A NEW CYBER THREAT DETECTION USING ARTIFICIAL NEUARAL NETWORKS (ANN) BASED ON EVENT PROFILES

V.KUMAR REDDY[1],V P SHAIK GOUSE[1],T. KAVYANJALI[1],T.SAILAJA[1], G.V. GOPAL KRISHNA REDDY[2]

B-Tech Student, Dept.of CSE,UNIVESAL COLLEGE OF ENGINEERING AND TECHNOLOGY,Andhra pradhesh, India [1]
Assist Professor, Dept.of CSE,UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY,Andhra pradhesh, India[2]
kumarvennapusa2309@gmail.com , gvgkreddy2101@gmail.com

ABSTRACT

One of the major challenges in cybersecurity 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. this work, we developed an AI-SIEM 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, k-NN, 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 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:Challenges,Combination,Discriminating,Intrusion,Detection,Conventional,Benchmark.

1. INTRODUCTION:

With the rapid growth of the internet, cloud computing, and interconnected digital systems, cyber security has become a critical concern for individuals,organizations, and governments. Modern networks continuously face various cyber threats

such as malware attacks, denial-of-service (DoS), phishing, bruteforce attacks, and unauthorized access. These threats can lead to data breaches, financial losses, service disruptions, and damage to organizational reputation. Therefore, effective and intelligent cyber threat detection mechanisms are essential to protect digital infrastructures. Traditional cyber threat detection systems mainly rely on signature-based and rule-based techniques, which are commonly implemented in Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) platforms. While these systems are effective in detecting known attacks, they suffer from several limitations, including high false-positive rates, inability to detect unknown or zero-day attacks, and poor scalability when handling large volumes of security events. As cyber-attacks continuously evolve in complexity and frequency, conventional approaches are no longer sufficient. To overcome these challenges, Artificial Intelligence (AI) and Machine Learning (ML) techniques have been increasingly adopted in cyber security. Among them, Artificial Neural Networks (ANN) have gained significant attention due to their strong learning and pattern-recognition capabilities. ANN models are inspired by the human brain and consist of interconnected neurons that can learn complex nonlinear relationships from data. This makes them highly suitable for analyzing large-scale and high-dimensional security data generated by modern networks. Cyber threat detection based on ANN focuses on automatically learning normal and malicious behavior patterns from historical security data. By training on labeled or semi-labeled datasets, ANN models can effectively distinguish between normal network activities and potential cyber threats. Unlike traditional methods, ANN-based systems are capable detecting previously unseen attacks by identifying anomalies and subtle deviations in network behavior. This significantly enhances the detection accuracy while reducing the number of false alert. In recent research, ANN models such as Fully Connected Neural Networks (FCNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks have been widely used for cyber threat detection. These models can process security event profiles, network traffic features, and temporal patterns to improve threat classification performance. When integrated with SIEM platforms, ANN- based cyber threat detection systems can assist

security analysts by prioritizing true threats and enabling faster response to cyber incidents. In conclusion, cyber threat detection based on Artificial Neural Networks provides an intelligent, adaptive, and scalable solution to modern cyber security challenges. By leveraging ANN's learning capabilities, such systems can significantly improve detection accuracy, reduce false positives, and enhance overall network security in real-world environments.

2. LITARATURE REVIEW

With the rapid growth of digital communication and cloud-based services, cyber threats such as malware, phishing, denial-of-service attacks, unauthorized access, and data breaches have become major security concerns. Traditional signature-based intrusion detection systems often fail to identify unknown or zero-day attacks, creating the need for intelligent detection methods using Artificial Intelligence and Neural Networks.

A foundational study by J. Lee et al. proposed a deep learning-based cyber threat detection framework using event profiles and artificial neural networks. The system converts raw security logs and network events into structured event profiles and applies neural network models such as FCNN, CNN, and LSTM for threat classification. The study demonstrated improved detection accuracy and reduced false positives when compared with conventional machine learning methods.

Another significant work focused on AI-SIEM (Security Information and Event Management) systems, where large volumes of system logs, firewall alerts, and intrusion events are preprocessed into meaningful event vectors before being passed to ANN models. This approach helps security analysts distinguish between true positive and false positive alerts, thereby enabling faster response to attacks.

A related study on IoT network threat analysis using ANN-based IDS employed multilayer perceptrons to classify normal and malicious packet traffic. The system achieved high accuracy in detecting DDoS and DoS attacks, highlighting the effectiveness of neural networks in real-time intrusion detection.

Further research on deep learning approaches for intrusion detection introduced autoencoder-enhanced ANN architectures, which compress and learn hidden representations of large-scale security data. These models significantly improved detection precision for complex cyberattacks and dynamic network behaviors.

Another important contribution is the use of CNN-based intrusion detection for IoT environments, where network traffic is transformed into feature maps for convolutional learning. This method achieved better true positive rates and lower false alarm rates compared to LSTM-based baselines.

3. EXISITING METHOD:

With the rapid growth of the internet, cloud computing, and interconnected digital systems, cyber security has become a critical concern for individuals,organizations, and governments. Modern networks continuously face various cyber threats such as malware attacks, denial-of-service (DoS), phishing, bruteforce attacks, and unauthorized access. These threats can lead to data breaches, financial losses, service disruptions, and damage to organizational reputation. Therefore, effective and intelligent cyber threat detection mechanisms are essential to protect digital infrastructures.Traditional cyber threat detection systems mainly rely on signature- based and rule-based techniques, which are commonly implemented in Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) platforms.While these systems are effective in detecting known attacks, they suffer from several limitations, including high false-positive rates, inability to detect unknown or zero-day attacks, and poor scalability when handling large volumes of security events. As cyber-attacks continuously evolve in complexity and frequency, conventional approaches are no longer sufficient.

3.1 DIS-ADVANTAGES:

1. While these systems are effective in detecting known attacks, they suffer from several limitations, including high false-positive rates, inability to detect unknown or zero-day attacks, and poor scalability when handling large volumes of security events.
2. As cyber-attacks continuously evolve in complexity and frequency, conventional approaches are no longer sufficient.

4.PROPOSED METHOD

The proposed AI-SIEM framework, event profiles represent the behavioral characteristics of network and system activities, enabling accurate detection of normal and malicious events. Each event profile is generated by extracting key features from security logs, such as source and destination IP addresses, ports, protocols, packet sizes, connection duration, and specific flags indicative of anomalous behavior. Features are normalized and weighted according to their significance, and a profile is represented as a multidimensional vector capturing both the quantitative and qualitative aspects of the event. For example, a typical event profile for a Denial-of-Service (DoS) attack may include high-frequency connections, large packet volumes, repeated SYN requests, and unusual traffic patterns. Similarly, a Probe attack profile may emphasize multiple port scans, unusual IP ranges, and low-volume connections spread across the network. These event profiles are then compared using cosine similarity or other distance metrics against known profiles in the database to detect anomalies. The use of such structured profiles allows the ANN and hybrid deep learning models to efficiently learn patterns, discriminate between normal and malicious activity, and minimize false positives, ensuring robust real-time intrusion detection.

4.1 ADVANTAGES:

1. These event profiles are then compared using cosine similarity or other distance metrics against known profiles in the database to detect anomalies.

2. The use of such structured profiles allows the ANN and hybrid deep learning models to efficiently learn patterns, discriminate between normal and malicious activity, and minimize false positives, ensuring robust real-time intrusion detection.

5.SYSTEM ARCHITECTURE

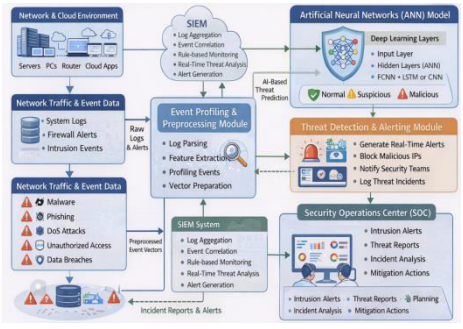

FIG 2.0: SYSTEM ARCHITECTURE

6. RELATED WORK:

6.1 DEEP LEARNING TECHNIQUES

An FCNN typically consists of an input layer, one or more hidden layers, and an output layer, enabling the model to learn

complex nonlinear mappings between input features and output classes through weighted connections and activation functions such as ReLU, sigmoid, or softmax. In cybersecurity and SIEM-based threat detection, FCNNs are widely used for classification tasks, where preprocessed and feature-engineered security event data—such as network traffic statistics, system call frequencies, and user activity metrics—are fed into the network to distinguish between normal and malicious

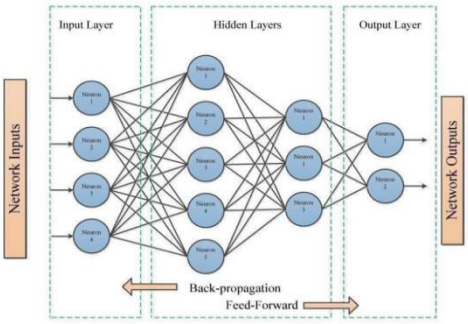

FIG 2.1:FCNN STRUCTURE

6.2 LONG SHORT -TERM MEMORY (LSTM)

This architectural advantage makes LSTMs particularly well suited for cybersecurity applications, where attack behaviors often unfold as sequences of events rather than isolated incidents. In SIEM-based threat detection, LSTMs are widely used to model temporal patterns in security logs, network traffic flows, user activities, and system events, allowing the detection of slow, stealthy, and multi-stage attacks such as advanced persistent threats and insider attacks. By learning normal temporal behavior, LSTM models can identify subtle deviations that indicate malicious activity, even when individual events appear benign in isolation.

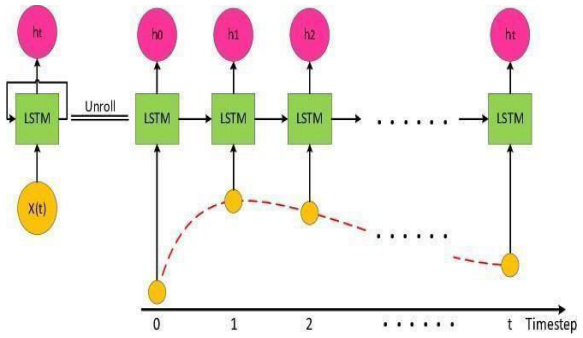

FIG:LSTM ARCHITECTURE

7. RESULTS:

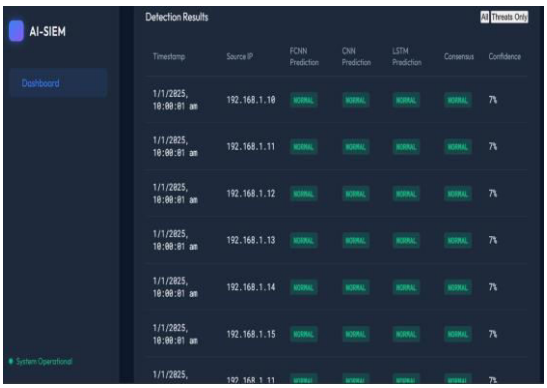

FIG 2.2: Thread Detection Results

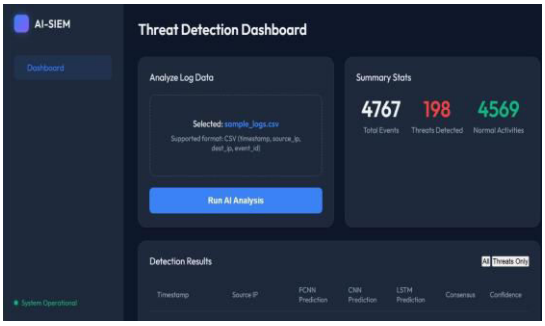

FIG2.3 : Thread Detection Dash Board

7. CONCLUSION:

This project presents a comprehensive framework for real-time cyber threat detection and response, integrating advanced AI and ANN-based techniques within an AI-driven Security Information and Event Management (AI-SIEM) system. The work began with extensive data collection and preprocessing, utilizing publicly available datasets like NSL-KDD and CICIDS-2017, as well as real-world datasets (ESX-1 and ESX-2), ensuring high-quality, normalized input data for analysis. Key features were extracted and processed through an event profiling and correlation pipeline, enabling the system to detect complex and subtle attack patterns. The framework incorporated an Artificial Neural Network (ANN) to enhance threat classification accuracy, minimize false positives, and identify both known and unknown attacks. Additionally, real-time threat visualization dashboards were developed to provide actionable insights for security analysts, enabling timely decision- making. Comparative analyses with conventional machine learning models and SVD-based dimensionality reduction approaches confirmed the superior performance of the proposed system across multiple metrics, including accuracy, True Positive Rate (TPR), False Positive Rate (FPR), and ROC-AUC. Overall, the work demonstrates a robust, scalable, and effective approach to modern cybersecurity threat detection and management.Future scope is the integration of hybrid deep learning models into the AI-SIEM framework significantly enhances the system's capability to detect, classify, and respond to cyber threats.Consequently, this capability ensures that the AI-SIEM system remains proactive, resilient, and capable of providing timely alerts for emerging cyber risks.

8. REFFRENCES

[1] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," IEEE Access, vol. 7, pp. 165607–165626, 2019, doi: 10.1109/ACCESS.2019.2953095.

[2] E. Hodo, X. Bellekens, A. Hamilton, P. L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion

Detection System," arXiv preprint arXiv:1704.02286, 2017.

[3] S. Hidalgo-Espinoza, K. Chamorro-Cupueran, and O. Chang-Tortolero, "Intrusion Detection in Computer Systems by Using Artificial Neural Networks with Deep Learning Approaches," arXiv preprint arXiv:2012.08559, 2020.

[4] A. Tuor, R. Baerwolf, N. Knowles, B. Hutchinson, N. Nichols, and R. Jasper, "Recurrent Neural Network Language Models for Open Vocabulary Event-Level Cyber Anomaly Detection," arXiv preprint arXiv:1712.00557, 2017.

[5] S. Parhizkari, M. B. Menhaj, and A. Sajedin, "A Cognitive Based Intrusion Detection System," arXiv preprint arXiv:2005.09436, 2020.

[6] "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," Scientific Digest: Journal of Applied Engineering, vol. 13, no. 6, pp. 128–134, 2025.

[7] "Cyber Threat Detection in Cloud Based on Artificial Neural Network Using Event Profiles," International Journal of Engineering Research and Science & Technology, vol. 20, no. 3, pp. 97–107, 2024.

[8] "Cyber Threat Detection Based on Artificial Neural Networks," IJRASET, 2023.

FIRST AUTHORS:

V.KUMAR REDDY pursuing his B.Tech in Computer Science And Engineering in Universal College Of Engineering And Technology.

V P SHAIK GOUSE pursuing his B.Tech in Computer Science And Engineering in Universal College Of Engineering And Technology.

T.KAVYANJALI pursuing her B.Tech in Computer Science And Engineering in Universal College Of Engineering And Technology.

T.SAILAJA pursuing her B.Tech in Computer Science And Engineering in Universal College Of Engineering And Technology.

Second Author:

G.V. GOPAL KRISHNA REDDY M.Tech received his M.Tech degree and B.Tech degree in computer science and engineering. He is currently working as an Assist Professor in , Universal College Of Engineering And Technology.