quicker features are initially described as being made up of a large number of identically coloured squares. Each pooling layer is blurred before work on the following pooling layer begins once the pooling process is complete. Every 2x2 matrixon the pooling layer edge is used when numerical data for logs entries is compressed to 1x1 matrix. The resulting data is 2x2 matrixwhen processing 4x4 matrix. With two pooling layers, an image's pixels are multiplied by two.

DenseNet-169+ is a type of neural network that uses dense links between layers using dense blocks to achieve its results. To keep classifiers as natural as possible, the top layer passes on its feature maps to the lower layers.

The DenseNet was built using four dense blocks with identical layers on all datasets except ImageNet, which was not used by the developer. This 16-output channel convolution occurs on the image input before it enters the first block. Each input side is zero-padded with a single pixel to retain the functional map size with a 3x3 kernel. The transitional layers are composed of 1x1 convolutions and an average 2x2 pooling in between two blocks. There is a softmax

classifier added to the final dense block after the global average is applied. The feature map is 32x32, 16x16, and 8x8 in the three dense blocks, respectively.

On the basis of the actual value, the settings are tweaked. A vector with Nc dimensions represents the output, while the vectortp is provided by Eq.(2) where the Kronecker delta function is found.

$$t_p(i) = \delta(i - i_c) \qquad \text{where } 1 \le i \le N_c \tag{2}$$

where,

δ- Kronecker delta function.

The goal output is one if the class is right, and zero if the class is incorrect. As a result, the classification result is as follows:

$$y_p(i) = P(i \mid x_p) = \frac{P(i) f(x_p \mid i)}{\sum_{j=1}^{N_c} P(j) f(x_p \mid j)} \tag{3}$$

where the xp- conditional density and it is represented as a function f (xp|i) of i

$$f(x_p \mid i) = \sum_{k=1}^{K} a_{ki} \frac{\exp\left(-\sum_{n=1}^{N} \left(x_p(n) - m_{ki}(n)^2 v_{ki}(n)\right)\right)}{(2\pi)_{0.5N} \left(\prod_{n=1}^{N} \sigma_{ki}^2(n)\right)^{0.5}} \tag{4}$$

where

mki- mean vector,

ak- component of a weighting parameter.

4. Results and Discussions

The entire system is implemented using Matlab on windows 10operating system with an Intel core i7 processor operating at 16GB RAM.The Movie Lens 100k Dataset is used to test the effectiveness of the present study. This data set consists of 100,000 ratings from 1-5 given by 943 users on 682 movies and each user is allowed to rate only 20 movies. The proposed method is tested in terms of two parameters: filler size and attack size. The former is the ratio between total items rated and total items in the recommender system and the latter is the ratio between total attack profiles and total profiles in the recommender system. In the proposed system, the filler size for shilling attack profile is set in the range between 10% and 20%.

The results are compared in terms of various performance metrics like accuracy, precision, recall, f-measure and execution time. The proposed DenseNet is compared with existing ResNets, convolutional neural network (CNN), Recurrent Neural Network (RNN), Back Propagation Neural Network (BPNN) and three-layered neural network (3LNN).

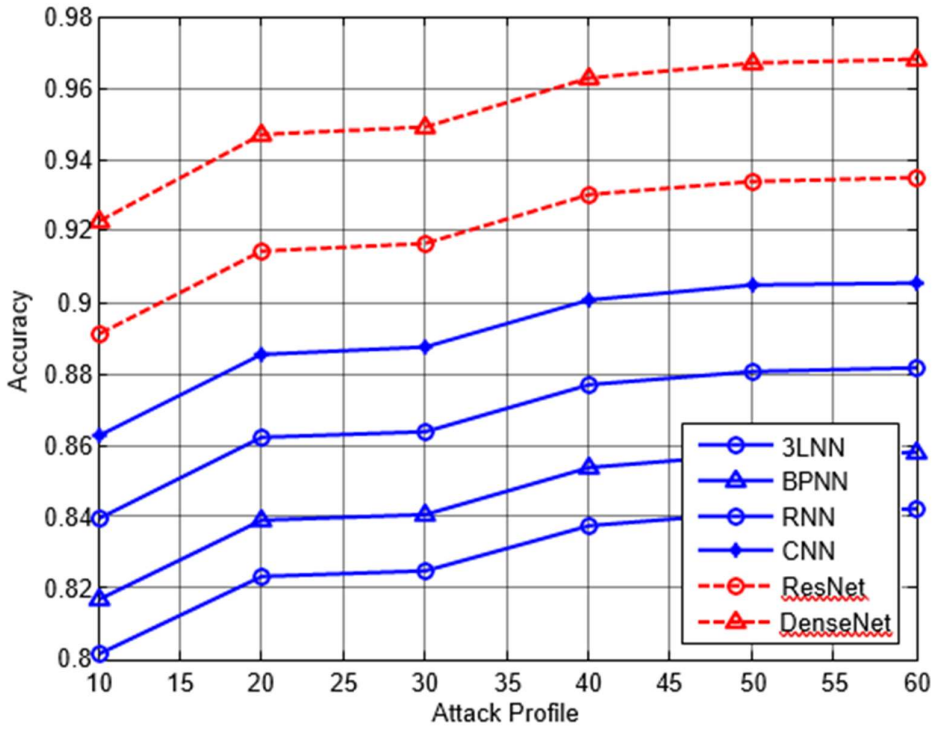

Figure 2: Accuracy

The Figure 2 shows the results of accuracy between proposed DenseNetand existing ResNets, CNN, RNN, BPNN and 3LNN. The results of simulation during testing show that the DenseNets obtains increased accuracy rate than other methods over various attack profiles.

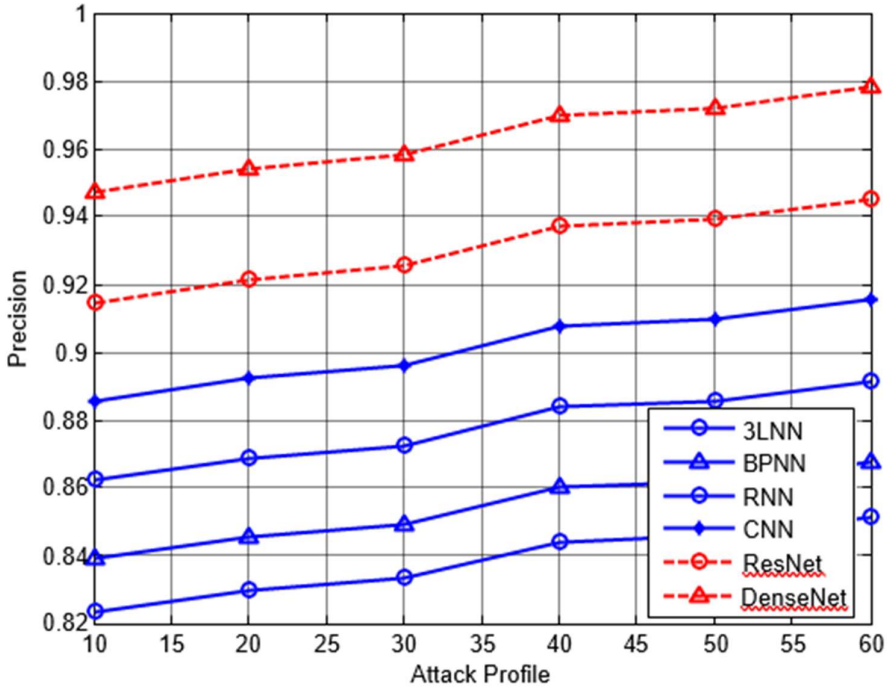

Figure 3: Precision

The Figure 3 shows the results of precision between proposed DenseNet and existing ResNets, CNN, RNN, BPNN and 3LNN. The results of simulation during testing show that the DenseNets obtains increased precision rate than other methods over various attack profiles.

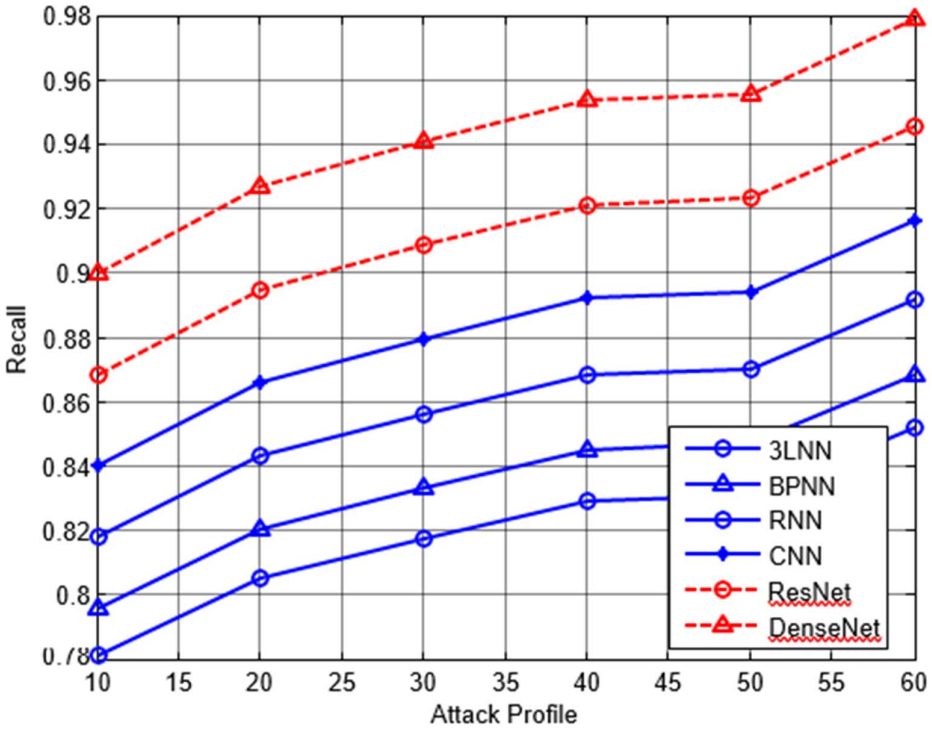

Figure 4: Recall

The Figure 4 shows the results of recall between proposed DenseNet and existing ResNets, CNN, RNN, BPNN and 3LNN. The results of simulation during testing show that the DenseNets obtains increased recall rate than other methods over various attack profiles.

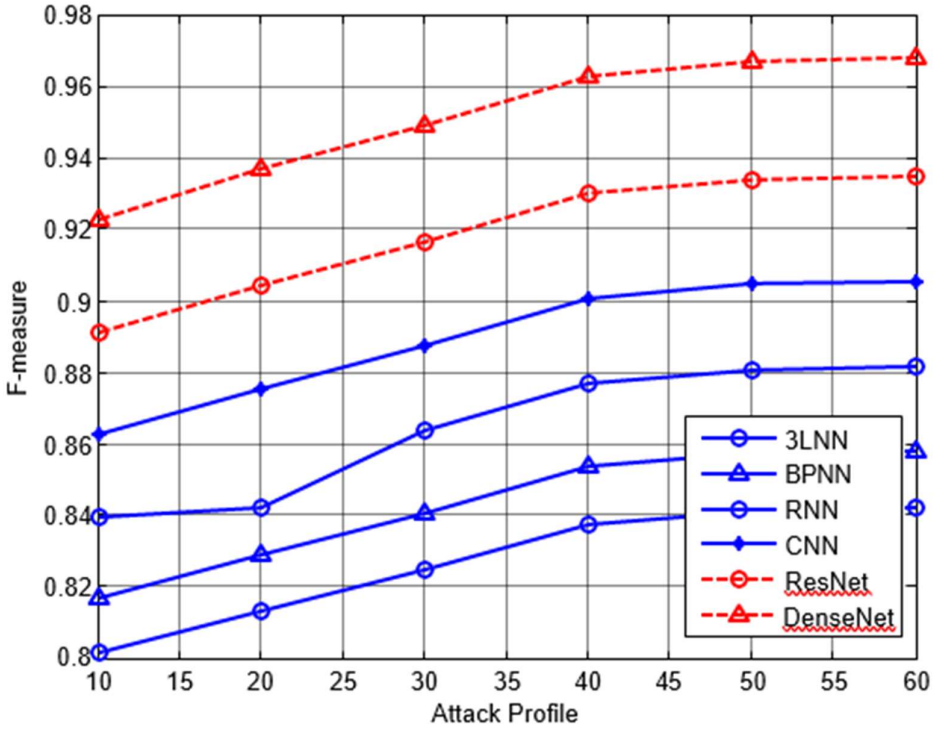

Figure 5: F-measure

The Figure 5 shows the results of f-measure rate between proposed DenseNet and existing ResNets, CNN, RNN, BPNN and 3LNN. The results of simulation during testing show that the DenseNets obtains increased f-measure rate than other methods over various attack profiles.

5. Conclusions

In this paper, we develop a classifier enabled with DenseNet that classifies the input data from the given datasets. The steps of the classification contain a series of processing involving pre-processing and feature extraction, which boosts the process of classification. The simulation is conducted on IoT environment to test the efficacy of DenseNet ability to classify the threats. The results show that the DenseNetis efficient in improving the classification than other deep learning architectures.

References

[1] Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2021). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Transactions on Emerging Telecommunications Technologies, 32(7), e4121.

[2] Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of Things (IoT). Journal of ISMAC, 2(04), 190-199.

[3] Naeem, H., Ullah, F., Naeem, M. R., Khalid, S., Vasan, D., Jabbar, S., & Saeed, S. (2020). Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. Ad Hoc Networks, 105, 102154.

[4] Ge, M., Syed, N. F., Fu, X., Baig, Z., & Robles-Kelly, A. (2021). Towards a deep learning-driven intrusion detection approach for Internet of Things. Computer Networks, 186, 107784.

[5] Rouzbahani, H. M., Bahrami, A. H., &Karimipour, H. (2021). A Snapshot Ensemble Deep Neural Network Model for Attack Detection in Industrial Internet of Things. In AI-Enabled Threat Detection and Security Analysis for Industrial IoT (pp. 181- 194). Springer, Cham.

[6] Popoola, S. I., Adebisi, B., Ande, R., Hammoudeh, M., Anoh, K., &Atayero, A. A. (2021). SMOTE-DRNN: A Deep Learning Algorithm for Botnet Detection in the Internet-of-Things Networks. Sensors, 21(9), 2985.

[7] Derhab, A., Aldweesh, A., Emam, A. Z., & Khan, F. A. (2020). Intrusion detection system for Internet of Things based on temporal convolution neural network and efficient feature engineering. Wireless Communications and Mobile Computing, 2020.

[8] Canbalaban, E., & Sen, S. (2020, October). A cross-layer intrusion detection system for RPL-based internet of things. In International Conference on Ad-Hoc Networks and Wireless (pp. 214-227). Springer, Cham.

[9] Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access, 8, 89337-89350.

[10] Ullah, I., Ullah, A., & Sajjad, M. (2021). Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks. IoT, 2(3), 428-448.

[11] Telikani, A., &Gandomi, A. H. (2019). Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things. Internet of Things, 100122.

[12] Koroniotis, N., Moustafa, N., &Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems, 110, 91-106.

[13] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., &Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE Access, 7, 124379-124389.

[14] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., &Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE Access, 7, 124379-124389.

[15] Moustafa, N., Turnbull, B., & Choo, K. K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), 4815-4830.

[16] Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., &Gacanin, H. (2020). Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks. IEEE Internet of Things Journal, 8(6), 4944-4956.

[17] Wu, D., Yan, J., Wang, H., & Wang, R. (2019, November). Multiattack intrusion detection algorithm for edge-assisted internet of things. In 2019 IEEE International Conference on industrial internet (ICII) (pp. 210-218). IEEE.

[18] Kotenko, I., Saenko, I., &Branitskiy, A. (2018). Framework for mobile Internet of Things security monitoring based on big data processing and machine learning. IEEE Access, 6, 72714-72723.

[19] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

[20] Luo, C., Tan, Z., Min, G., Gan, J., Shi, W., & Tian, Z. (2020). A novel web attack detection system for internet of things via ensemble classification. IEEE Transactions on Industrial Informatics, 17(8), 5810-5818.

[21] Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A Hybrid Deep Learning- Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors, 21(14), 4884.

[22] da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks, 151, 147-157.

[23] Parra, G. D. L. T., Rad, P., Choo, K. K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications, 163, 102662.

[24] Parra, G. D. L. T., Rad, P., Choo, K. K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications, 163, 102662.

[25] Dushimimana, A., Tao, T., Kindong, R., &Nishyirimbere, A. (2020). Bi-directional Recurrent Neural network for Intrusion Detection System (IDS) in the internet of things (IoT). Int J Adv Eng Res Sci, 7(3), 524-539.

[26] Sumathy S, Revathy M , Manikandan R(2021).Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine Learning.
Materials Today: Proceedings Published. http//doi.org/10.1016/j.matpr.2021.04.171