ENHANCED DETECTION OF CYBER THREATS BY ARTIFICIAL INTELLIGENCE SYSTEMS USING NEURAL NETWORKS AND EVENT PROFILES

D.V.DIVAKARARAO Professor, Department of Computer Science Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.
K.PREETHI[2], M.RAMANA[3], M.YESHWANTH KUMAR[4] Students, Department of Computer Science Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.
dusi@raghuenggcollege.in, 19981a0566@raghuenggcollege.in, 19981a0591@raghuenggcollege.in, 19981a0587@raghuenggcollege.in

ABSTRACT

A cyber threat is an imminent risk of attack or malicious action directed towards digital information, assets, or infrastructure, with the objective of causing damage, stealing sensitive data, or disrupting regular operations. Ensuring precise detection of cyber threats poses a significant challenge in the realm of cybersecurity. This paper proposes the use of SVM with Particle Swarm Optimization algorithm to enhance the precision of cyber threat detection. The method entails converting numerous collected security incidents into separate profiles for each event and using a detection method based on deep learning to enhance the identification of cybersecurity risks. The significance of each word is calculated using the TF-IDF method, which helps identify the most critical words in the dataset. The key objective of the system is to differentiate between genuine and false alerts, which is crucial for achieving effective cyber threat detection. By analyzing data it collects and considering the frequency of occurrence, the system is capable of learning normal and malicious patterns, ultimately minimizing the number of false positive alerts in cybersecurity. The proposed data model demonstrates strong performance, as evidenced by the results of experiments conducted on datasets of varying sizes.

KEY TERMS: Particle swarm optimization, Support Vector Machine, CNN, LSTM, neural networks.

I. INTRODUCTION

As the internet continues to integrate into people's social and professional lives, it has transformed the way people learn and work. However, this integration has also made us more susceptible to security threats. The need to identify sources of information and recognize various types of network attacks, many of which are novel and have not been encountered before, is a pressing issue that requires immediate attention. There exist two main systems for detecting cyber-threats and network intrusions. Detecting intrusions against intelligent network attacks remains a challenging task due to the high rate or frequency of false alerts and the vast amount of security data. Therefore, the objective of our current work is to develop an automated and effective cyber-threat detection framework utilizing Deep Learning (DL) techniques.

The proposed framework incorporates deep learning (DL) to identify normal and malicious patterns in collected data. This approach reduces false positive alerts and allows security analysts to respond more efficiently to cyber threats. The aim is to improve detection performance by removing incorrect, irrelevant, or insignificant features. Classification algorithms are utilized to predict the class of an object. The presence of a large amount of data in a dataset, some of which may be irrelevant or contain duplicate features, can increase the complexity of the classifiers and reduce their effectiveness. To address this issue, the PSO algorithm is used to select relevant features for classification. It ranks all attributes, selects the relevant features, and uses SVM to classify the data, with the primary objective of improving classification accuracy.

The suggested method proposes utilizing Particle Swarm Optimization (PSO) along with Support Vector Machines (SVM) to improve the precision of classification. PSO is utilized to rank the attributes, select relevant features, and then SVM is used to classify the data. Recent research on intrusion detection has focused on using deep learning technologies to automate the process, with performance evaluations conducted on established datasets such as NSL-KDD and CICIDS2017.A deep learning model can be constructed using the features in the provided dataset to detect potential threats

II. LITERATURE REVIEW

AI-based intrusion detection in cybersecurity has gained significant attention in recent times, and numerous AI and machine learning techniques have been proposed to improve the effectiveness of cyber threat detection. The capability of intrusion detection was improved by Naseer et al.[1] through the development and implementation of detection models utilizing various deep neural network structures such as Convolutional Neural Networks (CNNs), Autoencoders, and Recurrent Neural Networks (RNNs), have been trained specifically for this objective. These models were trained using the NSLKDD training dataset and assessed using the test datasets provided by NSLKDD. The DCNN and LSTM models achieved an accuracy of 85% and 89%, respectively, on the test dataset.

The hybrid intrusion detection system created by Vinayakumar [2] and colleagues is capable of analyzing both network and host-level activities to improve cybersecurity threat detection, the system implemented a distributed deep learning model that used a Deep Neural Network (DNN) for real-time processing and analysis of large-scale data. The system utilized a distributed deep learning model with a DNN (Deep Neural Network) for processing and analyzing large-scale data in real-time.

DeepLog , a deep neural network model proposed by Liao and Vemuri [3], the design of the system aims to employ LSTM to understand the log patterns of a system during regular execution, which includes both the log key patterns and their associated parameter value patterns. The study employs the TF-IDF vector in both the log key and parameter value anomaly detection models to detect abnormal log entries.

In industry, Network Intrusion Detection Systems (NIDS) usually utilize statistical measures or calculated thresholds on network traffic features such as packet length, inter-arrival time, and flow size to model them over a particular timeframe. However, these approaches may be susceptible to high rates of false positive and false negative alerts, causing security analysts to handle an excessive workload and potentially miss crucial security incidents.[4]

The study by Jonghoon Lee[5] is closely related to this paper. Lee proposed an AI-based approach to detect cyber threats using artificial neural networks. The approach they employ requires transforming a large number of security incidents into separate profiles for each event, and leveraging a detection technique based on deep learning to enhance the identification of cyber-security threats. The authors also developed an AI-SIEM (Security Information and Event Management) system that combines event profiling for data preprocessing and various artificial neural network methods

The field of deep learning has made notable progress in various long-standing tasks related to artificial intelligence, including but not limited to image processing, speech recognition, and natural language processing (NLP)[6].Furthermore, these achievements have been applied to a range of cybersecurity tasks, such as intrusion detection, classification of Android malware, traffic analysis, prediction of network traffic, detection of ransomware, categorization of encrypted text, identification of malicious URLs, detection of anomalies, and identification of malicious domain names[7].

An extensive review of the literature reveals that modern deep learning techniques are seldom employed for NIDS (network intrusion detection systems), and the standard benchmark datasets used for experimental evaluation are KDDCup 99 and NSL-KDD[8],[9],[10].On the NSL-KDD dataset, the intrusion detection system utilizing recurrent neural network (RNN) exhibited superior performance in detecting intrusion and identifying the type of intrusion, outperforming other traditional machine learning classifiers.

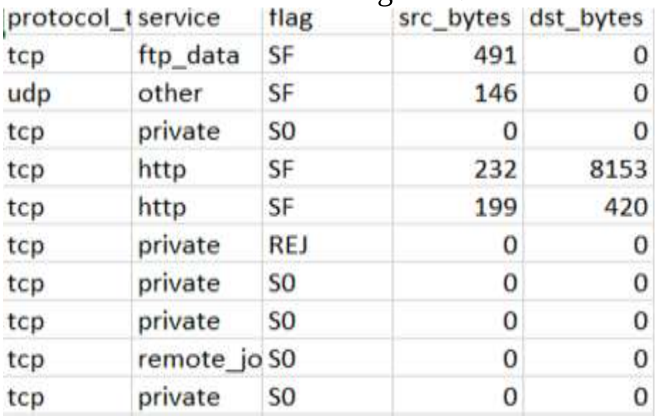
III. METHODOLOGY

In this section, we will discuss the event profiling technique that comprises data aggregation, information decomposition, and term frequency and inverse document frequency normalization. These steps collectively result in the creation of event profiles.In this scenario, 80% of the available data is allocated for training, while the remaining 20% is reserved for testing. The purpose of training is to develop a model, whereas testing is utilized to evaluate the model's accuracy.

A. DATASET EXPLANATION

Tavallaee and colleagues detected several instances of duplicated records in the initial KDDCUP99 dataset, which had an adverse effect on the training and evaluation performance of the models[11]. Therefore, the NSLKDD dataset was developed as a refined and updated version of the KDDCUP99 dataset to address these statistical problems. The NSL-KDD dataset encompasses four distinct attack categories, namely Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The NSL-KDD dataset serves as a standard dataset for intrusion detection and network security research, commonly used as a benchmark in the field.

We can observe the sample of NSL-KDD dataset in Figure 1.



protocol_t	service	flag	src_bytes	dst_bytes
tcp	ftp_data	SF	491	0
udp	other	SF	146	0
tcp	private	S0	0	0
tcp	http	SF	232	8153
tcp	http	SF	199	420
tcp	private	REJ	0	0
tcp	private	S0	0	0
tcp	private	S0	0	0
tcp	remote_jo	S0	0	0
tcp	private	S0	0	0

Fig 1 : NSL-KDD

B. DATA PREPROCESSING

Discovering a profiling technique to depict a pattern within a vast volume of data can be beneficial in condensing extensive information from event data, which can further be utilized as inputs for deep learning. The essential principle of our method is to capture the occurrence details of other events that were produced concurrently with the event of interest. . The significance of each word is calculated using the TF-IDF method, which helps identify the most critical words in the dataset.

C . PROPOSED ARCHITECTURAL MODEL

The objective of Particle Swarm Optimization (PSO) is to search for values of the variables that can minimize or maximize a given function, while ensuring that any constraints imposed on the problem are satisfied. In PSO, a cluster of particles (representing feasible solutions) traverse the solution space to locate the optimal solution. The movement of the particles relies on their present position, velocity, and the best solution discovered so far by the group. The algorithm modifies the position and velocity of each particle at every iteration, considering these aspects. The iteration proceeds until a stopping criterion is met, such as attaining a satisfactory solution or a maximum number of iterations. PSO is a form of artificial intelligence utilized to tackle complex numerical problems that are difficult to solve. Its underlying principle is based on the concept of social interaction among individuals to facilitate the problem-solving process.

Data pre-processing is a necessary set of procedures to prepare raw data for analysis, ensuring that the data is structured and free from any inconsistencies.. This involves handling missing values by either imputing or deleting them based on the extent and characteristics of the missing data. Additionally, duplicates are identified and removed to prevent skewing the results. Moreover, irrelevant data is excluded to reduce noise and prioritize essential features that are vital to the analysis

To create TF-IDF (Term Frequency-Inverse Document Frequency) and event vectors, a list of all distinct events in the dataset is compiled, and then, using TF-IDF, each word is evaluated to identify the most significant ones.

Figure 2 displays the workflow or architecture of the model.

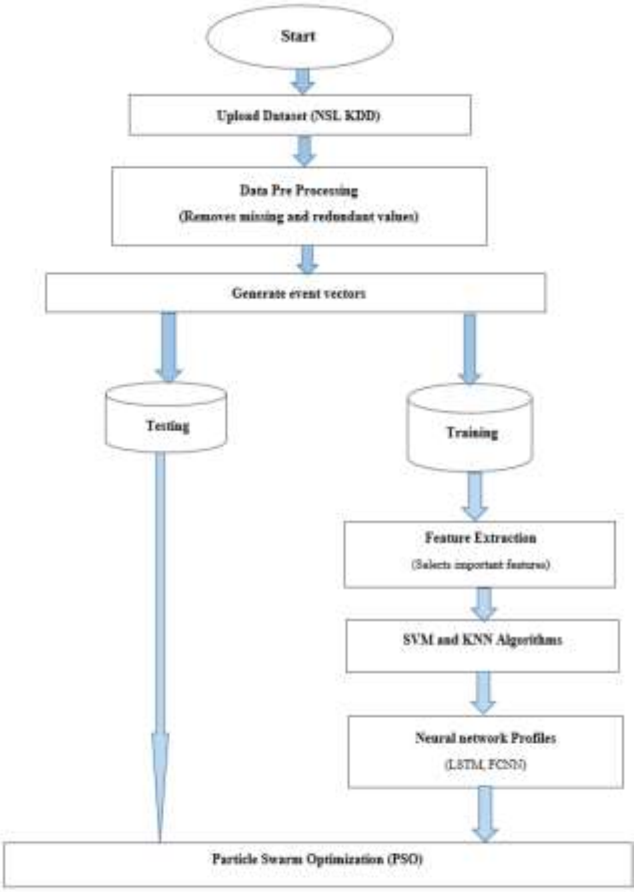


Fig 2 : Architecture/Framework

The process of training and testing involves utilizing 80% of the dataset for training purposes, while the remaining 20% is reserved for testing. During training, a model is created, whereas testing is carried out to evaluate the accuracy of the model.

C. ALGORITHMS

SVM:

Support Vector Machine (SVM) is a machine learning algorithm that operates under supervision and is commonly applied in classification and regression analysis tasks. SVM's primary objective is to identify a hyperplane, such as a line or a plane, that divides various data points into multiple classes while maximizing the margin between the hyperplane and the nearest data points of each class. This technique can be employed on data that is both linearly and non-linearly separable by converting it into a higher-dimensional feature space that makes it easier to distinguish.

RF: The model is characterized by three random components: random selection of training data, random feature subset selection when splitting nodes, and focusing on a subset of features when splitting each node in the decision tree. In a Random Forest, each decision tree is trained using a random sample of the input data. A Random Forest model is composed of numerous decision trees, and its predictions are based on the average of what the individual trees predict. This is the reason why it is referred to as a "forest".

K-NN: To identify the nearest neighbours, KNN calculates the distance between the new data point and all the data points in the training set. It then selects the k data points with the smallest distances and uses them to predict the label or value of the new data point**.**

Naive Bayes: Naive Bayes is a machine learning algorithm used for classification tasks. It predicts the category or class of a new data point based on the probabilities of the features or attributes in the data belonging to a specific class. The algorithm is referred to as "naive" because it assumes that the features are independent of each other given the class label.

PSO:

The algorithm involves a group of particles, each of which represents a potential solution, moving through the search space to find the optimal solution. Each particle has its own position and velocity, which are adjusted based on its own experience and the experience of its neighbouring particles. The objective function, which needs to be optimized, is used to evaluate the particles during the optimization process. The particles update their position and velocity by following the best-performing particle in their neighbourhood and their own previous best position. This process continues until a stopping criterion, such as a maximum number of iterations or reaching a satisfactory level of performance, is met.

IV. METRICS FOR EVALUTION

To evaluate the efficacy of our models, we utilize the Area Under the Curve (ROC-AUC) metric, which assesses the performance of score, accuracy, and receiver characteristics of operation. FPR, which stands for False Positive Rate, and TPR, which stands for True Positive Rate, are two metrics used to assess the performance of a model. The F1-score is a measure of accuracy, precision, and recall, which is also used in model evaluation. Therefore, we consider FPR, TPR, accuracy, precision, recall, and F1-score as key metrics in evaluating the performance of a model.

Accuracy is a fundamental metric for assessing the performance of machine learning models, and it is calculated as the ratio of correct predictions to the total number of observations, that is, the formula to calculate accuracy is: Accuracy = (True Positives + True Negatives)/(True Positives + False Positives + True Negatives + False Negatives)Recall is a measure of how well the model can identify positive observations, and it is calculated as Recall = True Positives / (True Positives + False Negatives). Precision, on the other hand, is used to assess the correctness of positive predictions and is defined as,the formula to calculate Precision is: Precision = True Positives / (True Positives + False Positives).

V. RESULTS AND ANALYSIS

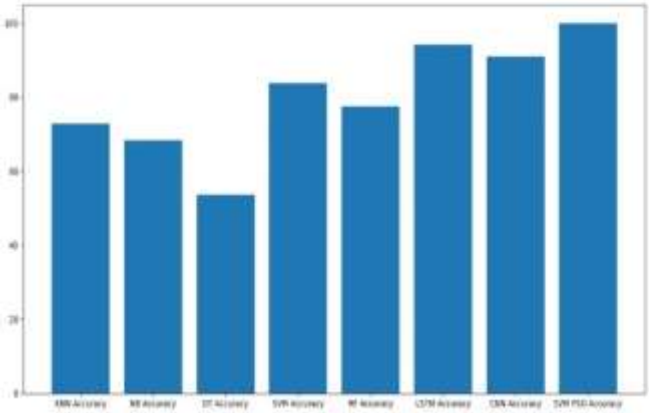


Fig 3: Accuracy comparison graph

Figure 2 displays the accuracy of different algorithms**.** The present study employs an AI-SIEM system that combines LSTM and CNN models, trained using the NSL-KDD dataset, to detect cyber threats.

We utilize the ROC-AUC metric to evaluate the performance of our models in terms of their operational area characteristics, such as score, accuracy, and receiver properties. PSO SVM demonstrates superior performance compared to CNN and LSTM models, achieving a remarkable accuracy of 99%

The F-measure (F1 score) is a widely used metric in binary classification and information retrieval tasks. It assesses how well a model balances both precision and recall, and is computed as the harmonic mean of these two metrics. The resulting F1 score ranges from 0 to 1, where a value of 1 indicates optimal precision and recall**.** PSO SVM outperforms CNN and LSTM models in terms of F-measure, achieving an impressive score of 99%.We can observe that PSO-SVM has highest FMeasure from Figure 4.

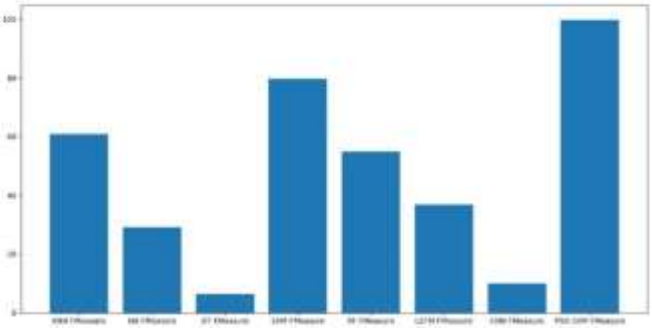


Fig 4: FMeasure comparison graph

Recall, also known as true positive rate or sensitivity, is a binary classification metric that evaluates how well a model can identify positive instances out of all actual positives. The resulting value ranges from 0 to 1, where a score of 1 denotes optimal recall. Figure 5 depicts the Recall comparison of various algorithms.

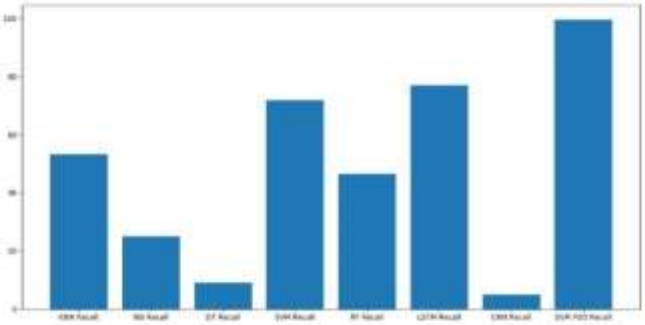


Fig 5: Recall comparison graph

SVM PSO exhibits superior recall performance compared to CNN and LSTM models, achieving the highest recall score of 99%. Therefore, when it comes to detecting cyber threats, PSO SVM is preferred over other algorithms. Its superior performance enables better detection of threats and differentiation between false and true alarms, ultimately leading to a more reliable and effective cybersecurity system.

V. CONCLUSION AND FUTURE SCOPE

In summary, the paper proposes the use of the PSO algorithm with deep learning to improve classification accuracy by accurately selecting and eliminating features through feature sub-selection. The PSO algorithm helps to identify the optimal feature subset for classification. The effectiveness of the proposed approach is evaluated using a benchmark dataset (NSLKDD) obtained from Kaggle. Based on the experimental results, it was shown that the proposed method surpasses other existing methods in terms of classification accuracy. This highlights the potential of the proposed method to classify data more accurately than other methods.

In light of the constantly evolving problem of cyber-attacks, our future efforts will be geared towards bolstering early threat detection by leveraging various deep learning methods to uncover persistent patterns in historical data. Additionally, to enhance the precision of labeled datasets for supervised learning and establish high-quality learning datasets, several SOC analysts will invest several months in carefully labeling individual raw security events.

VI. REFERENCES

S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal,and K. Han, ``Enhanced network anomaly detection based on deep neuralnetworks," IEEE Access, vol. 6, pp. 48231_48246, 2018.

R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, and S. Venkatraman, ``Robust intelligent malware detection using deep learning," IEEE Access, vol. 7, pp. 46717_46738, 2019.

Y. Liao and V. Vemuri, ``Use of K-nearest neighbor classi_er for intrusion detection," Comput. Secur., vol. 21, no. 5, pp. 439_448, Oct. 2002.

A. Azab, M. Alazab, and M. Aiash, ‘‘Machine learning based botnet identification traffic,’’ in Proc. 15th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (Trustcom), Tianjin, China, Aug. 2016, pp. 1788–1794

Jonghoon Lee “Cyber threat detection based on artificial neural networks and event profiles” in IEEE oct 2019.

Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", Nature, vol. 521, no. 7553, pp. 436, 2015.

Y. Xin et al., "Machine learning and deep learning methods for cybersecurity", IEEE Access, vol. 6, pp. 35365-35381, 2018.

R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection", South Afr. Comput. J., vol. 56, no. 1, pp. 136-154, 2015.

C. yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks", IEEE Access, vol. 5, pp. 21954-21961, 2017.

A. Javaid, Q. Niyaz, W. Sun and M. Alam, "A deep learning approach for network intrusion detection system", Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS), pp. 21-26, 2016.

M. Tavallaee, E. Bagheri, W. Lu, and 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. 1_6.