iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45407

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

DeepMIA: An Integrated and Accelerated approach for Malicious Insider Attack Detection in IOT using Deep Learning

Punith R M[1], Priya D[2]
[1]*Student of Department of Information Science and Engineering, RV College Of Engineering,* Bangalore, India
[2]*Assistant Professor of Department of Information Science and Engineering, RV College Of Engineering,* Bangalore, India

Abstract: ***The Internet of Things (IoT) are poised to transform our lives and are becoming increasingly popular in smart homes, smart industrial networks. IoT devices can be used for a variety of purposes, including healthcare. Always, IoT device security is an issue because they are in charge of creating and handling large amounts of sensitive data. A security breach has been found to have an influence on people and eventually, the entire planet. Artificial intelligence (AI) has a greater range of applications and is currently being investigated for use in IoT device security. A malicious insider attack is the most serious security concern associated with IoT devices. Although much IoT security research has focused on ways to prevent unauthorized and unlawful access to systems and information, the most severe malicious insider attacks, which are often the result of internal attack within an IoT network or environment, have gone unnoticed. Here we have proposed a model called 'DeepMIA', which uses Deep Learning to detect dangerous insider attacks in the IoT context. This in resource-constrained IoT contexts, the research proposes a lightweight technique for detecting insider assaults that can detect abnormalities arising from sensors data or device data that are connected in a IoT Environment. The DeepMIA model is evaluated with UNSW-NB15 Dataset and achieves a decent accuracy of 99% with deep learning models.***

Keywords: Internet of Things (IoT), Malicious Insider Attack (MIA), Machine Learning, Deep Learning.

I. INTRODUCTION

We live in a time where everything and everyone is linked together by physical gadgets and items. Embedded devices and things communicate with one another which are internet-connected. IoT devices, on the other hand offer numerous benefits, including automatic data collection, monitoring, and control in a cost-effective and efficient manner. Although technologies must provide numerous satisfactions, they are also liable to malfunction. Attacks on privacy and security concerns are limiting the usage of IoT devices on a greater scale, particularly in crucial contexts where delicate information is exchanged and sensitive data is involved. To protect against security and privacy threats. The attention on safeguarding the data and devices is required, in order to block unwanted or illicit access, and blocking communication information from being shared with a third party. However, there is minimal consideration of the potential for insider assaults in an organization (inside the system) and the harm that they may inflict, whether purposefully or accidentally.

Fig 1: Internet of Things (IOT)

According to a survey issued by IBM Security Intelligence Index in 2018, attacks are launched out from the inside itself. The most common source of insider ultimatum is when a person or a device on the network abuses their legal access to compromise the confidentiality, integrity, or organization's systems availability. Over 25 billion IoT devices are anticipated to be online by 2025. With the advantages, devices of IoT in current world, using latest technologies art have fully changed to IoT enabled.

II. MOTIVATION

Devices of IoT have limited power and measurable resources, they can't even run anti-malware or detect intrusions. Protecting devices which are connected in IoT environment or network on such a massive scale necessitates a good model or system in IoT device security. Therefore, deep learning Techniques are used to establish a detection system of malicious insider attack in the IoT environment.

III. RELATED WORK

IoT device security is always an issue since they are in charge of producing and processing large volumes of sensitive data. A security breach has been found to make an impact on people and, eventually, the entire planet. AI technology does have a wide range of applications, and its usage in IoT device security is now being researched. A hostile insider attack is the most significant security concern linked with Internet of Things devices. Although much IoT security study has focused on methods to prevent unwanted and unlawful access to information and systems, the most severe malicious insider attacks, which are often internal exploitation's outcome within an IoT network, have gone unnoticed. A. Y. Khan et.al [1] employed artificial intelligence to detect risky insider threats in the context of the Internet of Things. This in resource-constrained IoT contexts, their research proposes a simple technique for detecting insider assaults that can detect anomalies originating from incoming data sensors.D. C. Le et.al [2] proposes and examines a machine learning based approach for detecting insider threats from users. Using machine learning, information is analyzed on many levels of graininess under realistic situations for identifying not just malicious behavior, but also malicious insiders. An in-depth examination of common insider threat scenarios with wildly disparate outcomes. Measures are offered to help with realistic system performance estimate. According to the findings, the discovery system based on machine learning can learn from constrained ground truth. and uncover new harmful business leaders in data that has never been seen before and is of exceptional quality accuracy. [2].

The current explosion of mobile devices and social media has opened up new avenues for gathering geo social data, which will aid police operations and combat insider assaults. Such social data, in particular, enables North American countries to understand the circumstances and behavior of consumers. N. Baracaldo et.al [3] proposed a Geo-Social business executive Access Resilient control threat management Framework in this research to detect insider threats by including current and historical geo social data into the access management call process. By observing user's geo social activity, identifying people whose access behaviour differs from the normal designs. Suspicious conduct can point to prospective business executive attackers who may execute hostile acts intentionally or unintentionally. G-SIR often utilize this information to determine a user's trustworthiness before allowing access.

On the other hand, Botnets cause a significant danger to network security since they are widely utilized in a variety of online crimes such as email spamming, identity theft, DDoS attacks and click fraud. N. Hoque et.al [4] provides a thorough overview of DDoS assaults, including their types and taxonomy with causes, as well as technical data on various attack launching tools. There includes a detailed description of numerous botnet architectures, as well as tools created to exploit botnet architectures and execs and cons analysed. Furthermore, an inventory of necessary problems and analysis challenges is additionally rumored within the paper [4].

Previously, mathematical methods were used to check the difference between the data in order to check for abnormalities. Owen. Lo et.al [6] builds a method of detecting threats that are made from insider by using the Hidden Markov method on a CERT data set (CERT r4.2) and analyzing a number of distance vector methods (Damerau–Levenshtein Distance, Cosine Distance, and Jaccard Distance) to detect changes in behaviour, which have been shown to be effective in detecting various insider threats [5]. But it is not suitable for current technology systems, task become very complex to find the assaults in large scale data.

The most common cyberattack in the IoT environment is the multi-stage botnet assault, which starts with scanning activities and culminates with a DDoS attack. The studies that are now available mostly concentrate on identifying botnet assaults once IoT devices become infiltrated and begin to launch DDoS attacks. Similar to this, the performance of the majority of machine learning-based botnet detection algorithms now in use is constrained by the dataset they are trained on. Faisal husain et.al [6] created a two-step machine learning approach to prevent and identify IoT botnet attacks. In first fold, they created the ResNetScan-1 model utilising the ResNet-18 current deep learning model for scanning assault detection. In the case that the scanning detection model is unable to stop a botnet attack, in the second fold they trained and created another ResNet-18 model (named ResNetDDoS-1) to recognise DDoS attacks. Since the proposed approach has a difficulty to obtain better performance, poor Application Performance and Narrowly specialized knowledge. This can't be used for IOT devices.[6].

IoT devices are susceptible to a variety of threats, which somewhat offsets their advantages. Y. Jia et.al [7] introduces two new machine learning models for DDoS detection and classification, as well as FlowGuard, a novel IoT DDoS defensive strategy. they began by designing FlowGuard, which consists of a Flow Filter and a Flow Handler part.

The Flow Filter is in charge of finding unidentified hostile flows based on traffic fluctuations and filtering harmful flows in accordance with the Flow Handler's filtration criteria. Using the LSTM and CNN machine learning models, Flow Handler is in charge of identifying and classifying dangerous flows. But the proposed work has prone to Errors, High complexity, inaccuracy and have not been investigated thoroughly [7].

Insider threat detection has sparked a lot of interest among researchers and businesses. Previous research has primarily focused on using machine learning approaches to detect insider threats. Yuan, F et.al [8] explains such complex task, however, necessitates feature engineering, which is a tough and tedious process. Deep learning, as we all know, can learn significant features on its own. they described a novel detection method for insider threat based on user behaviour using a Deep Neural Network (DNN) in this study. To discover users with unusual behaviour, they use the LSTM-CNN architecture. First, they employ the Long Short-Term Memory (LSTM), which is akin to natural language processing, to learn the language of user behaviour through user actions and extract abstracted temporal aspects/features. Second, the retrieved features are transformed to fixed-size feature matrices, which are then used by the Convolutional Neural Network (CNN) to detect insider threats. they run tests on a publicly available dataset of insider threats.[8].

The harmful insiders frequently imitate regular activity and exploits valid access rights to avoid detection, making it challenging to identify them using conventional defensive measures. Degang Sun et.al [9] proposes DeepMIT, a framework for detecting malicious insider threats that makes use of recurrent neural networks (RNN) to describe user actions as temporal sequences and forecast the likelihood of abnormalities. Since the detections are made in real time, or as quickly as the data is supplied, this architecture enables DeepMIT to continue learning. Additionally, our framework does additional analysis of the anomaly scores and offers the contributions to the scores, considerably assisting the operators in comprehending the results and swiftly moving forward. Additionally, DeepMIT makes use of user-attributes as categorical characteristics to determine the user's actual usual behaviour, which aids in the detection of malevolent insiders who imitate regular activities. DeepMIT has outperformed other current malicious insider threat solutions, according to extensive experimental assessments conducted on the CERT (version 6.2) public insider threat dataset.[9].

APT stands for Advanced Persistent threat, is one of the complex challenges for cyber defence. Due to the insiders' access to and presence within the network that these attacks exploit, many typical defences are rendered useless. Mohammad Mamn et.al [10], In order to build a baseline model based on a series of tasks using a LSTM neural network that can be used across multiple users to recognise anomalous behaviour, this study introduces DeepTaskAPT. DeepTaskAPT uses a process, that is tree-based task generating method to produce sequential log entries for the deep learning model rather than applying the model directly to sequential log entries as most existing methods do. Task trees store a sequential information about log activities that is near in meaning but distant in time. Due to the fact that APT also reflects this property, this makes DeepTaskAPT an effective model for detecting APT assaults. Therefore, constructing effective event representations for LSTM-based sequence classification requires task tree-based sequence construction. While DeepTaskAPT accurately and with a low FPR detects anomalous behaviour in the OpTC dataset, we show that the task tree generation approach can enhance the performance of other prediction methods.[10].

Ahmed Saaudi et.al [11] presents a novel approach of identifying harmful actions and suggested applying a granularity level to users' log data: examples of text-based session-based data. Character embeddings and a deep learning model made up of CNN and LSTM are used to model the user's actions. Using character embeddings, the input samples are represented. Then, local tri-gram features are extracted from the input samples using a convolution layer, and the order of these features is taken into account using an LSTM layer (tri-grams). Several versions of model architectures without handmade characteristics are used in their research. A portion of the CERT Insider Threat dataset, version 4.2, is used to evaluate the proposed model. The outcome demonstrates better performance with excellent accuracy and with high recall and precision values. [11]. But all the mentioned models are restricted to specific domains, in order to deal with IoT device data or network-connected device in IoT environment, we have proposed a DeepMIA model, which uses a latest deep learning techniques to detect the type of attack made.

IV. FEATURES OF THE DATASET

The Dataset which we have used, is taken from UNSW-NB15 (Intelligent security group UNSW Canberra, Australia) Dataset. It contains a labelled data with all its network related features. Most commonly, Features of dataset that are related to network connected devices will have a greater number of features compared to other devices data. Various attack types that are associated with the data based on behaviour of patterns are present in the dataset. Manually, it is very hard to describe the features of network related device data, instead in this work we have utilized python inbuilt libraries to extract the domain specific features to train the model.

Numerous of attacks exists that are being made on the IoT devices or network connected devices, among all those, Brute force (BF) and Brute force SSH (BF-SSH) are considered in the dataset taken. BF attack are made that tries to access a device by using a list of well-known or default credentials, whereas BF-SSH uses trial and error to guess credentials to access data or server. In next section more detailed information about the features that are used is explained.

V. DeepMIA MODEL

The system architecture of DeepMIA model is shown in figure 2, with the components: exploratory data analysis, Data pre-processing, feature engineering and Training the DeepMIA model. A detailed description of the stages involved in the suggested technique is provided in this section. The following is a system architecture representation. IoT devices data are pre-processed in general by conducting data cleaning, finding missing data, removing null values and data resampling. Following that, feature analysis is carried out representing the data which is most relevant

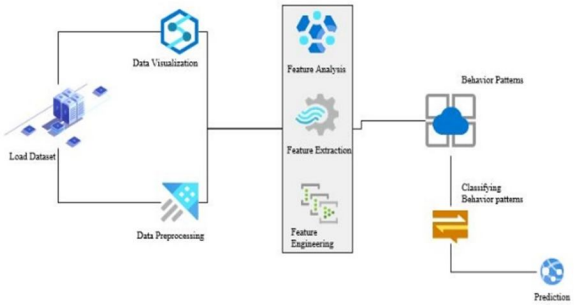


Fig 2: System architecture of DeepMIA

A. Exploratory Data Analysis

The initial phase in data analysis process is probing and visualizing the data. Here, we will figure out how to best utilize of the data we have, what type of data we want to train and how to extract them, as well as how to best modify the collected data to get the domain specific features. We achieve this by careful observation at unexpected outcomes, unknown patterns and outliers, also other aspects of our existing data in broad terms, utilizing visuals and quantitative methods to obtain a cleaned data. Data analysis is advantage to data science projects because it allows you to get clear insight that your future results will be more accurate, appropriately interpreted, and applicable to the business settings you desire. Such a degree of certainty can only be reached once raw data has been validated and checked for anomalies, ensuring that the data set was gathered without mistakes. Data analysis is used to define and tune the set of feature variables that will be used in concepts of machine learning. Here, by visualizing the data through different types of charts and plots, we get a more insights of data that how best it is suited to train the model, if the data contains any null value columns, infinity data and unstructured data, in that case we need to pre-process the data.

B. Data Pre-processing

It's possible that some data is missing in the dataset. When we hit an issue, we must be taken care of it. Obviously, you could delete the entire line of data, but what if you're erasing important information without knowing its importance Of course, we would never do such a thing. One of the most typical solutions is to take the average values which are present in the same column and use that to fill in the gaps. Scikit-Learn is the name of the python library we'll utilize for this process. Pre-processing is something you should learn. It has a class in it named Imputer, which will help us to fill the empty data and to remove the Null value columns. Our data is sometimes in qualitative form. In the text form, we can find categories. Because the models are built on calculations and mathematical equations, it is now more difficult for machines to interpret and process texts rather than numerical. As a result, we should cipher categorical data. Next to this, we need to train our deep learning model equally with all types of attack specific behaviours, resampling is one such process we do here to convert the imbalanced dataset to balanced dataset, we call this process as data **'resampling'**. Figure 3 and 4 represents imbalanced dataset and balanced dataset.

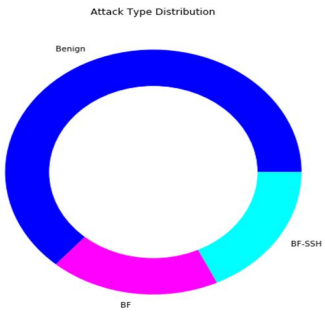


Fig 3: Imbalanced Dataset

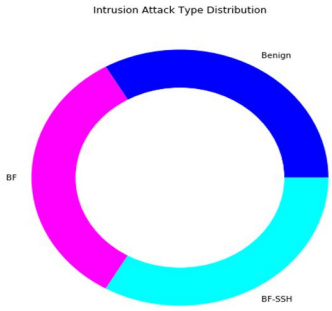


Fig 4: balanced Dataset

Upon getting a balanced dataset, now we can divide our dataset into a test set and a training set. We can use training set data to train our deep learning models, in which they will try to learn characteristics and behaviours of the data, and models will then be put to the test on data set to determine how well they can give outcome. As a general rule, allocate 80 percent of the dataset to the training set and the remaining 20% to the test set. We'll use the model_selection library of scikit by importing test_train_split method for this purpose.

C. Feature Engineering

Filter methods are commonly employed as a stage in the pre-processing process. Machin learning algorithms will not have any impact on feature selection. Rather, the selection of features is based on relationship to the result variable, as determined by various statistical tests or feature extraction methods. Using domain comprehension, Feature engineering is the activity of extracting features from raw data. The purpose is to use these extra attributes to increase the calibre of outcomes produced by a machine learning process as opposed to only providing raw data to the process. The process of translating information into numerical options which will be processed whereas keeping the knowledge within the original dataset is thought as feature extraction. Compared to directly using machine learning on raw data, it yields superior results. Since, we are dealing with data that are related to IoT environment or network connected devices, it is very hard to extract the domain specific features manually, instead we use python inbuilt method **'selectKbest'.** Features having k highest score will be select from the dataset, internally selectKbest method makes this complex task easier and helps in achieving the good accuracy

.

D. Training the DeepMIA model

In order to successfully identify Malicious insider attack in a IoT Environment, we explored the various deep learning techniques to produce a trustworthy outcome. Based upon all the study made, Feed forward neural network (FFNN), Long short-term memory (LSTM) and convolutional neural network (CNN) are the preferred one over the all algorithms available in deep learning in order to achieve a notable accuracy. Deep learning models can be used for both classification and regression type of problems, since here we are dealing with multi-class classification FFNN, LSTM and CNN are suitable. Initially, DeepMIA model is trained with FFNN and evaluated, inputs variables are passed and activation function make it capable to learn and perform a computational task. ReLU activation function is used as hidden layers of neural network and desired output variables are obtained.

Secondly, model is trained with LSTM, which works on recurrent neural network (RNN) architecture, more number of hidden layers are added in LSTM model to make computational task more complex and to get the better results. ReLU is a non-linear activation function gained its popularity in deep learning by giving a good result, LSTM also uses ReLU activation function as hidden layers of neural network. Lastly, the powerful deep learning model i.e... CNN, which tends to give a more accurate results among all other deep learning models is used to train the DeepMIA model. Since, this work related to the data which is in the row and column format, 1D Convolutional neural network is used.

VI. RESULTS AND COMPARATIVE ANALYSIS

The experimental results for the Malicious Insider attack detection and classification using deep learning were evaluated for their accuracy of training and validation and also tested with data that is not used during training for accurate classification of the insider attack made. The validation accuracy and training accuracy with their loss are plotted in the following graphs. Further the model was tested with testing data for the validation of the model and also the usefulness of the model. The results obtained are detailed in the next section. The detailed analysis of the results obtained from different Deep Learning models are depicted in the following graphs. The dataset was divided into training set and test set. 60000 rows, 6000 rows are used to train, test and validate the models respectively. The next section shows the performance analysis of different models.

1) *Feed-Forward Neural Network:* The Feed-forward neural network (validation vs training), the custom artificial neural network yielded a training accuracy of the 83.53% vs validation accuracy of 83.57% with the loss of 0.374 loss for training and 0.4256 loss for validation for 30 epochs at initial stage. training accuracy and validation accuracy with their loss of feed-forward neural network is plotted in figure 5 and 6 respectively.

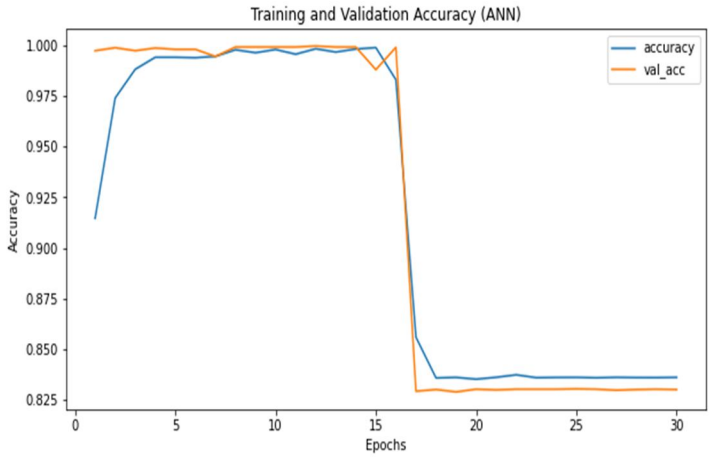


Fig 5: Training accuracy of FFNN vs Validation accuracy of FFNN plot

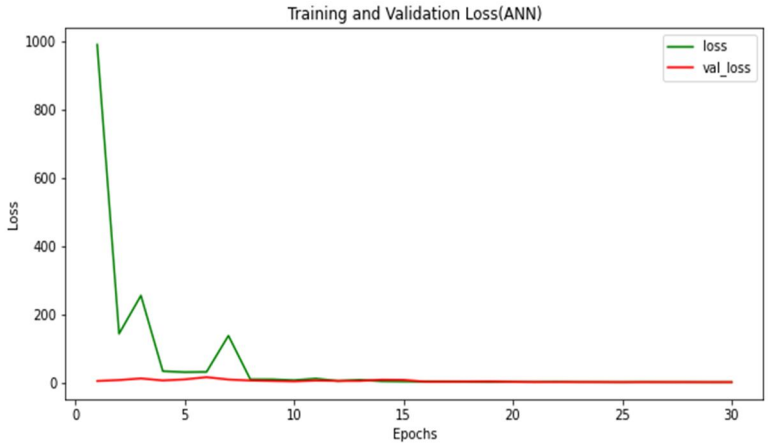


Fig 6: Training loss of FFNN vs Validation loss of FFNN plot

2) *Long short-term Memory (RNN):* The Long short term memory accuracy (validation vs training), the custom neural network yielded a training accuracy of the 76.63% vs validation accuracy of 73.56% with the loss of 0.235 loss for training and 0.264 loss for validation for 30 epochs at initial stage. training accuracy and validation accuracy with their loss of LSTM is plotted in figure 7 and 8 respectively.

Fig 7: Training accuracy of LSTM vs Validation accuracy of LSTM plot

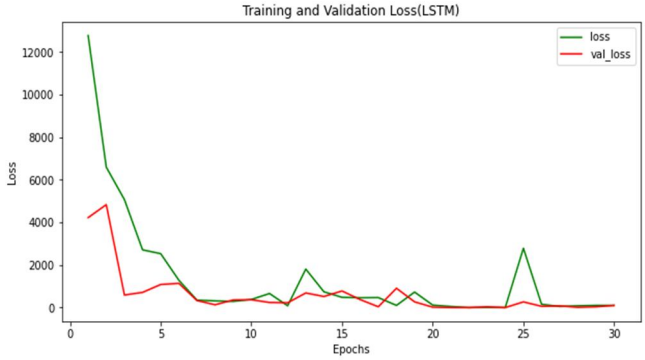


Fig 8: Training loss of LSTM vs Validation loss of LSTM plot

LSTM is implemented next to the feed-forward neural network, LSTM works on the recurrent neural network architecture. Recurrent Neural Network is also called as Long short-term memory. Accuracy of the LSTM is relatively low when compared with the Feed forward neural network. Since time sequence prediction and classification are more suitable with RNN, as we can observe training the LSTM model, more fluctuation can be seen in the accuracy and loss.

3) *1D Convolutional neural network (CNN):* Next model that is implemented is CNN, The Convolutional neural network accuracy (validation vs training) yielded a training accuracy of the 98.2% vs validation accuracy of 98.4% with the loss of 0.18 loss for training and 0.16 loss for validation for 30 epochs at initial stage. training accuracy and validation accuracy with their loss of CNN is plotted in figure 9 and 10 respectively.

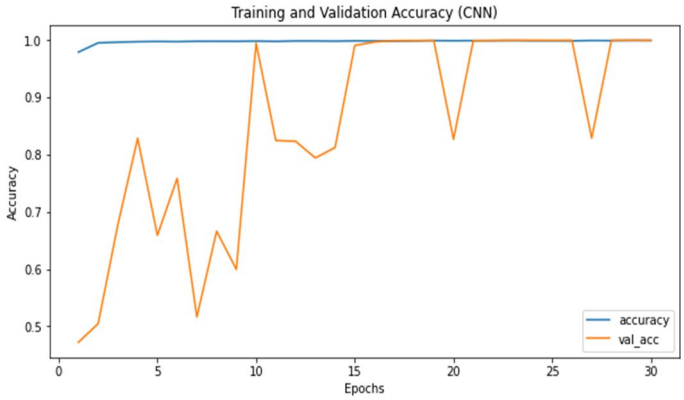


Fig 9: Training accuracy of CNN vs Validation accuracy of CNN plot

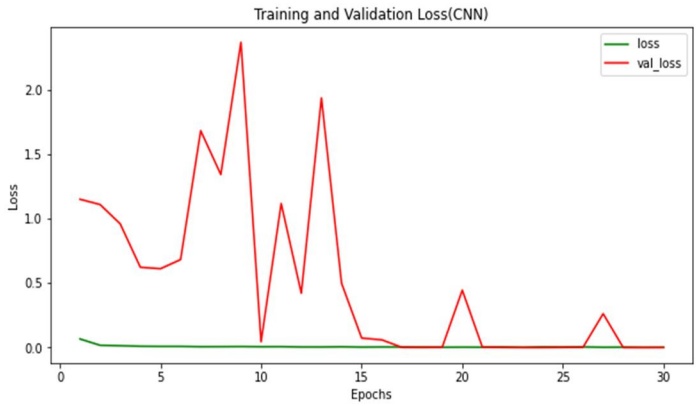


Fig 10: Training loss of ANN vs Validation loss of ANN plot

Computational model of CNN uses a variation of multilayer perceptron and contains one or more convolutional layers that are connected directly or somehow pooled. To build a CNN model here we are using 1D convolutional layer, where 1DConvo is suitable for numerical data related classification models. Even though CNN extensively gives a very good result when we are dealing with the image kind of data, using CNN 1DConvo in this implementation computed a better result compared to other deep learning algorithms.

DeepMIA model when tested with the test data below mentioned are the accuracy that are obtained with all the different model used

Table 1: Accuracy comparison of DeepMIA models

Model	Test Accuracy
FFNN	91.10%
LSTM	66.93%
CNN	99.605

From the testing results that are obtained for the different models, CNN gives best classification results to detect the malicious insider attack type in the IoT environment data. To define the performance of the classification results, figure 11 shows the confusion matrix of multiclass classification of Insider attack made.

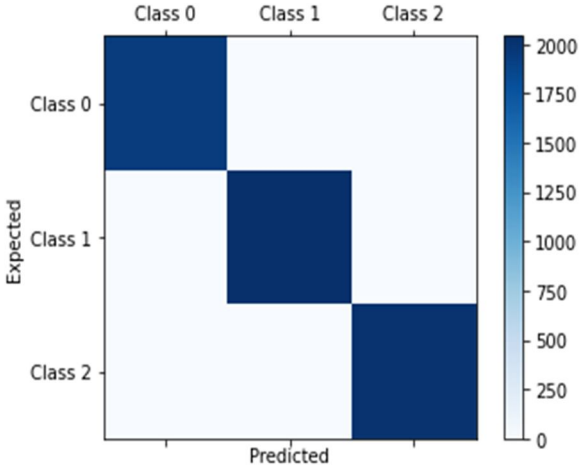


Fig 11: Confusion matrix for multiclass classification

VII. CONCLUSION

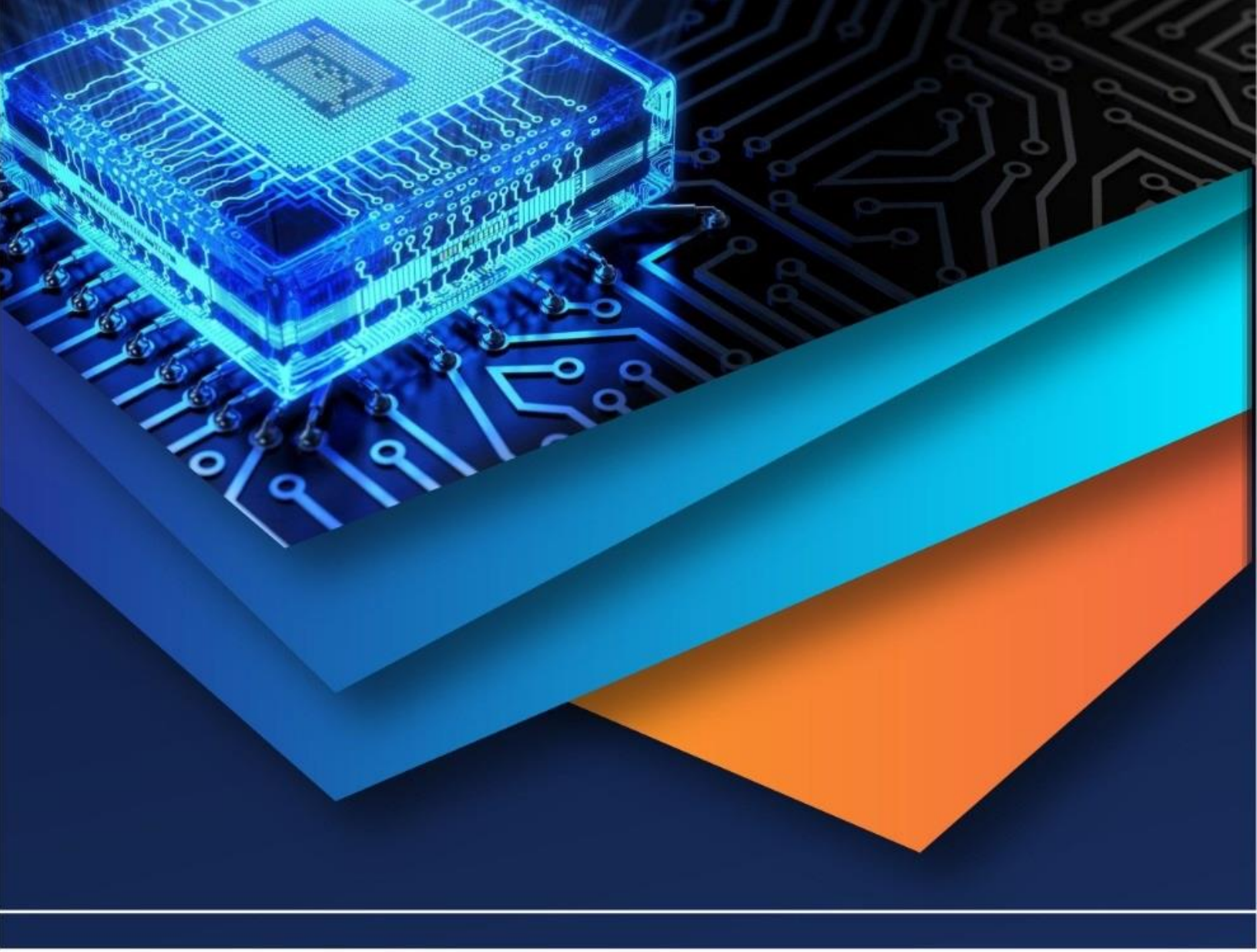
DeepMIA is an accelerated and integrated model, which is based on deep learning technique in the field of artificial Intelligence proposes the work to detect the insider attack. By extracting the domain specific patterns of IoT device, data cleaning, data resampling, feature extraction and format conversion are performed to extract the attack characteristics. Then features that are extracted used as input features of deep learning models, and the feed-forward neural network, long short-term memory and convolutional neural network algorithms are used to train and obtain the DeepMIA detection model. Then the normal IoT device data or network-connected device data is mixed with the attack data for model test. The experimental results show that the proposed DeepMIA detection method based on deep learning has a good detection accuracy rate of 98% for the current popular Malicious Insider attacks.

VIII. FUTURE ENHANCEMENT

Model can be implemented on other attacks like Application Layer Attack, Protocol Attack, Volumetric Attack with large dataset using deep learning techniques. Increasing the size of the data we can achieve the better accuracy with other deep learning algorithms. More Deep learning techniques can be incorporated for the detection purpose and comparison analysis

REFERENCES

[1] Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," in IEEE Access, vol. 8, pp. 11743-11753, 2020.
[2] D. C. Le, N. Zincir-Heywood and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 30-44, March 2020.
[3] N. Baracaldo, B. Palanisamy and J. Joshi, "G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, pp. 84-98, 1 Jan.-Feb. 2019.
[4] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2242-2270, Fourth quarter 2015.
[5] Owen. Lo, William. J. Buchanan, Paul. Griffiths, and Richard. Macfarlane "Distance measurement methods for improved insider threat detection". Security and Communication Networks, vol 2018, Article ID 5906368, 2018.
[6] Faisal. Hussain, Syed Ghazanfar Abbas, Ivan Miguel Pires, Sabeeha Tanveer, Ubaid U Fayaaz, Nuno M Garcia, Ghalib A shah. "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021.
[7] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020.
[8] Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., Fang, B. (2018). Insider Threat Detection with Deep Neural Network. In International Conference on Computational Science – ICCS 2018. Lecture Notes in Computer Science, vol 10860.
[9] D. Sun, M. Liu, M. Li, Z. Shi, P. Liu and X. Wang, "DeepMIT: A Novel Malicious Insider Threat Detection Framework based on Recurrent Neural Network," 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2021, pp. 335-341.
[10] M. Mamun and K. Shi, "DeepTaskAPT: Insider APT detection using Task-tree based Deep Learning," in 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 2021 pp. 693-700.
[11] Saaudi, Z. Al-Ibadi, Y. Tong and C. Farkas, "Insider Threats Detection Using CNN-LSTM Model," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 2018, pp. 94-99.
[12] S.-K. Choi, C.-H. Yang, and J. Kwak "System hardening and security monitoring for iot devices to mitigate iot security vulnerabilities and threats." In KSII Transactions on Internet and Information Systems, 2018.
[13] A. J. Hall, N. Pitropakis, W. J. Buchanan and N. Moradpoor, "Predicting Malicious Insider Threat Scenarios Using Organizational Data and a Heterogeneous Stack-Classifier," 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 5034-5039.
[14] K. Huang, L. -X. Yang, X. Yang, Y. Xiang and Y. Y. Tang, "A Low-Cost Distributed Denial-of-Service Attack Architecture," in IEEE Access, vol. 8, pp. 42111-42119, 2020.
[15] H. Mohammed, S. R. Hasan and F. Awwad, "Fusion-On-Field Security and Privacy Preservation for IoT Edge Devices: Concurrent Defense Against Multiple Types of Hardware Trojan Attacks," in IEEE Access, vol. 8, pp. 36847-36862, 2020.
[16] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020.
[17] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020.
[18] M. M. Rana and R. Bo, "IoT-Based Improved Human Motion Estimations Method Under Cyber Attacks," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10934-10935, Dec. 2019.
[19] J. Jiang et al., "Anomaly Detection with Graph Convolutional Networks for Insider Threat and Fraud Detection," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019, pp. 109-114.
[20] P. Chattopadhyay, L. Wang and Y. -P. Tan, "Scenario-Based Insider Threat Detection From Cyber Activities," in IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 660-675, Sept. 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY