Design and Implementation of deep learning algorithms for anomaly based intrusion detection for internet of things (iot)

Vibhore wahi
2k18/IT/131(Information technology)
Delhi Technological University
Delhi, India
vibhorewahi_2ki18it131@dtu.ac.in

Sarthak Yadav
2k18/IT/111(Information Technology)
Delhi Technological University
Delhi, India
sarthakyadav_2k18it111@dtu.ac.in

Yash Thenuia
2k18/IT/136(Information Technology)
Delhi Technological University
Delhi, India
yashthenuia_2k18it136@dtu.ac.in

Anamika Chauhan
Information Technology
Delhi Technological University
Delhi, India
anamika@dce.ac.in

***Abstract*—"THE WAY WE COMMUNICATE, LEARN, AND WORK IS CHANGING AS A RESULT OF TECHNOLOGY".The world's dependency on the Internet is growing all the time.Data is the most valuable resource on the planet. Protect the information from prying eyes. When an organisation splits up, data is taken with it. To carry out such a future, we require high-security. As a result, IoT security has risen to the top of the priority list. In terms of privacy, authentication, and recovery from attacks.We have assembled a high level Network Intrusion Detection System (NIDS) in light of profound learning technique, we have used classical AI strategy such as (decision tree and random forest) and also deep-learing model like Artificial Neural Network and Convolutional neural network .we are utilizing the NSL-KDD data for training our model.**

***Index Terms*—IOT,Neural Network,Intrusion Detection System,Machine learning, Convolutional neural network.**

I. Introduction

Internet of Things is viewed as the 3rd present day Revolution. THE WAY WE COMMUNICATE, LEARN, AND WORK IS CHANGING AS A RESULT OF TECHNOLOGY . Our motivation should be clear after the evaluation focus on, demonstrating how we intend to be offered a good malware recognition response for IoTs. Such a drive will enable us to be prepared for vindictive focus points that are linked on a foundation, allowing them to connect securely in any environment that contains secure IoT gadgets. A large amount of data is generated on a regular basis, and private data is safely sent. a variety of associations Rely on network communication to send data, and any disruption in the organisation will hinder such communication.The Internet of Things (IoT) is a collection of closely related things, organisations, people, and instruments that will blend, share information, and data to achieve desired outcomes in better places and applications [22] It's a case of taking one modest step at a time to open new doors for industry trailblazers to create new products and associations that were previously unthinkable.

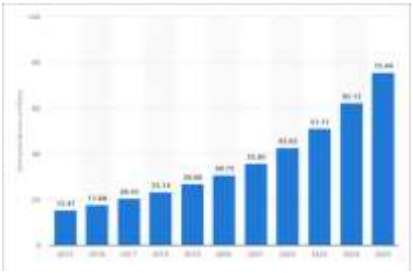

Fig. 1. Graph for yearly distribution of connected devices

As you can see in the figure 1,the number of gadgets using IoT is increasing year by year [11].

A. NETWORK SECURITY

In 2025, it is expected that the number of connected devices will exceed 70 billion. Such a networked environment can have a lot of advantages. To maintain the security of IoT environments, however, effective security management methodologies are required. Analysis of the connections between all different components (e.g., devices, infrastructures, etc.) at physical and cyber levels, as well as the potential vulnerabilities that arise from those connections, is a major security challenge for IoT , to minimise unauthorised access and reduce possible security threats

Security for IoT must be tackled in a proactive manner in response to such a challenge.Aggressors are taking use of dark weaknesses (vulnerabilities) and avoiding known markings in advanced attacks.A security-by-design approach demands the construction of new systems (or the analysis of existing systems) that conform to security-by-design principles, i.e.,

development and analysis based on security requirements engineering.

Really remarkable and realized specialist network game plans for this is IDS(intrusion detection system). There are two kinds of intrusion detection systems (IDS).

- Signature-based area that detects attacks based on known marks.
- second is an Anomaly-based area that recognises assaults based on unknown marks

It detects assaults that aren't based on standard usage patterns. When it comes to distinguishing dark assaults, eccentricity acknowledgment has an advantage over signature-based disclosure. This is difficult for signature-based ID, but the peculiarity area can detect dark attacks. For IDS improvement, we need to employ Machine Learning and deep learining model to produce inconsistency-based recognised proof.

B. MACHINE LEARNING

- Computer based intelligence is described as a data assessment procedure that processes reasonable model plan. decrease of IDS.item We want to routinely refresh our unmistakable base IDS to experience new danger

A portion of the NIDS dependent on the system of AI are as per the following:-

1) Decision Tree: A decision tree generates classification or regression models in the form of a tree structure. It gradually divides a dataset into smaller and smaller bits while also constructing a decision tree. The resulting output is a tree with decision and leaf nodes.

The ID3 method for creating decision trees, developed by J. R. Quinlan, employs a top-down, greedy search through the universe of possible branches with no backtracking. ID3 uses Entropy and Information Gain to build a decision tree.

2) Random Forest: For unlabeled instances, Random Forest Classification (RFC) use an ensemble of classification algorithms to determine the classlabel. When dealing with skewed datasets, this strategy has proven to be quite precise and effective. It pr

3) Deep Neural Network: An artificial neural network (ANN) having mutiple hidden layers between the input and output layers is known as a deep neural network (DNN). Neural networks, which exist in a variety of forms and sizes, are made up of neurons, synapses, weights, biases, and functions. These components function similarly to human brains and can be learned in the very same manner that any other machine learning algorithm can.

- Input layer - It is a layer that acknowledges the free factors as a contribution of the ML IDS model for additional expectations.
- Hidden layer-For expanding precision.
- Output layer - It creates the result of a model which is delivered by forecast models.

4) convolutional Neural Network: A convolutional neural network has three layers: input, hidden layers, and output. Because the activation function and final convolution cover

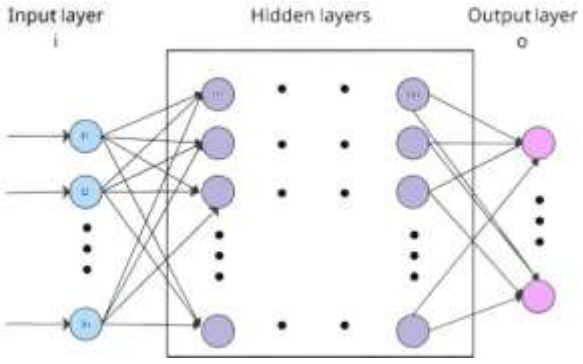

Fig. 2. ANN architecture

their inputs and outputs, middle layers of neural network are know as hidden. Convolutional layers and pooling layer are included in the hidden layers of a convolutional neural network. A layer that does a dot product of the convolution kernel and the layer's input matrix is commonly used. This product's activation function is commonly ReLU, and it's the Frobenius inner product.By sliding the convolution kernel along the layer's input matrix, which then feeds into the input of the next layer, the convolution approach builds a feature map. Different types of layer in CNN are:-

- Convolutional layer:- Initial layer of a Convolutional network.This layer focus on basic aspects such as colors and border.There can be many convolutional layers.
- Pooling layer:- it is the middle(hidden) layer of the network. there can be many pooling layers.
- Fully-connected (FC) layer:-It is last layer of thenetwork.

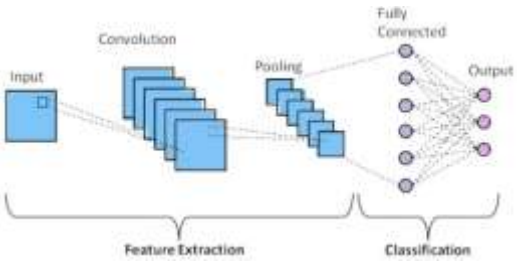

Fig. 3. CNN architecture

This paper's contributions are summarized as follows:

- analyzing and comparing 3 different models to predict air quality

- implementing ANN , CNN Decision Tree and Random Forest on NSL-KDD Dataset

The rest of this paper is structured as follows.Section II is devoted to a review of relevant works. The suggested architecture and estimating models are described in Section III. Section IV has the Results whereas the paper is concluded in Section V.

II. RELATED WORK

Internet of Things (IoT) is an infrastructure that incorporates many items such as sensors ,software and devices to interact with and share information via internet between differnt devices. As shown in fig 3.

For safeguarding PC organizations and PC frameworks, Network interruption location is one of the significant security guards.

one of the recent popular academic research topic is in the field of resolving intrusion detection problem and many paper have been proposed in this field. we have found that many paper have used conventional machine learning techniques to develop detection model [21].The studies [1]–[3] have used data mining methods to network events to classify network attacks.They have used various machine learning model such as naives bayes,decision trees and k-means on the NSL-KDD 99 Dataset.In all these all model naives bayes found to be have better accuracy and less time for training.Because of its simplest,elagance and effectiveness.

The IDS model was built using a variety of machine learning approaches. Traditional machine learning techniques that require well-crafted features engineering, on the other hand, require extensive research efforts to extract representative features from massive and unstructured data generated by IoT devices, due to the pace and volume of data generated by IoT devices. As a result, traditional machine learning-based solutions still face numerous hurdles.

However, adopting a technology like CNN and ANN proved to be more accurate. On the KDD-CUP 99 Datset, another study [4] employed the CNN approach. The suggested approach not only enhances intrusion traffic classification detection performance, but it also helps to reduce classification time, which is useful in real-time applications. Furthermore, CNN is regarded as a fairly broad approach, which may be related to ConvNets. Aside from these, numerous other studies have been conducted, as stated in Table 1.

III. PROPOSED MODEL

A. Dataset

we are utilizing the "NSL-KDD" dataset which is newest version of old "KDD Cup 99" dataset introduced in "The Third International Knowledge Discovery And Data Mining Tools Competition". we have downloaded data from kaggle.We are using NSL-KDD dataset beacuse it doesn't have duplicate data in training set which result in better performance of model. "NSL-KDD" Datasets have 42 columns, 41 of which are features which gives all the information of the traffic , and the attributes labelled 42 are known as "class" features, which tell us if a network packet is normal or attack. The dataset have two subset:-

- KDD-Train+ :- which is used for training our model.
- KDD-Test+ :- which is used for testing out model.

further we have classified our dataset into 4 categories shown in fig.4.

Attributes/Features Name			
Label B	Label C	Label T	Label H
1) Duration 2) Protocol_type 3) Service 4) src_bytes 5) dst_bytes 6) Flag 7) land 8) Wrong fragment 9) urgent	10) Hot 11) num_failed_logins 12) logged_in 13) num_compromised 14) root_shel 15) su_attempted 16) num_root 17) num_file_creation 18) num_shells 19) num_access_files 20) num_outbound_cmds 21) is_hot_login, 22) is_guest_login	23) count, 24) serror_rate 25) rerror_rate 26) same_srv_rate 27) diff_srv_rate 28) srv_count 29) srv_serror_rate 30) srv_rerror_rate 31) srv_diff_host_rate	32) dst_host_count 33) dst_host_srv_count 34) dst_host_same_srv_rate 35) dst_host_diff_srv_rate 36) dst_host_same_src_port_rate 37) dst_host_srv_diff_host_rate 38) dst_host_serror_rate 39) dst_host_srv_serror_rate 40) dst_host_rerror_rate 41) dst_host_srv_rerror_rate 42) Class

Fig. 4. classfication of "NSL-KDD" Dataset

B. Model Architecture

We can now go on to model construction with a completely preprocessed dataset. we have used both machine learning models and neural network models.After preprocessing of the data we have 122 features in our two sets and we have to predict what is the observation out of 11 target. we have combined little part of our testing data with our training data to make our model learn better. we have split our training set into training and validation data set so that we can use both resulting sets during model training to check that the model converges on the right optimum.

In our ANN model their our 5 layers, here the first layer has 256 nodes and after that we have decreased the number of nodes by half for every layer till the output layer which has 11 nodes. And our CNN model have 7 layers which inculdes convolutional layer with activation function "relu". Then we have maxpooling layer and flatten layer and then output layer. Basic architecture of both ANN and CNN are in fig. 3 and fig.4.

TABLE I
LITERATURE REVIEW OF EXISTING INTRUSION DETECTION SYSTEM

Reference	dataset	Algorthim	accuracy
[1]	NSL-KDD	The database used in the proposed model is NSL- KDD and used data preprocessing for improving classification. Algorithm: Naive Bayes.	88.2%
[2]	NSL-KDD	An intrusion Detection System(IDS) is built using Data Mining Algorithms. Algorithm used: K- means. [2]	81.61%
[3]	NSL-KDD	The model used in the given model is a Decision Tree split for NIDS.	79.52%
[4]	KDD-CUP 99	The CNN–IDS model is made up of three layers: an input layer, an output layer, and five hidden layers. To predict categorization, the output layer translates the outcome of feature extraction to a one-dimensional array.	92.2%

C. Data Preprocessing

1) Visualization: In both training and testing, each record has 42 elements, with 41 of the highlights related to the traffic input itself and one highlights is related to which type of attack has happen. We also observe that some things appear to belong to distinct "groups," which gives us some insight into how we might organise our data for model structure:

- Categorical Features: A few elements have specified qualities that identify anything in the component, such as protocol_type, which informs us that convention is in effect in the observation, or banner, which identifies what banner occurs throughout this record.And we have to use one-hot encode in this record.
- Numeric Count Features: Highlights such as duration, src-bytes, dst_bytes, and so on look to be individual integer counts of what they track. We don't know yet, but they might have a significant impact. we can see that if we take dst_bytes it's value might be anywhere between 0 and 8153 or past from the top of the component. We'll almost certainly need to standardise these highlights in some way.

Let's see if we can confirm or refute our fundamental assumptions by conducting some exploratory data analysis. There are only four article/straight out highlights in each of the two sets, all with somewhat sensible level measures. These aspects include duration, protocol type, administration, and markings, to name a few. The help has up to 70 distinct characteristics. This level of cardinality may be hazardous, but we shall decide whether or not to limit it based on the circumstances.

The two sets each include a unique number of highlights with massive reaches. These aspects are duration ,src_bytes,dst_host_count ,dst host srv count dst bytes, hot, num_compromised ,num root ,count ,srv count.

We quickly notice that our data has a significant skew, which is primarily perceptions of regular conduct and neptune assaults, which are attacks in which the assailant exploits flaws in the TCP convention's three-way-handshake and transmits a continuous stream of progressive faked SYN packets.

2) Preprocessing: Clearly, without the preprocessing the data , we won't be able to derive any good knowledge from perceptions or other techniques unless we remove the tilt from our data. So, in our preparation set, we'll downsample our normal and neptune perceptions to just 5000 perceptions, and in our testing set, we'll downsample to just 1000 perceptions, of both.

Despite this, we may see that some objective names have limited perceptions and that a few types of assaults are only noticed in the test set. We'll tackle two problems at once right now by maintaining the markings of attacks that have adequate perceptions and renaming any remaining assaults Other.

We'll keep the attacks normal, neptune, satan, ipsweep, portsweep, smurf, nmap, back, teardrop, and warezclient and rest of them as other.

We'll do a one-shot encoding of our object/categorical preparationhighlights for the time being. Despite the fact that we had the option of discretizing our objective element levels, we will accept our preparation highlights level crossing with greater scepticism. We'll combine our train and test sets first, then encode all of our object/categorical elements before separating the combined dataset into preparation and testing sets.

IV. RESULT

we have utilized relu(rectified linear activation function) as the activation function in both ANN and CNN model it gives less execution time and better precision. For the last layer we have used softmax activation function that predict a multinomial probability distribution. We have not used sigmoid funtion beacuse the regardless of the input it always gives value between 1 and 0.

Other then this we have use decision tree and random forest model to which also gives very good result.

For Performance Evaluation of all the model we have used confusion matrix and accuarcy which we have shown in the below table.

- Confusion matrix:- To evaluate performance, a n x n matrix is employed. Where n is the number of classes

in the categorization model. We use confusion matrix because rather than accuracy it is more specific about models performance. we have shown the confusion matrix of testing set of all the models in in Fig.6 , Fig.7, Fig.8,Fig.9..

- F1 score , it is mainly used to compare the performance of two classifiers.it combines recall and precision of the classifier into single metric by taking harmonic mean. More the f1-score the better the classifier is working.

$$f\,1score = 2 * (p * r / p * r)$$

where, p=precision and r=recall.

The f1-score of the all the model is shown in the below table when ANN and CNN model has been runed for 200 epoches.

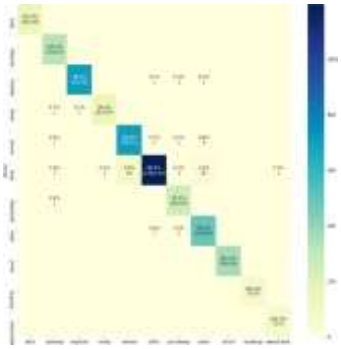

Fig. 5. confusion metrics random forest

Fig. 6. confusion metrics decision tree

Model	f1-score	accuarcy
decison tree	0.976	0.959
random forest	0.979	0.963
ANN	0.973	0.972
CNN	0.978	0.963

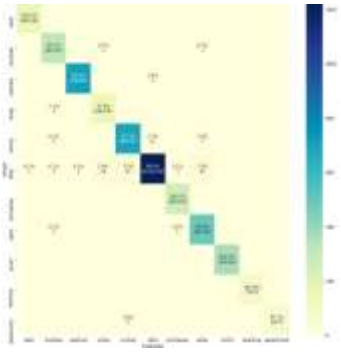

Fig. 7. confusion metrics ANN

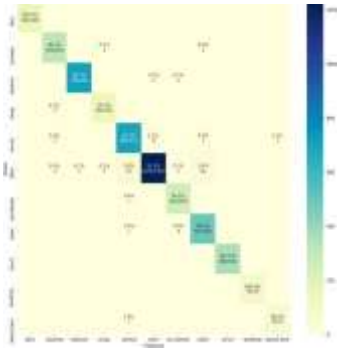

Fig. 8. confusion metrics CNN

V. Conclusion

As the IoT contraptions numbers are increasing rapidly, so does the attack and threats on them .So settling we have proposed a learning models using ANN , CNN , random forest and decision tree with f1-score of .973,.978,.979,.976 . All of the used model have given very good result in which random forest have given highest f1-score but accuracy of ANN model is high. AS IoT numbers is increasing day by day so does the their data so it is expected that their will be more improvement in the ANN models.And for the future work we can implement recurrent neural network like RNN and LSTM and we can also use some hybrid models like CNN and LSTM hybrid model . We are also trying to find bigger datasets so that we can apply neural networks more precisely and we can make intrusion detetction system better.

References

[1]D. H. Deshmukh, T. Ghorpade and P. Padiya, "Intrusion detection system by improved preprocessing methods and Na¨ıve Bayes classifier using NSL-KDD 99 Dataset," 2014 International Conference on Electronics and Communication Systems (ICECS), 2014, pp. 1-7, doi: 10.1109/ECS.2014.6892542.

[2]Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). ProcediaComput Sci 61:46–51.

[3]K. Rai, M. S. Devi, and A. Guleria, "Decision Tree Based Algorithm for Intrusion Detection," vol. 2834, pp. 2828–2834, 2016.

[4] Xiao, Yihan Xing, Cheng Zhang, Taining Zhao, Zhongkai. (2019). An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access. 7. 1-1. 10.1109/ACCESS.2019.2904620.

[5] Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A.; Lloret, J. Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT. Sensors 2017, 17, 1967, https://doi.org/10.3390/s17091967.

[6] Munir, M.; Siddiqui, S.A.; Dengel, A.; Ahmed, S. DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. IEEE Access 2018, 7, 1991–2005, https://doi.org/10.1109/access.2018.2886457.

[7]M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[8]C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 184–208, 2016, doi: 10.1109/COMST.2015.2402161.

[9] Xiao, Yihan Xing, Cheng Zhang, Taining Zhao, Zhongkai. (2019). An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access. 7. 1-1. 10.1109/ACCESS.2019.2904620.

[10] Karatas G, Demir O, Sahingoz OK. Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. IEEE Access. 2020;8:32150-32162.

[11] Dean, Andrew Opoku Agyeman, Michael. (2018). A Study of the Advances in IoT Security. 1-5. 10.1145/3284557.3284560.

[12] Awad, Mariette Khanna, Rahul. (2015). Support Vector Machines for Classification. 10.1007/978-1-4302-5990-9_3.

[13]A. M. N. Zaza, S. K. Kharroub and K. Abualsaud, "Lightweight IoT Malware Detection Solution Using CNN Classification," 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 212-217, doi: 10.1109/5GWF49715.2020.9221100.

[14]Ding, Yalei Zhai, Yuqing. (2018). Intrusion Detection System for NSL-KDD Dataset Using Convolutional Neural Networks. CSAI '18: Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence. 81-85. 10.1145/3297156.3297230.

[15]M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452-0457, doi: 10.1109/CCWC.2019.8666588

[16] Rawat, Shisrut Srinivasan, Aishwarya Ravi, Vinayakumar Ghosh, Uttam. (2020). Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. Internet Technology Letters. 10.1002/itl2.232.

[17] Aggarwal, P., Sharma, S. K. (2015). Analysis of KDD Dataset Attributes - Class wise for Intrusion Detection. Procedia Computer Science, 57, 842–851. doi:10.1016/j.procs.2015.07.490

[18]W. Lin, H. Lin, P. Wang, B. Wu and J. Tsai, "Using convolutional neural networks to network intrusion detection for cyber threats," 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1107-1110, doi: 10.1109/ICASI.2018.8394474.

[19]J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-Based Network Intrusion Detection against Denial-of-Service Attacks," Electronics, vol. 9, no. 6, p. 916, Jun. 2020.

[20] Kim, Jiyeon Shin, Yulim Choi, Eunjung. (2019). An Intrusion Detection Model based on a Convolutional Neural Network. Journal of Multimedia Information System. 6. 165- 172. 10.33851/JMIS.2019.6.4.165.

[21] da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learningbased intrusion detection approaches. Comput. Netw. 2019, 151, 147–157.

[22] Yousuf, Tasneem Mahmoud, Rwan Aloul, Fadi Zualkernan, Imran. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. International Journal for Information Security Research. 5. 608-616.

[23]A. Meena, D. Nigam, D. Sharma and A. Chauhan, "Anomaly Based Intrusion Detection For IoT: (A Deep Learning Approach)," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 1349-1356, doi: 10.1109/ICAC3N53548.2021.9725494.