Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 3, pp 20-24, March 2026
ISSN (online): 30491967
DOI: https://doi.org/10.47001/JAIET/2026.303004
Available Online at https://www.jaiet.com

AI-Based Cyber Threat Detection Using Event Profiling and Deep Neural Networks

[1]Y Mohan Das, [2]M Manjula, [3]B R Harshitha, [4]G Koushik Vadan, [5]N Sai Sree, [6]M Hemalatha

[1,2,3,4,5,6]Department of Computer Science Engineering (Cyber Security), GATES Institute of Technology, Gooty, Andhra Pradesh, India
Email: [1]Mohandas.sonu@gmail.com, [2]mechirimanjula@gmail.com, [3]harshithabrreddy@gmail.com, [4]koushikvadan994@gmail.com, [5]saisreereddy63@gmail.com, [6]mhemalathapamidi@gmail.com

Abstract: One of the major challenges in cyber security is the provision of an automated and effective cyber threats detection technique. In this paper, we present an AI technique for cyber threats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learning based detection method for enhanced cyber threat detection. For this work, we developed an AISIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods, including FCNN, CNN, and LSTM. The system focuses on discriminating between true positive and false positive alerts, thus helping security analysts to rapidly respond to cyber threats. All experiments in this study are performed by authors using two benchmark datasets (NSLKDD and CICIDS2017) and two datasets collected in the real world. To evaluate the performance comparison with existing methods, we conducted experiments using the five conventional machine learning methods (SVM, kNN, RF, NB, and DT). Consequently, the experimental results of this study ensure that our proposed methods are capable of being employed as learning based models for network intrusion detection, and show that although it is employed in the real world, the performance outperforms the conventional machine learning methods.

Keywords: Cyber security, intrusion detection, network security, artificial intelligence, deep neural networks.

I. INTRODUCTION

In the modern digital world, the use of computers, internet services, and online communication has increased rapidly. Along with these advancements, cyber threats such as malware attacks, phishing, denial of service attacks, and unauthorized access are also increasing. These cyber attacks can cause serious damage to organizations by compromising sensitive information and disrupting network operations. Therefore, detecting cyber threats at an early stage has become a critical requirement for maintaining cyber security.

Traditional security systems mainly rely on predefined rules and signature based detection methods. However, these methods are not always effective in identifying new or unknown cyber attacks. To overcome this limitation, intelligent techniques from machine learning are being widely used. One such technique is the Artificial Neural Network (ANN), which is capable of learning complex patterns from large datasets and identifying abnormal activities in network systems.

In this project, cyber threat detection is performed using event profiles, which are generated from system logs, user activities, and network traffic events. These event profiles contain important information about system behavior. By analyzing these profiles using ANN, the system can learn the difference between normal and malicious activities and detect potential cyber threats more accurately.

The main objective of this work is to design an efficient cyber threat detection system that uses ANN to analyze event profile data and identify suspicious activities. This approach helps improve detection accuracy, reduce false alarms, and enhance the overall security of computer networks.

II. LITERATURE SURVEY

[1] Saleem, Y., & Bashir, M. K. (2018) In their study on enhanced network anomaly detection, Saleem and Bashir explored the application of deep neural networks (DNNs) to intrusion detection systems (IDS), aiming to improve detection accuracy in the face of evolving cyber threats. Utilizing models like Convolutional Neural Networks (CNN), Autoencoders, and Recurrent Neural Networks (RNN), they trained and test Neural Networks (RNN), they trained and tested their architectures on the NSLKDD dataset and demonstrated improved performance in anomaly detection compared to traditional machine learning methods. The study highlighted the advantage of using DNNs for

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 3, pp 20-24, March 2026
ISSN (online): 30491967
DOI: https://doi.org/10.47001/JAIET/2026.303004
Available Online at https://www.jaiet.com

automatic feature extraction and better generalization, which led to high accuracy and robust performance in realtime network intrusion environments. This work emphasizes the promising role of deep learning for enhancing the capabilities of IDS in detecting both known and unknown attacks.

[2] Network Intrusion Detection Based on Directed Acyclic Graph and Belief Rule Base (2017) This paper introduced a novel approach for intrusion detection using a Directed Acyclic Graph (DAG) integrated with a Belief Rule Base (BRB), called DAGBRB. The DAG structure enabled a hierarchical and multilayered representation of rules to address the scalability issues posed by a large set of intrusion scenarios. The use of a Covariance Matrix Adaptation Evolution Strategy (CMAES) further optimized the system's parameters, improving its accuracy and adaptability. Experimental evaluations showed that DAGBRB outperformed traditional models in terms of detection rates, particularly due to its ability to handle uncertainty and complex rule combinations effectively. This methodology presents a strong framework for intelligent and adaptive IDS design.

[3] HASTIDS: Learning Hierarchical SpatialTemporal Features Using Deep Neural Networks The HASTIDS model was developed to overcome limitations in traditional IDS by learning both spatial and temporal features from raw network traffic using deep learning architectures. This approach utilized Convolutional Neural Networks (CNNs) to capture spatial patterns and Long ShortTerm Memory (LSTM) networks for temporal behavior learning, thereby enabling more accurate anomaly detection without manual feature engineering. Evaluated on DARPA1998 and ISCX2012 datasets, HASTIDS demonstrated superior performance with reduced false alarm rates and higher detection accuracy. The method sets a new standard by leveraging hierarchical feature extraction directly from raw input, making it effective for identifying complex, timedependent intrusions.

[4] Hussein, M. K., & Jaber, A. N. (2015) Hussein and Jaber proposed a security analysis framework for cloudbased networks using honeypot technology to combat DDoS attacks. Their system focused on using researchoriented honeypots for behavior analysis of potential attackers in virtualized environments. The study stressed the importance of proactive security mechanisms, particularly in cloud computing, where sensitive data is frequently at risk. The proposed model offers a method to monitor, trap, and analyze attack vectors, aiding in the formulation of more robust defense strategies. This research underscores the growing need for intelligent intrusion tracking tools as cloud services become increasingly prevalent.

[5] Profiling SIEM Tools and Correlation Engines for Security Analytics This work analyzed and compared Security Information and Event Management (SIEM) tools, focusing on their ability to collect, correlate, and analyze security event data. The paper provided a comparative profile of widely used SIEM platforms and correlation engines, emphasizing their role in realtime threat detection and incident response. The authors discussed how effective SIEM systems enhance organizational security by providing centralized visibility and automated analytics. This review supports the selection and deployment of SIEM tools that align with specific enterprise security requirements and demonstrates their increasing importance in modern cybersecurity infrastructures.

[6] Suryanarayanan, V., & Hubballiand, N. (2014) In their comprehensive survey, Suryanarayanan and Hubballiand examined various techniques for minimizing false alarms in signaturebased intrusion detection systems. The authors classified and evaluated methods such as alert correlation, pattern clustering, and neural networkbased filtering. They highlighted the persistent challenge of IDS developers aiming to enhance detection reliability while maintaining system efficiency

[7] Trusting Cloud Computing for Personal Files (2014) This study addressed key security concerns in cloud computing, particularly related to the storage and management of personal and sensitive information. It discussed vulnerabilities in current cloud storage systems and proposed strategies to improve data confidentiality and integrity. The paper emphasized the societal implications of cloud security, including the potential for largescale disruptions in urban digital infrastructure. The authors highlighted realworld applications such as IBM’s Smarter Cities and Cisco’s Busan initiative, demonstrating the potential of secure cloud solutions to support urban mobility, energy management, and public services. This research forms a crucial foundation for trustbuilding in widespread cloud adoption.

III. PROPOSED SYSTEM

In this paper author is describing concept to detect threats using AISIEM (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) and this technique works based on events profiling such as attack signatures. Author evaluating propose work performance with conventional algorithms such as SVM, Decision Tree, Random

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 3, pp 20-24, March 2026
ISSN (online): 30491967
DOI: https://doi.org/10.47001/JAIET/2026.303004
Available Online at https://www.jaiet.com

Forest, KNN and Naïve Bayes. Here I am implementing CNN and LSTM algorithms.

Propose algorithms consists of following module:

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

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

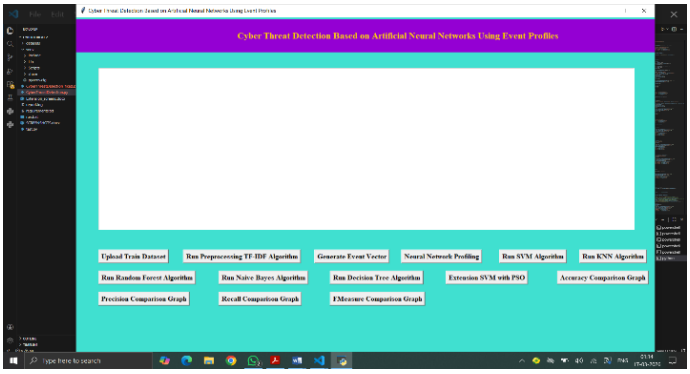
3) Event Profiling Stage: Processed data will be splitted into train and test model based on profiling events.

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 F Measure. Algorithm will learn perfectly will yield better accuracy result and that model will be selected to deploy on real system for attack detection.

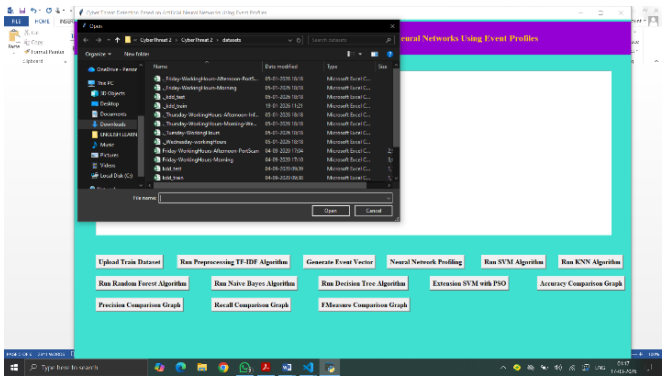
Datasets which we are using for testing are of huge size and while building model it's going to out of memory error but kdd_train.csv dataset working perfectly but to run all algorithms it will take 5 to 10 minutes. You can test remaining datasets also by reducing its size or running it on high configuration system.

IV. RESULTS

To run project double click on 'run.bat' file to get below screen:



In above screen click on 'Upload Train Dataset' button and upload dataset

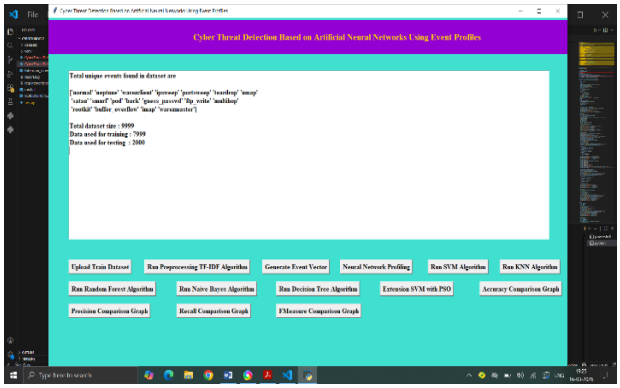


In above screen uploading 'kdd_train.csv' dataset and after upload will get below screen.

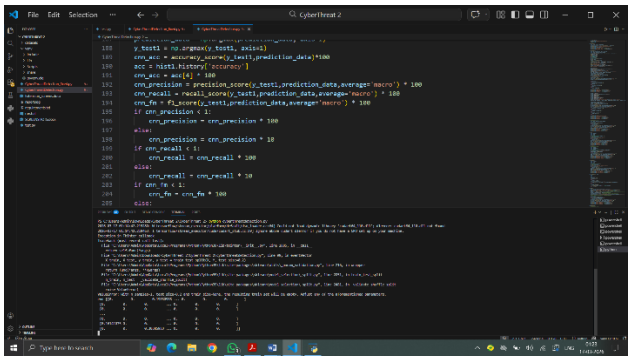
In above screen we can see dataset contains 9999 records and now click on 'Run Preprocessing TFIDF Algorithm' button to convert raw dataset into TFIDF values

In above screen TFIDF processing completed and now click on 'Generate Event Vector' button to create vector from TFIDF with different events

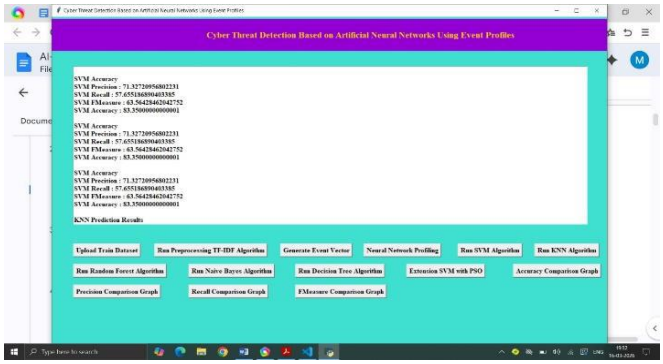
Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 3, pp 20-24, March 2026
ISSN (online): 30491967
DOI: https://doi.org/10.47001/JAIET/2026.303004
Available Online at https://www.jaiet.com



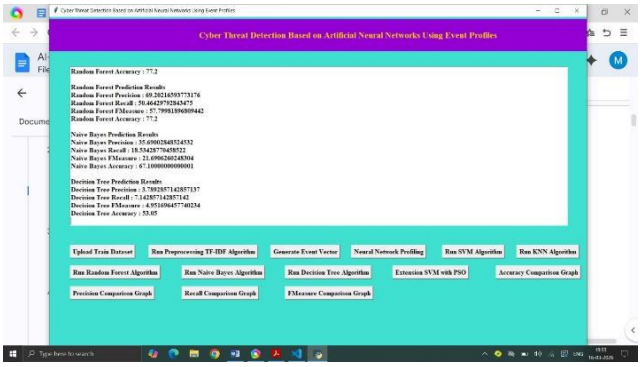
In above screen we can see total different unique events names and in below we can see dataset total size and application using 80% dataset (7999 records) for training and using 20% dataset (2000 records) for testing. Now dataset train and test events model ready and now click on 'Neural Network Profiling' button to create LSTM and CNN model



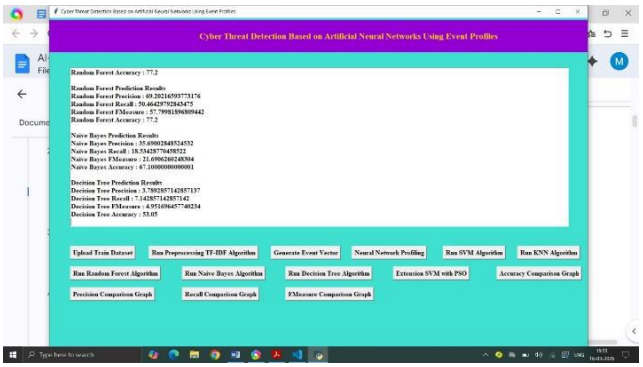
In above screen LSTM model is generated and its epoch running also started and its starting accuracy is 0.94. Running for entire dataset may take time so wait till LSTM and CNN training process completed. Here dataset contains 7999 records and LSTM will iterate all records to filter and build model. In above selected text we can see LSTM complete all iterations and in below lines we can see CNN model also starts execution.



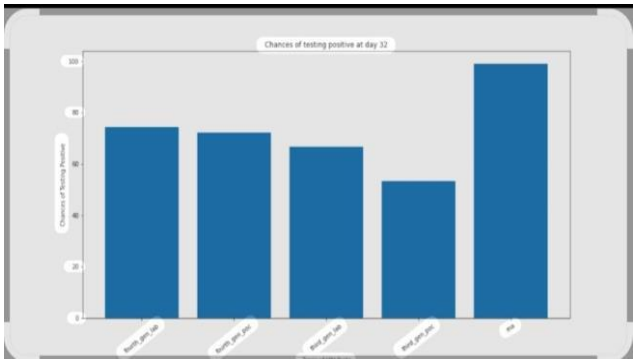
In above screen we can see SVM algorithm output values and now click on 'Run KNN Algorithm' to run KNN algorithm



In above screen we can see Random Forest algorithm output values and now click on 'Run Naïve Bayes Algorithm' to run Naïve Bayes algorithm.

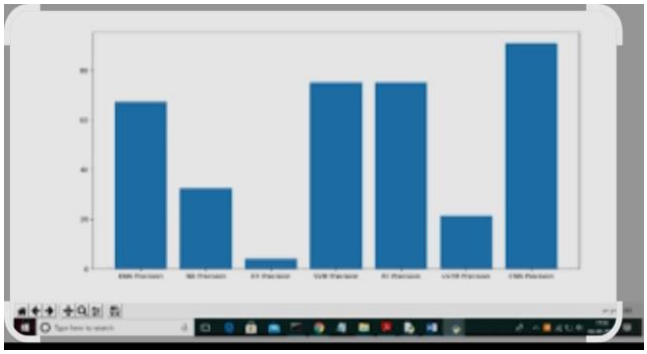


In above screen we can see Naïve Bayes algorithm output values and now click on 'Run Decision Tree Algorithm' to run Decision Tree Algorithm



In above graph x axis represents algorithm name and yaxis 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

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 3, pp 20-24, March 2026
ISSN (online): 30491967
DOI: https://doi.org/10.47001/JAIET/2026.303004
Available Online at https://www.jaiet.com



In above graph CNN is performing well and now click on 'Recall Comparison Graph'. From all comparison graph we can see LSTM and CNN performing well with accuracy, recall and precision.

V. CONCLUSION

The event profiling technique effectively condenses largescale security data for deep learning applications. By utilizing base points and concurrency patterns, the AISIEM system achieves high accuracy and a significant reduction in false positives compared to conventional ML and SVD methods. Future work will refine labeled datasets through continuous SOC analyst feedback and enhance early stage threat prediction models.

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, K. Han, "Enhanced Network Anomaly Detection Based on Deep Neural Networks," IEEE Access, vol. 6, pp. 4823148246, 2018.

[2] B. Zhang, G. Hu, Z. Zhou, Y. Zhang, P. Qiao, L. Chang, "Network Intrusion Detection Based on Directed Acyclic Graph and Belief Rule Base", ETRI Journal, vol. 39, no. 4, pp. 592604, Aug. 2017.

[3] W. Wang, Y. Sheng and J. Wang, "HASTIDS: Learning hierarchical spatial temporal features using deep neural networks to improve intrusion detection," IEEE Access, vol. 6, no. 99, pp. 17921806, 2018.

[4] M. K. Hussein, N. Bin Zainal and A. N. Jaber, "Data security analysis for DDoS defense of cloud based networks," 2015 IEEE Student Conference on Research and Development (SCOReD), Kuala Lumpur, 2015, pp. 305310.

[5] S. Sandeep Sekharan, K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," In Proc. Int. Conf. Wireless Com., Signal Proce. and Net.(WiSPNET), 2017, pp. 717 721.

[6] N.Hubballiand V.Suryanarayanan, ''False alarm minimization techniques in signaturebased intrusion detection systems: A survey,'' Comput. Commun., vol. 49, pp. 117, Aug. 2014.

[7] A.Naser, M. A. Majid, M. F. Zolkipli and S. Anwar, "Trusting cloud computing for personal files," 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, 2014, pp. 488489.

[8] Y. Shen, E. Mariconti, P. Vervier, and Gianluca Stringhini, "Tiresias: Predicting Security Events Through Deep Learning," In Proc. ACM CCS 18, Toronto, Canada, 2018, pp. 592605.

[9] Kyle Soska and Nicolas Christin, "Automatically detecting vulnerable websites before they turn malicious,", In Proc. USENIX Security Symposium., San Diego, CA, USA, 2014, pp.625640.

[10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, K. Li, "AI2: training a big data machine to defend," In Proc. IEEE Big Data Security HPSC IDS, New York, NY, USA, 2016, pp. 4954.

Citation of this Article:

Y Mohan Das, M Manjula, B R Harshitha, G Koushik Vadan, N Sai Sree, & M Hemalatha. (2026). AI-Based Cyber Threat Detection Using Event Profiling and Deep Neural Networks. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(3), 20-24. Article DOI: https://doi.org/10.47001/JAIET/2026.303004

***** End of the Article *****