Intrusion Detection System to Detect Anomalies using Convolution Neural Network in IOT

Santhanakrishnan C
Department of Computing Technologies, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur 603203, India, santhanc@srmist.edu.in

Jagadeesan S
Department of Computing Technologies, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur 603203, India, jagadees@srmist.edu.in

Senthil Raja M
Department of Computing Technologies, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur 603203, India, snthl.rj@gmail.com

Aditya S
Department of Computing Technologies, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur 603203, India, as8678@srmist.edu.in

Ramya M
Department of Computing Technologies, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur 603203, India, rm0394@srmist.edu.in

Abstract

The Internet of Things (IoT) is a network for communication that is linked together by wired or wireless networks. It has progressed magnificently in today's world, whether in smart homes, where all electronics and gadgets, such as tube lights, are linked to the internet, or in the medical, educational, or government industries. As the use of the IoT is increasing rapidly, so are the security concerns. Security is the most crucial aspect to look after as the quantity of IoT devices spreads. Several attacks, such as replay, DoS, Distributed Denial of Service, and spoofing, will result in substantial data loss. To overcome these challenges, a very popular system, Intrusion Detection System (IDS) is being proposed. In this paper, deep learning Intrusion Detection System (DL-IDS) is used to check the accuracy, precision, and recall of the Convolutional Neural Network (CNN) algorithm to be detecting the attacks.

Keywords: *Convolutional Neural Network (CNN), Denial of Service (DOS), Distributed Denial of Service (DDOS), Deep Learning - Intrusion Detection System (DL-IDS).*

I. Introduction

The IoT is composed of various devices using sensors that are connected through the Internet. Every second, almost 127 devices get connected to the IoT as stated by McKinsey Digital. An attacker can invade the system and can have access to all the information of the victim. Security of IoT is the most important and crucial issue that is being faced in cloud computing. Frequent cases of cyber attacks and intrusions have been brought to the attention. According to a report, it was found that the infected devices in the IoT devices now comprise 33% which has been increased by almost 16% from 2019. Many security issues concern everyone like privacy, accessibility, information protection, and more. The above example and statistics show that it is not only the concern of an individual's security but also the national security.

There have been a plethora of researches and writings regarding IoT security issues. Deep learning intrusion detection is a current research hotspot. The traditional IDS uses sensors to gather information and provides it the investigation motor which identifies the type of information and any anomalies that might be included in that information. If the anomaly is recognized, it is being informed to the organization to secure the system. ML and DL algorithms identify system anomalies. In researches, it was found that ML algorithms though predict anomalies but the accuracy is not better than the DL algorithms. Deep Learning is Machine Learning based on ANNs and representational learning.

A Convolutional Neural Network (CNN) is a Deep Neural Network inference that can get a data set, provide significance (loads and inclinations) to different points in the image, and separate one from the other. To improve the accuracy of the features of the dataset that have been extracted, classifiers like Dropout and ADAM are used.

II. LITERATURE SURVEY

An intrusion detection system is till now one of the most important security protection techniques for computer systems and networks. Many researchers have shown interest in finding the more dependable algorithm to detect the anomalies in the network and it has been seen that the deep learning approach brings out better solution in terms of accuracy when compared to machine learning.

Various similar works done by the auxiliary authors are described here: -

[1] Yazan Otoum, Dandan Liuet al. deep learning-based intrusion detection system using SMO calculation and SDPN algorithm for ideal discovery acknowledgement. The outcomes came out to have an accuracy of practically 99%.

[2] Bambang Susilo et al. Sari in their work compared the deep learning model machine learning model and to detect anomalies and depicted that Random Forest and the CNN gave the best outcome as far as precision and the AUC for multiclass characterization. Multiplying the adjustment of clump size on the MLP could make the computation interaction 1.4–2.6 occasions quicker, though the CNN could make the estimation cycle 1.8–2.4 times quicker.

[3] Elike Hodo et al. suggested to use Artificial Neural Network (ANN) Intrusion Detection to perform vulnerability analysis on IoT networks The network was trained with feed-forward and backward algorithms. The ANN algorithm effectively detected DDoS/DoS attacks on IoT network traffic.. Additionally, it aids in strengthening the stability of the company by detecting the response party early in the attack and avoiding major organisational disruptions.

[4] Dehua Zheng et al. in their work suggested an enhanced linear discriminant analysis (LDA)-based extreme learning system (ELM) arrangement for interruption recognition estimation (specifically, ILECA), which allows for fast and accurate assault position.

[5] The aim of Guojie Liu et al. was to conduct various types of organization disruption order experiments; each dataset has normal (negative) and attack (positive) examples. Neural convolution (CNN) with three

boundaries: neighboring vision, boundary sharing, and pooling.

[6] Jiyeon Kim et al. in their paper proposed a convolutional neural network (CNN) model which gets grayscale or RGB pictures as its info. The CNN model is feasible to change two additional boundaries, for example, the quantity of convolutional layers and size of the kernel. The outcomes showed that the double arrangement for KDD, RGB pictures are more precise than grayscale pictures, yet GS-8 has higher exactness than RGB pictures

III. PROPOSED MODEL:

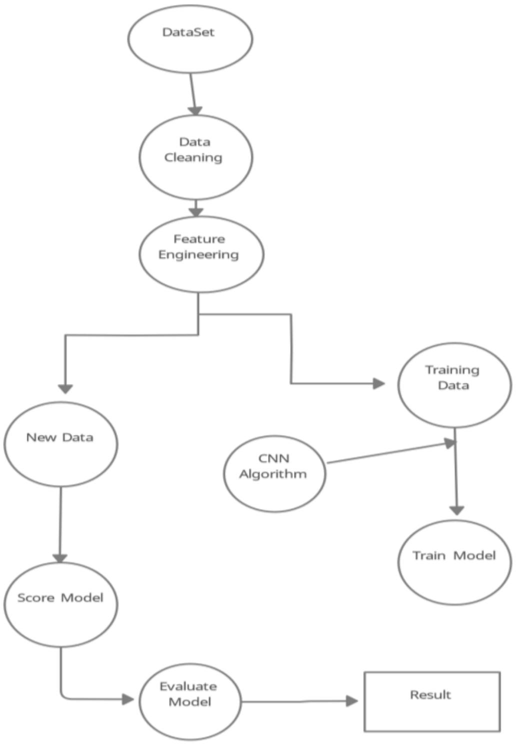
There are a few distinct sorts of intrusion detection systems. An intrusion detection system is a free framework which distinguishes interruptions by checking network traffic. Network detections systems monitor all network traffic by connection to a hub or switch. A convention based intrusion detection system is specialist that sits at the front end of a server that is utilized to screen and examine certain conventions between associated gadgets. These are typically utilized with web worker to screen the HTTPS convention. An application-based intrusion detection system is a system that monitors a certain application within a group of servers on a network. Figure 1 depicts the overall beneficial arrangement of the intrusion detection system using a convolutional neural network. The cycle comprises of three utilitarian modules comprising of data collection and preprocessing, self learning feature, classifier and result. In the information preprocessing module, the dataset is first cleaned then transformed and the appropriate data is selected, the model is then provided with the CNN algorithm to find and calculate the model accuracy. The model includes a bunch of change governs, each standard addresses a nuclear change the assailant can use to shroud the assault signature, and an excellent occasion of the assault from which any remaining occurrences utilizing any mix of the guidelines can be determine.

IV. SYSTEM ARCHITECTURE

Configuration is a multi-step that centers on information structure programming engineering, procedural subtleties, system and so forth… and interface among modules. The plan system additionally disentangle the prerequisites into show of programming that can be gotten to for greatness prior to coding starts. Computer software design change ceaselessly as novel techniques; improved examination and line understanding developed. Programming proposition is at moderately essential stage in its upheaval.

As a result, software design practise lacks the depth, resilience, and conceptual nature often associated with more traditional engineering disciplines. However, plan programming methods do exist, plan features models exist, and schedule documents can be used.

Fig. 1. System architecture overview



V. CONVOLUTIONAL NEURAL NETWORK

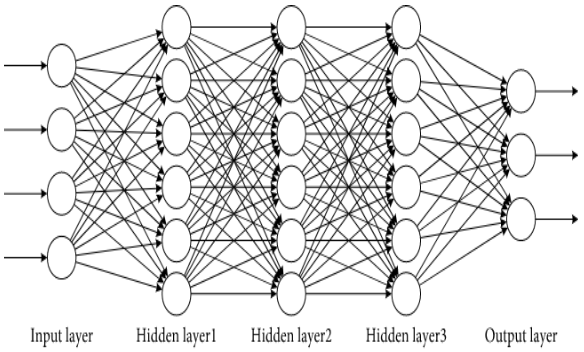
In numerous investigates it has been portrayed, contrasted with other AI calculations, CNN has given altogether better precision to intrusion detection systems. Being a semi-supervised neural network, it can address low-level interruption traffic information highlights as undeniable level highlights, as a result, they are gradually being used in the field of network intrusion prevention systems.

CNN refers to a kind of deep neural network like a counterfeit neural network that utilizes in any event one secret layer or convolutional layer to prepare the input layer. As demonstrated in figure 2. Convolutional neural network use convolutional tasks rather than framework increase activities. Every convolution portrays various attributes of the picture or network. The model trains itself by learning straightforward qualities of the picture including the space, recurrence and shading in every convolution.

In purely mathematical terms, convolution is a function derived from two given functions by integration which expresses how the shape of one is modified by the other as given in formula (1).

$$(f * g)(t) \overset{\mathrm{def}}{=} \int_{-\infty}^{\infty} f(\tau)\, g(t-\tau)\, d\tau \qquad (1)$$

Fig 2. Convolutional Neural Network



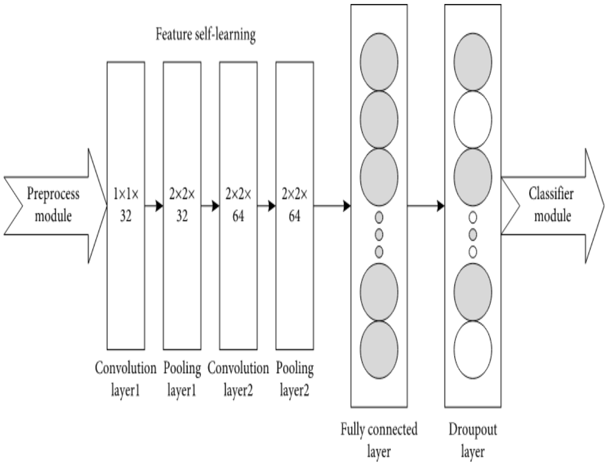
VI. DATA COLLECTION AND PREPROCESSING

Data collection is the most important task in building a deep learning model. It is the gathering of the information related to the task on some targeted variables to analyze and produce some valuable output. Some data in the dataset may be noisy and may contain inaccurate values, incomplete values, or incorrect values. Hence it is important to process the data before analyzing it and coming to the results. Data preprocessing can be done by data cleaning, data transformation, and data selection. Data cleaning is filling up missing values, filtering the noisy data, identifying or removing outliers, and resolving inconsistencies. Data transformation may include smoothing, aggregation, generalization and transformation which improve the quality of the data. Data selection includes some methods or functions which allow us to select the useful data for our system. In this paper sklearn preprocessing package is used to transform the data into appropriate features. The transformer API is used to compute the mean and standard deviation on the training dataset which will be used for testing purposes.

VII. FEATURES SELF LEARNING

The feature self-learning module is utilized to consequently learn and get the helpful highlights from the information contribution by utilizing convolutional neural network and to plan the learnt highlights to various convolutional layers and produce new highlights from the original dataset. The essential construction of the feature self-learning module is portrayed in figure 3. This module essentially incorporates convolutional operation, cooling operation, dropout, dense, activation functions and streamlining calculations like the Adam calculation.

Fig.3. Feature Self Learning



The core concepts of convolution neural networks are local perception, parameter sharing and cooling. Convolutional operations are used to handle the local perception. Cooling operation is used to reduce the dimensions of the features, in this paper reluis used as an activation function which is the highly preferred activation function to prevent overfitting dropout layer is inserted in the feature self-learning module. The Adam algorithm is a widely used optimization algorithm because it has advantages of both the adaptive radiant algorithm and root mean square propagation algorithm.

VIII. CLASSIFIER MODULE

It gives the end-product that the model has gained from self-learning module. The softmax classifier is utilized as the classifier module. The softmaxactivation function is represented by the equation theorem (2).

$$y_j = \frac{e^{\theta_j x^{(i)}}}{\sum_k \theta_k x^{(i)}}. \quad (2)$$

The weight factor is represented by j, and the data set is represented by x(i).

IX. RESULTS AND DISCUSSIONS

It comprises of various stages in which the principal stage preprocesses the data set then the information is given to self learning module comprising of convolutional layers to prepare the information. At that point the classifier module is utilized to assess the information being handled. Precision of the convolutional neural network model outcomes in 96.9%.

X. CONCLUSION

Intrusion Detection System is pivotal in the field of organization security. There has been a ton of examination in the field of the intrusion detection system. Numerous arrangements have been proposed.CNN is recommended as the most useful and reliable model, and the computation is streamlined. The investigation reveals that the proposed model increases accuracy and aids in the detection of anomalies. The precision of the model has opportunity to get better.

Fig.4. Protocol Type Feature

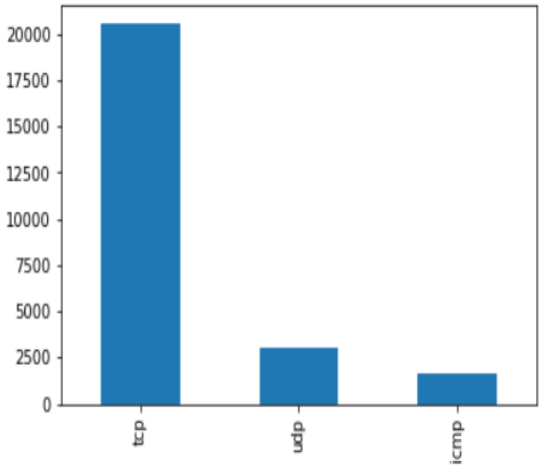


Fig.5. Service Feature

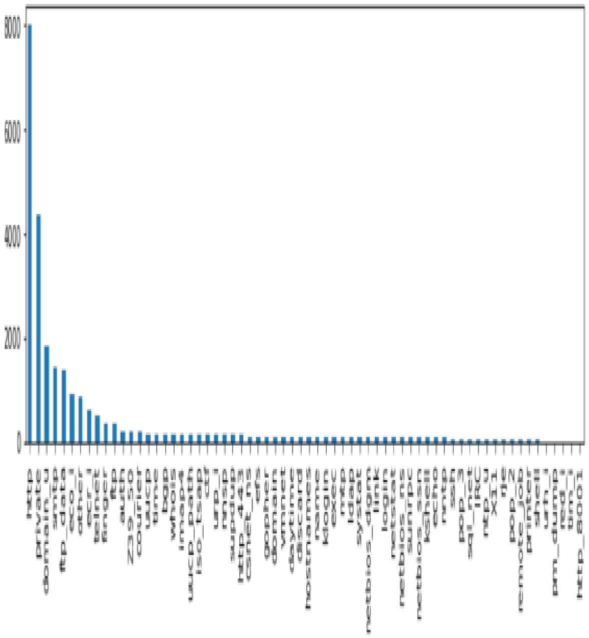
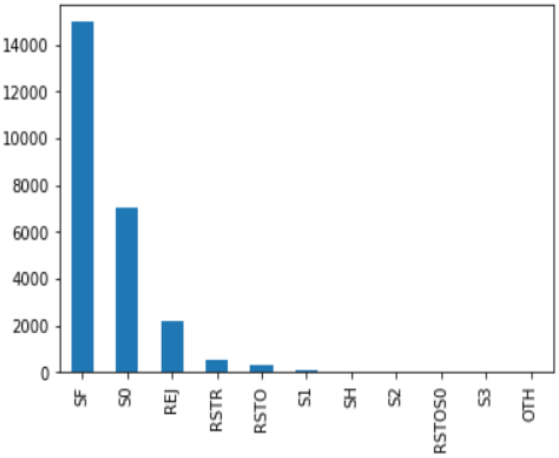


Fig.6. Flag Feature



References

[1] Yazan Otoum, Dandan Liu, Amiya Nayak. “DL-IDS: A deep learning-based intrusion detection framework for securing IoT, Transactions on Emerging Telecommunications Technologies”, November 2019

[2] Bambang Susilo and Riri Fitri Sari. “Intrusion Detection in IoT Networks Using Deep Learning Algorithm”, Information (ISSN 2078-2489; CODEN: INFOGG), May 2020

[3] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson. “Threat analysis of IoT networks Using Artificialz Neural Network Intrusion Detection System", 2016 International Symposium on Networks, Computers and Communications (ISNCC), Published by IEEE

[4] Dehua Zheng, Zhen Hong, Ning Wang , and Ping Chen. “An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application”, March 2020

[5] Guojie Liu and Jianbiao Zhang. “Research of Network Intrusion Detection Based on Convolutional Neural Network”, May 2020

[6] Jiyeon Kim, Jiwon Kim, Hyunjung Kim, Minsun Shim and Eunjung Choi. “CNN-Based Network Intrusion Detection against Denial-of-Service Attacks”, June 2020

[7] Weizhi Meng. “Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling”, Published by the IEEE Computer Society, July 2018

[8] Daming Lia, Lianbing Deng, Minchang Lee, Haoxiang Wang. “IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning”, May 2019

[9] Eirini Anthi, Lowri Williams, MałgorzataSłowinska, George Theodorakopoulos, Pete Burnap. “A Supervised Intrusion Detection System for Smart Home IoT Devices”, 2019 IEEE

[10] Sheikh Tahir Bakhsh , Saleh Alghamdi , Rayan A Alsemmeari and Syed Raheel Hassan. “An adaptive intrusion detection and prevention system for Internet of Things, International Journal of Distributed Sensor Networks” 2019

[11] Simone Facchini, Giacomo Giorgi, Andrea Saracino and Gianluca Dini. “Multi-level Distributed Intrusion Detection System for an IoT based Smart Home Environment”, January 2020

[12] Zeeshan Ali Khan and Peter Herrmann. “Recent Advancements in Intrusion Detection Systems for the Internet of Things”, January 2019

[13] Yulong Fu, Zheng Yan, Jin Cao, Ousmane Koné, and Xuefei Cao. “An Automata Based Intrusion Detection Method for Internet of Things”, January 2017

[14] M. Ponkarthika and V. R. Saraswathy, “Network intrusion detection using deep neural networks”, 2018

[15] C. Yin, Y. Zhu, J. Fei, and X. He. “A deep learning approach for intrusion detection using recurrent neural networks”, 2017

[16] H. Yang and F. Wang. “Network intrusion detection model based on improved convolutional neural network”, 2019