IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Behavioral Based -Insider Thread Detection using Deep Learning

Chepkwony Collins Kiprotich[1], Dr. Devi Kannan[2]

[1]Student,[2] Associate Professor, Department of Computer Science and Engineering

[1,2]Atria Institute of Technology| ASKB Campus,Anandnagar,Bangalore; Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka India

Abstract Recent studies have highlighted that insider threats are more destructive than external network threats. This project mainly focuses on the user behavior to detect the insider attack within the organization. Based on the above considerations, we have come up with some solutions where we focus on the behavior of individual user, User activities and analysis on the access rights and usage to check the outcome as whether they are Normal user with no harm or Abnormal (Malicious). Feature Engineering is the process where we select the fixed set of procedures to identify behavior of the employee effectively. The implementation is done by applying various machine learning and deep learning algorithms to get high classification accuracy of the model. The trained data is feed to the Model engine to gain the experience about the user activities and test data is used to find the accuracy of the model and defining the behavior of the user a normal or malicious. The data used is the CMU CERT synthetic insider threat dataset version r5.2 Our unique approach produces comparatively good accuracy of 100%.

INDEX TERMS include insider threat, deep learning, machine learning, user behavior, and information security.

I. INTRODUCTION

The major impact of problem to the cyber security in not basically from the outsider malicious malwares or spywares, the insider can harm the organization by leaking the information to the outside world. The problem is getting worst every day as information is growing bigger and bigger. According to the survey from the survey testimony i.e. Insider Report 2020, it is proven that 92% of the organizations are prone to insider threat from their own resources. As the insider has the access to the resources and organizational assets, there might be the chances that they can demoralize the data availability, Confidentiality and Integrity of confidential information than exterior attackers. There may be many reasons behind the motivation to the insider to leak the organizational data such as Organizational political affairs, Pressure, Greediness, Anger, Commercial Gain, Betrayal, Jealousy, Dissatisfaction over work pressure and other parameters which affect the system as shown in figure 1:

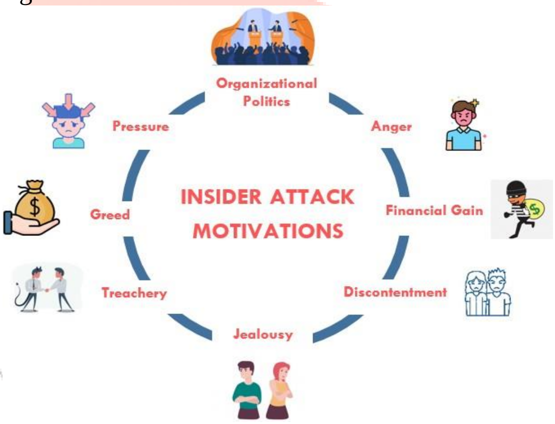


FIGURE 1. Insider attack motivations.

The malicious employee is first who can breach the security and harm the company security system by theft and defacement of records. Almost 65% of the damage happens due to carelessness and negligent employees (Inadvertent Insiders, Malicious Insiders, and Discontented Insiders, External third parties, Contractors and IT Employees and software suppliers as shown in Figure 2

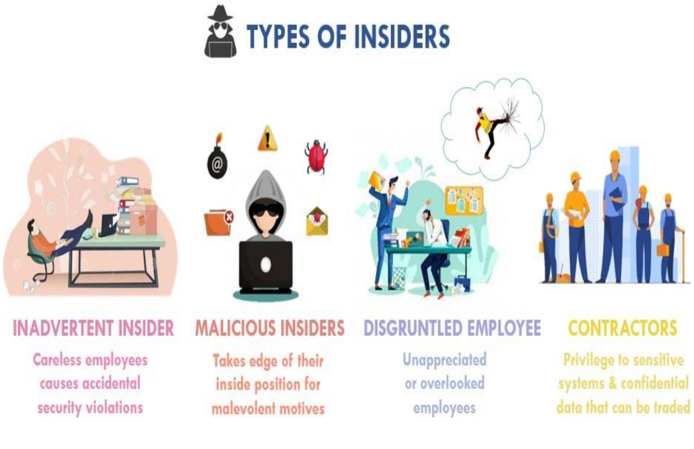

TYPES OF INSIDERS
INADVERTENT INSIDER
Careless employees causes accidental security violations
MALICIOUS INSIDERS
Takes edge of their inside position for malevolent motives
DISGRUNTLED EMPLOYEE
Unappreciated or overlooked employees
CONTRACTORS
Privilege to sensitive systems & confidential data that can be traded

FIGURE 2. Insider types.

According to the survey, the chief hazards are personnel workers (50%), Restricted IT Employees (59%) and other contractors (52%) as shown in Figure 3. Every organization having many employees, among them some of the employees use unnecessary access right by damaging confidentiality of data, complexities in technology usage, lack of knowledge in knowing the system prototyping and harm the system as well as thoughtful data.

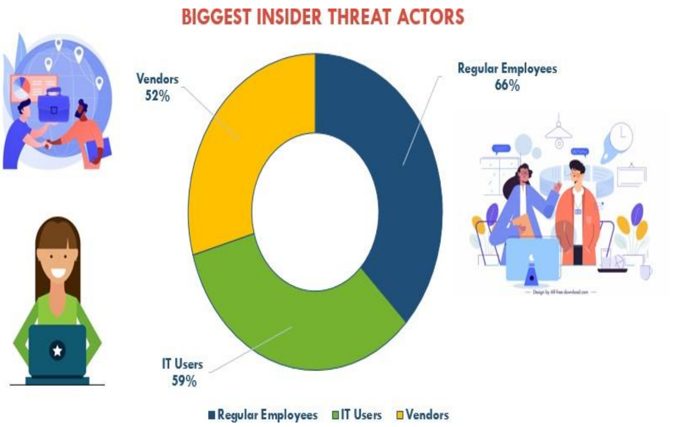


FIGURE 3. Biggest insider threat actors.

Machine Learning, Deep Learning, Artificial Intelligence are the trending focused areas to define the effective system or architecture deployment to minimize the damage from the insider by proving more security features to the existing system. Machine Learning provides the solution to highest extent, but deep learning also into the competition to detect the insider threat activities and present the improved results. This results in outstanding security system that can be robust and available to adapt easily by all the organizations to save themselves from information leakage.

II. LITERATURE REVIEW

Many authors have contributed their research on the above trending technologies and problem. The survey helps in enhancing the knowledge towards the field of cyber security. Many theories, Novel Approaches and strategies are deliberated to stop the unintentional entertainments that undesirably affect the privacy, secrecy, confidentiality and organizational assets. [1] The authors have given the description about the current scenario over the detection of insider threat using machine learning techniques. The proposed system uses Feature Engineering algorithm i.e. Convolutional Neural Networks (CNN) algorithm to resolve the above stated problem. The user behaviour is the central point of study and used Deep Neural Network (DNN) approach and has produced the novel methodology to detect the insider threat and analyze the user behavior. [2] The author proposed the experimental study to detect the mischievous insiders using the Recurrent Neural Networks (LSTM-RNN) model. Framework design includes various components such as Feature Engineering, Aggregator for occurrence of events, different attribute-based classifiers anomaly detection calculator application, all together integrated to form the final insider threat detection system. [3] The hybrid model has been used to mitigating the insider threat problem, which is founded on the Graphical Investigation scheme and anomaly detection strategies to solve the cyber threat of insider employees. The Graphical Processing unit (GPU) contains of Induced Sub Graphs, Graph/Sub graph Attribute Extraction, Generate Original Graph and Graph/Sub graph attributes. [4] The author explained the detailed explanation about the Data mining technique to identify the insider threat using unbalanced CERT Dataset. They have mainly concentrated the reducing the time to Train, Test and validate the data rather than the findings of accuracy of the Machine Learning Models. The impact on analysis is more on the imbalanced dataset. They have made extensive survey of machine learning algorithms taking the parameters such as Framework design, System configurations, Proposed Environment, Experimental Outcomes, Parameters study during the evaluation and implemented in Real-time or not. [5] The author has done an excellent job on Multiple Data Granularity stages to find the threat detection in organization and Anomaly-based detection on ML algorithms. The Evaluation metrics are calculated on individual and group of users. Here the supervised Machine Learning (ML) algorithms and Unsupervised Anomaly-Based detection creates a better impact on the data high precision and low recall rate. The proposed algorithms consist of 5 stages of design interfaces namely Data collection (CERT), Data Acquisition (Reasoning, User Data, Probability, and Frequency Distributions), Detection Unit (Anomaly-Based Detection Stage and ML-Based Detection Stage) and the final phase is performance evaluation and predictions (Normal or Malicious).

III. SYSTEM ANALYSIS AND IMPLEMENTATION

Across the globe, there are lot of research going on to address the different issues pertaining to the Threat from the insiders. Here in our proposed system, we have mentioned the various methods to resolve the issue. The process of detecting the insider and misbehavior der threat traces the fake alarms to the administrator whenever it finds the malicious activity of many employees in the organization.

a) Aim

To tackle the aforementioned shortcoming in the problem statement, we have tried to focus on the detection of malicious or non-malicious using deep learning model and Standard CERT CMU r5.2 Dataset and predicting the possibility of Malicious or Normal (Non-Malicious).

b) Comparative study of Existing techniques.

Some of the techniques in existing system are efficient, but have some deficiencies in terms of complexity, performance evaluation metrics and evaluation dataset. Some models are not evaluated on real life scenarios and are processing & memory intensive. Some have relatively small test data, which does not fully evaluate the performance of the technique.

c) Proposed Scheme for Insider Detection.

The proposed system consists of various stages of executions. Initially the input, Dataset is collected from the CERT CMU (Computer Emergency Readiness Team Carnegie Mellon University) by version r5.2. The dataset are namely File.csv, logon.csv, http.csv, device.csv, email.csv. The second stage of the proposed system is importing the python APIs. Next stage is to pre-process the input dataset. As the dataset is not labelled, we need to apply the methodologies to convert the categorical data into similar to integer format and assign the label to the dataset. Once the labelling is done, we can train the deep learning model and dataset is divided into training and testing data based on some split ratios. The developed Models such as LSTM-CNN and Bidirectional LSTM-CNN are applied to get the highest accuracy of the model. The prediction can be shown as Malicious and Non-Malicious data values.

d) Objectives

To accomplish the aforementioned aims, we set the objectives of our research work that are substantially grounded on the behavior of the users within the organization.

The objectives of the project are categorized as:

1. Data Gathering or the collection of dataset for the study from the genuine source.
2. Data Preprocessing and Feature Extraction of the attributes which are important part of data analysis.
3. Building the Deep Learning models (LSTM-CNN and Bidirectional LSTM-CNN)
4. Finding the accuracy and loss of the model
5. Classification and Predictions
6. Exploratory Analysis on the Dataset and finding the various scenarios of data presentations.

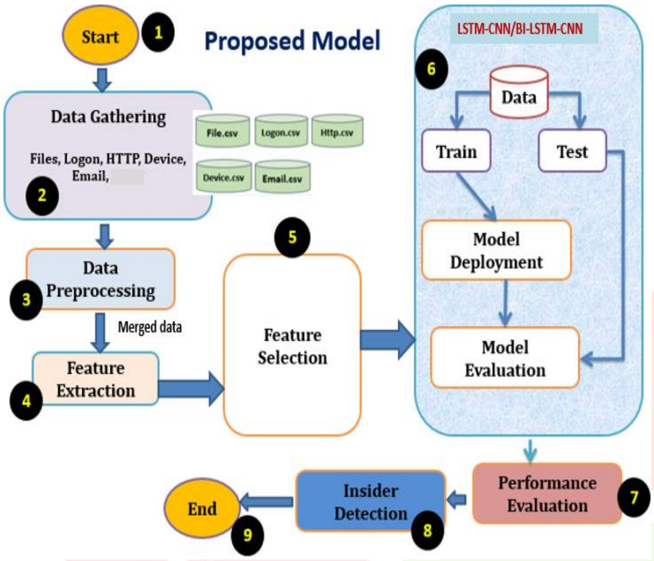


FIGURE 4. Structure of our proposed solution.

1. Data Collection.

The data acquisition is the first phase of every system design. Here we have used the existing Dataset from the Carnegie Mellon University CMU-CERT with various versions of version r1 to version r6. Basically the information present in the dataset comprises of Malicious and Non-Malicious User's Activities. We have collected the data and converted data into .csv files (Comma Separated Value). The next step is Data extraction before producing the data to the model development. We have taken 1000 Instances of data from each dataset, according to the survey collected, among 1000 users, 70 users are malicious insiders.

- **logon.csv:** Information about the User's Login and Logout
- **Device.csv:** The users connecting and disconnecting to the External USB devices
- Http.csv: The complete browsing history information is recorded here.
- **Email.csv:** Email information like sent, received, cc, Bcc etc.
- **file.csv:** Information pertaining to the file transfer (Sent and Received from the system)
- **Psychometric.csv:** Users personal features.
- **LDAP** (Lightweight Directory Access Protocol): Directory service & Job roles and files related to users.

2. Data Preprocessing.

Before feeding data to the model, the information or the input need to be preprocessed, we are applying various schemes of preprocessing like cleaning the data, removing irrelevant rows and columns, data abstraction and final data aggregation. We are parsing all the above mentioned .csv files, aggregate files and convert into preprocessed_filename.csv format. Finally, we are creating the master preprocessed csv files. The feature engineering process can be applied on both textual and numerical type of data.

3. Feature Extraction.

Feature extraction is a process of renovating the fresh input data into the integral attributes and the main thing is we must preserve the data during the extraction phase. The data integrity, data confidentiality and storage are important and retain the original information of dataset. The raw data is processed at each stage and cleaned attributes which required for the study are extracted. First stage in feature extraction refers to the parsing of data; the important attributes are extracted, which are useful in predicting the behavior of the users. Usually the working hours for the first shift for the employee are around 8:00AM to 7: 00PM. If any user login with the credentials after the office hour and login from the different computer, that activity can be logged and considered as malicious activity. Some of the features like Day, Time, Personal Computer, User identification Number, User roles, Functional Units; Departments are extracted for the study of our project. Some of the Feature Extraction table are mentioned below:

4. Model Building.

The deep learning models we are implementing here are, Namely LSTM-CNN and Bidirectional LSTM-CNN. We have used CNN layers for feature extraction and LSTM module for the prediction. CNN LSTM is a powerful category of deep learning model that is used for deep data learning for both spatially and temporally dataset and performs all the input and output. CNN uses a process called Convolution in finding the relationship between the two variable or functions. The function shape can be modified.

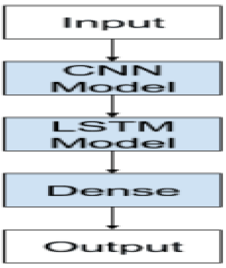


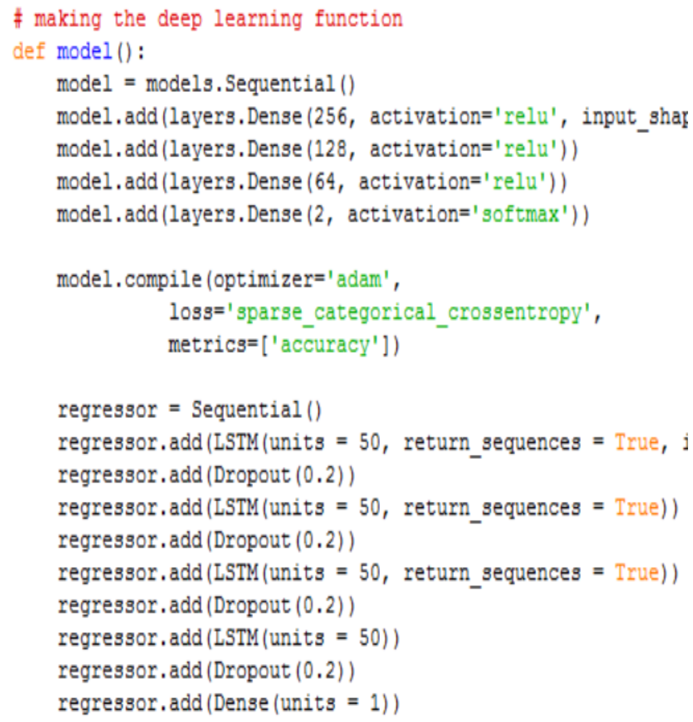
FIGURE 5. LSTM-CNN Model Structure

e) Methodology

Building the Deep Learning Models:

1. Long Short-Term Memory networks (LSTMs)

LSTM-CNN is a variant of Recurrent Neural Network (RNN) mostly used in time series and gradient problems and long term convolutions. LSTM –CNN can be implemented on three basic layers Input Layer, Hidden Layer and Output Layer. When there is an autocorrelation in the input data, time series forecasting is very easily adopted by using LSTM. Here we are using LSTM stateful architecture for real time prediction and finding the accuracy of the model.

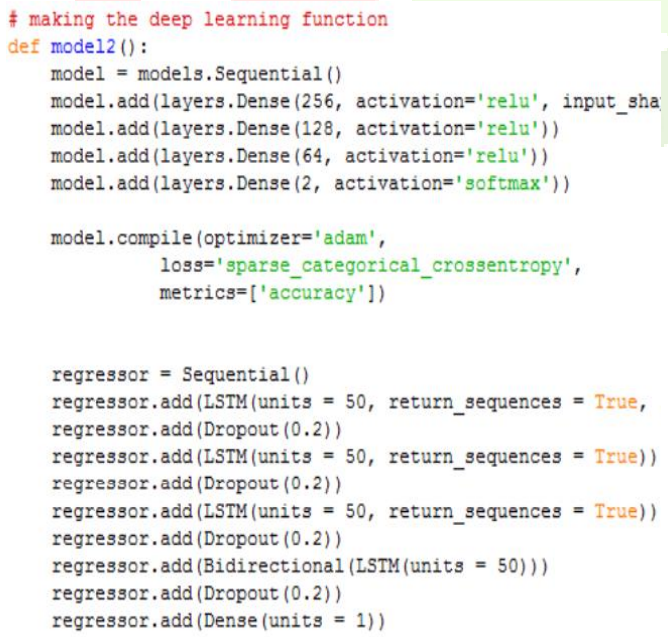


```
# making the deep learning function
def model():
    model = models.Sequential()
    model.add(layers.Dense(256, activation='relu', input_shap
    model.add(layers.Dense(128, activation='relu'))
    model.add(layers.Dense(64, activation='relu'))
    model.add(layers.Dense(2, activation='softmax'))

    model.compile(optimizer='adam',
                  loss='sparse_categorical_crossentropy',
                  metrics=['accuracy'])

    regressor = Sequential()
    regressor.add(LSTM(units = 50, return_sequences = True, i
    regressor.add(Dropout(0.2))
    regressor.add(LSTM(units = 50, return_sequences = True))
    regressor.add(Dropout(0.2))
    regressor.add(LSTM(units = 50, return_sequences = True))
    regressor.add(Dropout(0.2))
    regressor.add(LSTM(units = 50))
    regressor.add(Dropout(0.2))
    regressor.add(Dense(units = 1))
```

FIGURE 6. LSTM-CNN Model Configuration

2.Bidirectional LSTM-CNN.

Whenever we need to design a model to run the sequence of information in either direction i.e. Forward Engineering and Backward Engineering, we use Bidirectional LSTM-CNN model. Here we can save the information of Past and Future values.



```
# making the deep learning function
def model2():
    model = models.Sequential()
    model.add(layers.Dense(256, activation='relu', input_sha
    model.add(layers.Dense(128, activation='relu'))
    model.add(layers.Dense(64, activation='relu'))
    model.add(layers.Dense(2, activation='softmax'))

    model.compile(optimizer='adam',
                  loss='sparse_categorical_crossentropy',
                  metrics=['accuracy'])


    regressor = Sequential()
    regressor.add(LSTM(units = 50, return_sequences = True,
    regressor.add(Dropout(0.2))
    regressor.add(LSTM(units = 50, return_sequences = True))
    regressor.add(Dropout(0.2))
    regressor.add(LSTM(units = 50, return_sequences = True))
    regressor.add(Dropout(0.2))
    regressor.add(Bidirectional(LSTM(units = 50)))
    regressor.add(Dropout(0.2))
    regressor.add(Dense(units = 1))
```

FIGURE 7. Bidirectional LSTM-CNN Model Configurations

3. Prediction

The prediction can be done on insider threat data and we trained the model using LSTM-CNN and Bidirectional LSTM-CNN. The outcome can be either malicious or non-malicious. The accuracy and loss for both the models are shown here.

IV. RESULTS AND ANALYSIS.

The two algorithms Namely CNN-LSTM and Bidirectional LSTM-CNN are used and model is deployed. Accuracy of the both models is 100%. The prediction shows that whether the users are malicious or Normal in behavior. Although they both have the same accuracy we observe Bidirectional LSTM-CNN executes the results faster and with very negligible loss as compare with CNN-LSTM. This is shown in below figures:

1. Results of LSTM-CNN

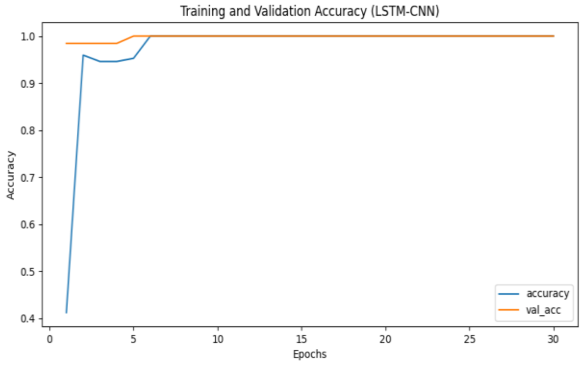


FIGURE 8. Training and Validation Accuracy (LSTM-CNN)

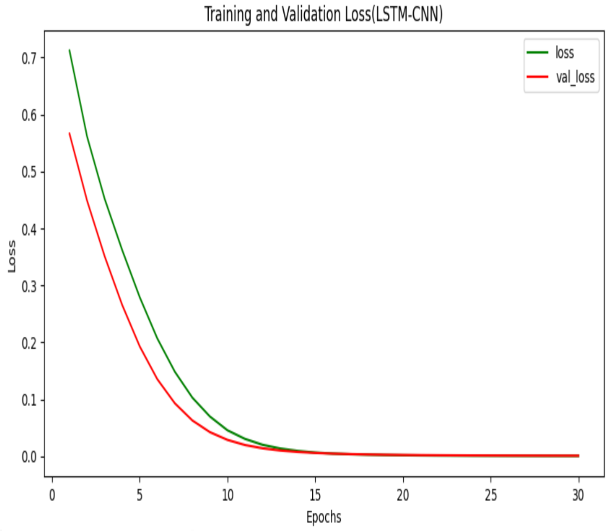


FIGURE 9. Training and Validation Loss (LSTM-CNN)

2. Results of Bidirectional (LSTM-CNN)

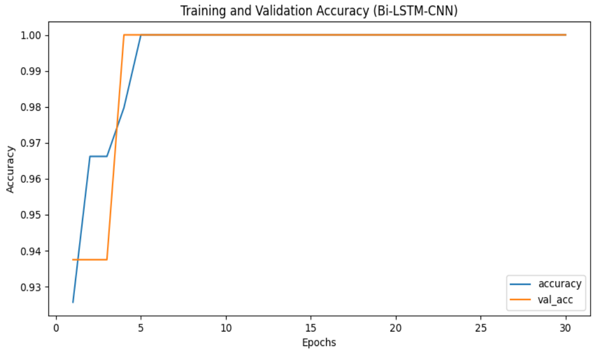


FIGURE 10.Training and Validation Accuracy (Bi-LSTM-CNN)

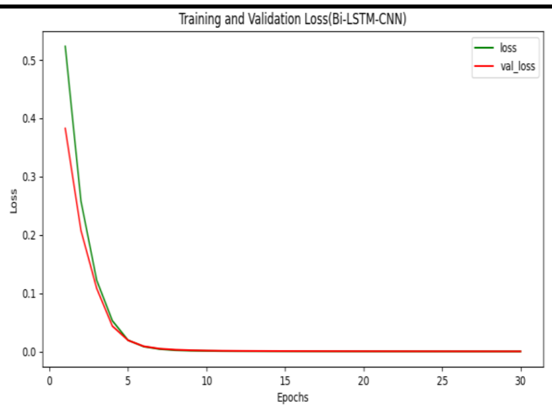


FIGURE 10.Training and Validation Loss (Bi-LSTM-CNN)

V. CONCLUSION

The project aim was to detect the insider threat detection using r5.2 CERT CMU dataset. We have taken various .csv log files to carry out the experiment. In the initial stage the Dataset used are not having the labels, so we applied the process of data mining techniques such as Pre-processing and Feature Extractions. We processed all the files and merged to form the new dataset for training, Testing and validation. The preprocessed dataset is used here to develop the models. The two Models LSTM-CNN and Bidirectional LSTM-CNN models are developed and found the accuracy of the models 100% respectively. We experimented the model and calculated the Accuracy and loss.

REFERENCES

[1] Fangfang Yuan1, Yanan Cao1, Yanmin Shang, Yanbing Liu1, Jianlong Tan1, and Binxing Fang, “Insider Threat Detection using Deep Learning,” in ICCS 2018: Computational Science – ICCS ,2018.

[2] Authors: Fanzhi Meng, Fang Lou, Yunsheng Fu, Zhihong Tian “Deep Learning based Attribute Classification Insider Threat Detection for Data Security,” in IEEE Third International Conference on Data Science in Cyberspace, 2018.

[3] Lingli Lin , Shangping Zhong , Cunmin Jia , Kaizhi, “Insider threat detection based on deep belief network feature representation,” in International Conference on Green Informatics, 2018.

[4] Naghmeh Moradpoor Sheykhkanloo, “Insider Threat Detection Using Supervised Machine Learning Algorithms on an Extremely Imbalanced Dataset,” in International Journal of Cyber Warfare and Terrorism ,April-June 2020.

[5] Duc C. Le, Nur Zincir-Heywood, “Exploring anomalous behavior detection and classification for insider threat identification,” in International Journal of Network Management , 2020.

[6] Insider Report 2018, CA Technol., New York, NY, USA, 2018.

[7] Insider Threat Report 2019, CA Technol., San Jose, CA, USA, 2019. [3] S. R. Band, D. M. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw, and R. F. Trzeciak, ‘‘Comparing insider IT sabotage and espionage: A model-based analysis,’’ Carnegie Mellon Univ., Softw. Eng. Inst., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2006TR-026, 2006

[8] P. Chattopadhyay, L. Wang, and Y.-P. Tan, ‘‘Scenario-based insider threat detection from cyber activities,’’ IEEE Trans. Comput. Social Syst., vol. 5, no. 3, pp. 660–675, Sep. 2018.

[9] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, ‘‘Insider threat detection with deep neural network,’’ in Proc. Int. Conf. Comput. Sci. Cham, Switzerland: Springer, 2018.

[10] W. Jiang, Y. Tian, W. Liu, and W. Liu, ‘‘An insider threat detection method based on user behavior analysis,’’ in Proc. Int. Conf. Intell. Inf. Process. Amsterdam, The Netherlands: International Federation for Information Processing, 2018, pp.

[11] J. Jiang, J. Chen, K.-K.-R. Choo, K. Liu, C. Liu, M. Yu, and P. Mohapatra, ‘‘Prediction and detection of malicious insiders’ motivation based on sentiment profile on webpages and emails,’’ in Proc. MILCOM, Oct. 2018, pp. 1–6.

[12] D. Zhang, Y. Zheng, Y. Wen, Y. Xu, J. Wang, Y. Yu, and D. Meng, ‘‘Role-based log analysis applying deep learning for insider threat detection,’’ in Proc. SecArch, Toronto, ON, Canada, Jan. 2018, pp. 18–20.

[13] K. A. Tabash and J. Happa, ‘‘Insider-threat detection using Gaussian mixture models and sensitivity profiles,’’ Comput. Secur., vol. 77, pp. 838–859, Aug. 2018. [12] O. Lo, W. J. Buchanan, P. Griffiths, and R. Macfarlane, ‘‘Distance measurement methods for improved insider threat detection,’’ Secur. Commun. Netw., vol. 2018, pp. 1–18, Jan. 2018.

[14] A. Gamachchi, L. Sun, and S. Boztas, ‘‘Graph based framework for malicious insider threat detection,’’ in Proc. 50th Hawaii Int. Conf. Syst. Sci. (HICSS), 2017, p. 10.

[15] F. Meng, F. Lou, Y. Fu, and Z. Tian, ‘‘Deep learning based attribute classification insider threat detection for data security,’’ in Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace, Jun. 2018,pp.576–581