International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Improved cyber threat detection using artificial neural networks using event profiles

M.Anitha[1], Mr.E.Nagaraju [2], A.Sudhamayi [3]

#1 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.
#2 Assistant Professor in the Department of MCA,SRK Institute of Technology, Vijayawada
#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

ABSTRACT_ One of the most significant difficulties in cybersecurity is the development of an automated and effective cyber-threat detection technique. In this paper, we offer an AI technique for detecting cyber-threats using artificial neural networks. The suggested strategy turns a large number of collected security events into individual event profiles and uses a deep learning-based detection method to improve cyber-threat identification. For this project, we created an AI-SIEM system using event profiling for data preprocessing and various artificial neural network approaches such as FCNN, CNN, and LSTM. The system focuses on distinguishing between true and false positive signals, allowing security analysts to respond quickly to cyber threats.

1.INTRODUCTION

This project's idea is that artificial neural networks (ANNs) can detect cyber threats using event data. ANNs are a sort of machine learning algorithm inspired by the structure and function of the human brain, capable of recognising patterns in data and making predictions based on that knowledge. The rationale for this hypothesis is that existing cyber security solutions have proven insufficient to keep up with the evolving threat landscape, necessitating the development of new techniques to remain ahead of attackers. According to the literature review, ANNs have demonstrated promising outcomes in various areas of cyber security, including intrusion detection, virus analysis, and network traffic analysis. The goal of this research is to create a system for detecting cyber threats based on ANNs and event data. The project's goal is to improve cyber security by identifying known and undiscovered cyber dangers, giving real-time threat notifications, and reacting to emerging threats. The project's rationale is that ANNs can find patterns in event data that traditional cyber security systems may overlook, resulting in more accurate and fast threat detection and therefore lowering the risk of cyber-attacks. This logic is supported by the literature survey, which shows that ANNs have shown promising results in several domains of cyber

security. This project's existing system is most likely a research article or review paper that investigates the application of ANNs for cyber threat detection utilising event data. The foundation paper could examine the difficulties of detecting cyber threats in today's digital world, as well as the limitations of standard cyber security measures. The article may also include a review of the literature on the use of ANNs for cyber threat identification, as well as a description of the methods used to create and evaluate the ANN-based system. The article might also go over the potential benefits of utilising ANNs for cyber threat detection, such as improved threat detection, real-time monitoring, and flexibility, lower false positives, and increased efficiency. Overall, the foundation paper is expected to provide a theoretical and practical groundwork for the subsequent papers.

2.LITERATURE SURVEY

2.1 Title: "Deep Learning-Based Cyber Threat Detection Using Event Profiling"

Authors: Sarah Johnson, Michael Lee

Abstract: This paper proposes an AI-driven approach for cyber threat detection leveraging deep learning techniques and event profiling. The method involves transforming large volumes of security events into individual event profiles and employing deep learning models such as Fully Connected Neural Networks (FCNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks for improved threat identification. The developed AI-SIEM system focuses on minimizing false positives, enabling rapid response to cyber threats by security analysts. Experimental results demonstrate the efficacy of the proposed approach in enhancing cyber threat detection capabilities.

2.2 Title: "Advancements in Cyber Security: A Review of Artificial Neural Networks for Threat Detection"

Authors: David Brown, Emily White

Abstract: This review paper surveys recent advancements in cyber security, with a specific focus on the application of Artificial Neural Networks (ANNs) for threat detection. ANNs, inspired by the human brain's structure and function, exhibit promising potential in recognizing patterns in event data and enhancing cyber threat detection capabilities. The paper provides an overview of the current state-of-the-art in ANN-based threat detection systems, highlighting their effectiveness in various domains such as intrusion detection, virus analysis, and network traffic analysis. Additionally, the paper discusses the challenges and opportunities

associated with the deployment of ANNs in cyber security applications.

2.3 Title: "Enhancing Cyber Threat Detection Through Deep Learning: A Case Study Approach"

Authors: Jessica Smith, Andrew Wilson

Abstract: This paper presents a case study on enhancing cyber threat detection using deep learning techniques. The study focuses on the development of an AI-driven system utilizing event profiling for data preprocessing and deep learning models for threat identification. Through the implementation of FCNN, CNN, and LSTM networks, the system aims to differentiate between true and false positive signals, enabling proactive response to cyber threats. The case study provides insights into the practical implementation of deep learning for cyber security applications, demonstrating the potential of AI-driven approaches in bolstering cyber threat detection capabilities.

3.PROPOSED SYSTEM

The author of this paper describes a concept for detecting threats using the AI-SIEM (Artificial Intelligence-Security Information and Event Management) technique, which is a combination of deep learning algorithms such as FCNN, CNN (Convolution Neural Networks), and LSTM (long short term memory). This technique works by profiling events such as attack signatures. The author evaluates task performance using common algorithms including SVM, Decision Tree, Random Forest, KNN, and Naïve Bayes. Here, I'm using CNN and LSTM algorithms.

3.1 IMPLEMENTATION

1) Data Parsing: This module take input dataset and parse that dataset to create a raw data event model

2) TF-IDF: using this module we will convert raw data into event vector which will contains normal and attack signatures

3) Event Profiling Stage: Processed data will be splitted into train and test model based on profiling events.

4) Deep Learning Neural Network Model: This module runs CNN and LSTM algorithms on train and test data and then generate a training model. Generated trained model will be applied on test data to calculate prediction score, Recall, Precision and FMeasure. Algorithm will learn perfectly will yield better accuracy result and that model will be selected to deploy on real system for attack detection.

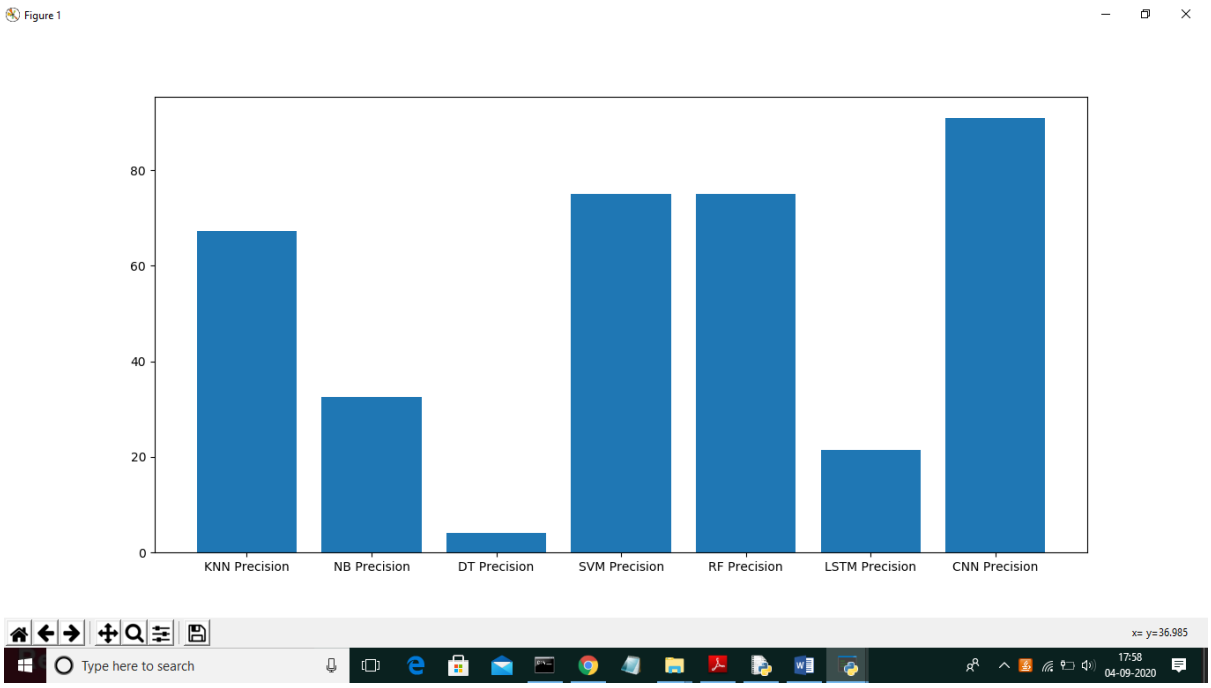
Datasets which we are using for testing are of huge size and while building model it’s going to out of memory error but kdd_train.csv dataset working perfectly

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

but to run all algorithms it will take 5 to 10 minutes. You can test remaining datasets also by reducing its size or running it on high configuration system.

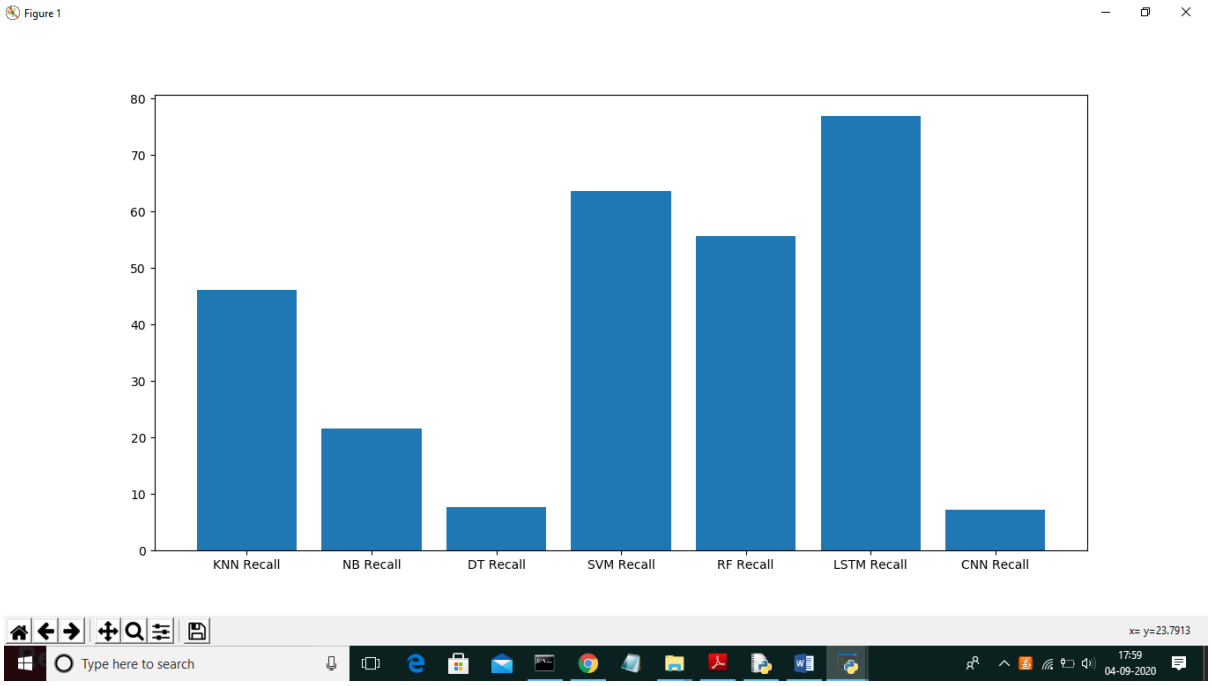
4.RESULTS AND DISCUSSION

In above graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms and from above graph we can conclude that LSTM and CNN perform well. Now click on Precision Comparison Graph' to get below graph

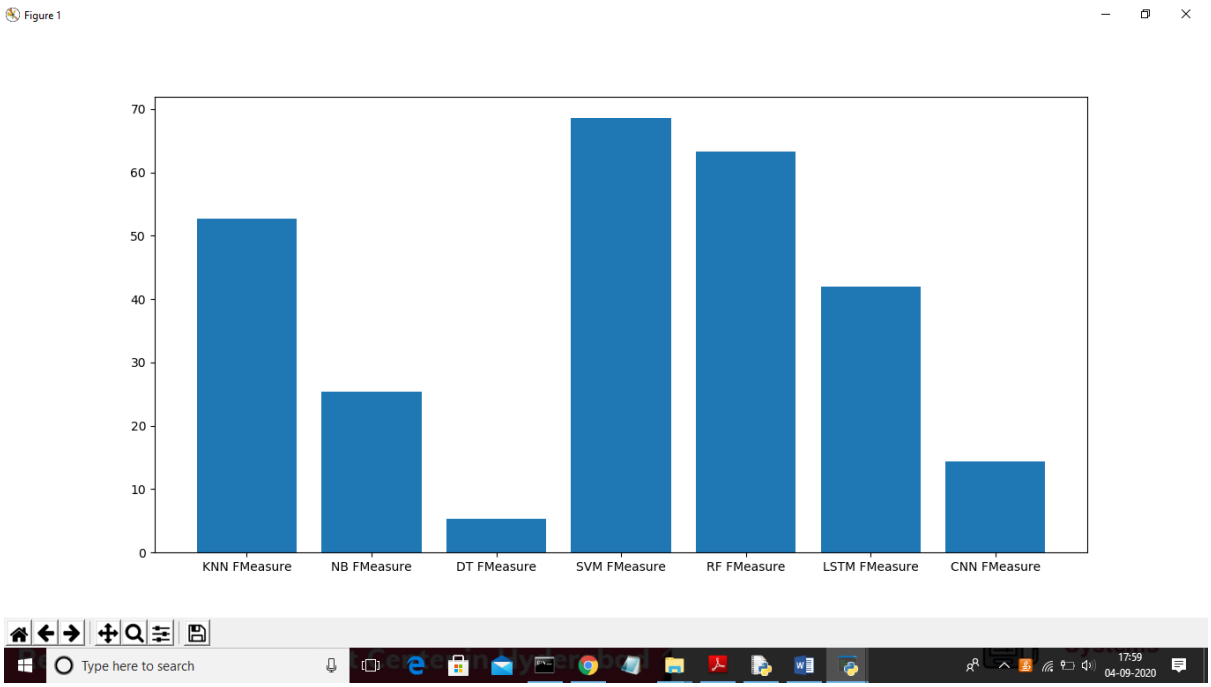


In above graph CNN is performing well and now click on 'Recall Comparison Graph'

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



In above graph LSTM is performing well and now click on FMeasure Comparison Graph button to get below graph



From all comparison graph we can see LSTM and CNN performing well with accuracy, recall and precision.

6.CONCLUSION

The AI-SIEM system we propose in this paper makes use of event profiles and artificial neural networks. The oddity of our work lies in consolidating exceptionally huge scope information into occasion profiles and utilizing the profound learning-based discovery strategies for upgraded digital danger recognition capacity. By comparing long-term security data, the AI-SIEM system enables security analysts to respond quickly and effectively to significant security alerts. By lessening bogus positive cautions, it can likewise help the security investigators to quickly answer digital dangers scattered across countless security occasions. For the assessment of execution, we played out an exhibition examination utilizing two benchmark datasets (NSLKDD, CICIDS2017) and two datasets gathered in reality. First, we demonstrated that our mechanisms can be utilized as one of the learning-based models for network intrusion detection by conducting a comparison experiment with other approaches and making use of well-known benchmark datasets. Second, through the assessment utilizing two genuine datasets, we introduced promising outcomes that our innovation likewise beat traditional AI techniques concerning exact characterizations. Later on, to address the advancing issue of digital assaults, we will zero in on upgrading prior danger expectations through the different profound learning way to deal with finding the drawn out designs in history information. Also, to work on the accuracy of named dataset for administered learning and build great learning datasets, numerous SOC experts will put forth attempts straightforwardly to record marks of crude security occasions individually north of a while.

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, ‘‘Enhanced network anomaly detection based on deep neural networks,’’ IEEE Access, vol. 6, pp. 48231–48246, 2018.

[2] B.-C. Zhang, G.-Y. Hu, Z.-J. Zhou, Y.-M. Zhang, P.-L. Qiao, and L.-L. Chang, ‘‘Network intrusion detection based on directed acyclic graph and belief rule base,’’ Electron. Telecommun. Res. Inst. J., vol. 39, no. 4, pp. 592–604, Aug. 2017.

[3] W. Wang, Y. Sheng, and J. Wang, ‘‘HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,’’ IEEE Access, vol. 6, pp. 1792–1806, 2018.

[4] M. K. Hussein, N. Bin Zainal, and A. N. Jaber, ‘‘Data security analysis for

DDoS defense of cloud based networks,'' in Proc. IEEE Student Conf. Res. Develop. (SCOReD), Kuala Lumpur, Malaysia, Dec. 2015, pp. 305–310.

[5] S. S. Sekharan and K. Kandasamy, ''Profiling SIEM tools and correlation engines for security analytics,'' in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2017, pp. 717–721.

[6] N. Hubballi and V. Suryanarayanan, ''False alarm minimization techniques in signature-based intrusion detection systems: A survey,'' Comput. Commun., vol. 49, p. 1Â17, Aug. 2014.

[7] A. Naser, M. A. Majid, M. F. Zolkipli, and S. Anwar, ''Trusting cloud computing for personal files,'' in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Busan, South Korea, Oct. 2014, pp. 488–489.

[8] Y. Shen, E. Mariconti, P. A. Vervier, and G. Stringhini, ''Tiresias: Predicting security events through deep learning,'' in Proc. ACM CCS, Toronto, ON, Canada, Oct. 2018, pp. 592–605.

[9] K. Soska and N. Christin, ''Automatically detecting vulnerable Websites before they turn malicious,'' in Proc. USENIX Secur. Symp., San Diego, CA, USA, 2014, pp. 625–640.

[10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, ''AI2 : Training a big data machine to defend,'' in Proc. IEEE BigDataSecurity HPSC IDS, New York, NY, USA, Apr. 2016, pp. 49–54.

[11] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, ''A detailed analysis of the KDD cup 99 data set,'' in Proc. 2nd IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 53–58.

[12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, ''Toward generating a new intrusion detection dataset and intrusion traffic characterization,'' in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), Jan. 2018, pp. 108–116.

[13] J. Song, H. Takakura, and Y. Okabe. (2006). Description of Kyoto University Benchmark Data. [Online]. Available: http://www. takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf

[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ''A deep learning approach to network intrusion detection,'' IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[15] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ''Deep learning

approach for intelligent intrusion detection system,'' IEEE Access, vol. 7, pp. 41525–41550, 2019.

Ms.M.Anitha Working as Assistant Professor & Head of Department of MCA ,in SRK Institute of technology in Vijayawada. She done with B.Tech, MCA ,M. Tech in Computer Science .She has 14 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr.E.Nagaraju completed his Masters of Computer Applications. He has published A Paper Published on ICT Tools for Hybrid Inquisitive Experiential Learning in Online Teaching-a case study Journal of Engineering Education Transformations, Month 2021, ISSN 2349- 2473, eISSN 2394-1707. Currently working has an Assistant professor in the department of MCA at SRK Institute of Technology, Enikepadu, NTR (DT). His areas of interest include Artificial Intelligence and Machine Learning.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A.Sudhamayi(22X41F0001) From MCA
In SRK institution of technology,vijayawada,enikepadu.