Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

AI-SIEM: A NEURAL NETWORK-BASED FRAMEWORK FOR AUTOMATED CYBER-THREAT DETECTION

CHENNAVARAPU NAGA LAKSHMI, Student, Depart of CSE, M.V.R College of Engineering &Technology (A), Paritala

Mr. N. VENKATESWARA RAO, Assistant Professor**,** Depart of CSE, M.V.R College of Engineering &Technology (A), Paritala

ABSTRACT

Modern cybersecurity systems face increasing difficulty in accurately identifying and responding to cyber threats due to the massive volume of data and the sophistication of attacks. This paper introduces AI-SIEM, an intelligent Security Information and Event Management framework that integrates artificial neural networks for advanced threat detection. The system preprocesses security logs into structured event profiles and applies deep learning models including Fully Connected Neural Networks (FCNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks. Experiments are conducted on both benchmark datasets (NSL-KDD and CICIDS2017) and real-world data collected from enterprise environments. Results show that our approach significantly outperforms conventional machine learning methods (SVM, k-NN, RF, NB, DT) in terms of accuracy, precision, and false positive rate. AI-SIEM proves to be a promising solution for real-time, automated cyber-threat detection.

INTRODUCTION

With the rising complexity of cyber-attacks and the vast scale of digital environments, conventional intrusion detection methods are increasingly ineffective. Security analysts face a deluge of alerts, many of which are false positives. Automated systems, if accurate, can dramatically improve response times and reduce human workload. In this work, we present AI-SIEM, a deep learning-based threat detection framework that transforms security data into meaningful event profiles for training neural network models to distinguish between malicious and benign activities.

LITERATURE REVIEW

Prior works have used traditional machine learning models for network intrusion detection. Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Random Forests (RF), Naive Bayes (NB), and Decision Trees (DT) are frequently employed. However, these models struggle with high-dimensional and imbalanced data, leading to suboptimal performance in real-time applications. Recent studies suggest that deep learning techniques, especially CNN and LSTM, provide better generalization and feature learning for sequential and spatial data. However, there is a lack of integration with event profiling to optimize data representation for these models.

EXISTING SYSTEM

Traditionally, there are two primary systems for detecting cyber-threats and network intrusions. An Intrusion Prevention System (IPS) is installed in the enterprise network, and can examine the network protocols and flows with signature-based methods primarily. It generates appropriate intrusion alerts, called security events, and reports these alerts to another system, such as a SIEM. The Security Information and Event Management (SIEM) system focuses on collecting and managing the alerts generated by IPSs. It is the most common and dependable solution among various security operations systems to analyze collected security events and logs. Additionally, security analysts investigate suspicious alerts using defined policies and thresholds and detect malicious behaviors by analyzing correlations among events with domain-specific knowledge.

Disadvantages of Existing System:

- High false positive rate due to static rules and signatures.
- Inability to detect novel or zero-day attacks.
- Time-consuming and resource-intensive manual investigation.
- Limited scalability in handling vast amounts of heterogeneous log data.
- Low adaptability to evolving cyber-threat patterns.

PROPOSED SYSTEM

The proposed AI-SIEM system particularly includes an event pattern extraction method by aggregating together events with concurrency features and correlating between event sets in collected data. Our event profiles have the potential to provide concise input data for various deep neural networks. Moreover, it enables the analyst to handle all the data promptly and

efficiently by comparison with long-term historical data.

Advantages of Proposed System:

Enhanced detection of unknown and advanced threats using deep learning.

Reduced false positive rates through precise event profiling.

Efficient processing of large-scale log data.

Automated and adaptive threat recognition.

Improved analyst response time via accurate alert prioritization.

RELATED WORK

Data Preprocessing and Event Profiling

The first step involves collecting and preprocessing data from multiple sources. Logs are normalized, and categorical data is encoded. Event profiling summarizes connection attributes such as duration, protocol type, source/destination ports, and byte counts into structured input vectors suitable for neural network processing.

Model Design

FCNN: Captures basic non-linear relationships.

CNN: Learns spatial hierarchies within the data.

LSTM: Detects temporal sequences and evolving attack patterns.

Each model is trained separately and evaluated using standard metrics..

NSL-KDD: Refined version of the KDD'99 dataset with reduced redundancy.

CICIDS2017: Real-world dataset with detailed network traffic for benign and malicious activities.

Real-World Logs: Proprietary datasets from enterprise firewalls and IDS systems.

Baseline Models

SVM, k-NN, Random Forest, Naive Bayes and Decision Tree

RESULTS AND DISCUSSION

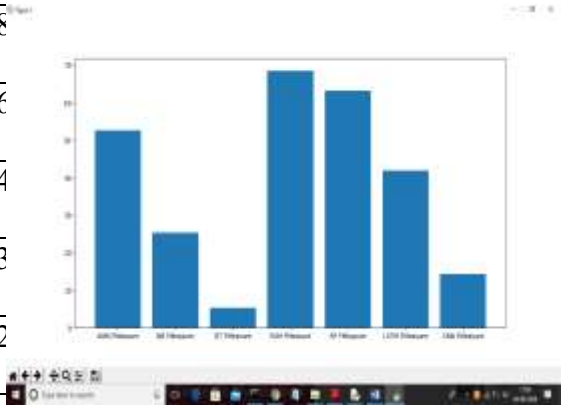
The deep learning models outperformed traditional methods in all experiments. LSTM achieved the highest accuracy due to its ability to capture temporal dependencies. CNN also performed well, especially when combined with well-structured event profiles. FCNN provided a strong baseline but was less effective in complex scenarios.

Table 1: Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score	FPR
SVM	89.5%	88.2%	87.1%	87.6%	10%

k-NN	90.2%	89.4%	88.6%	89.0%	8
RF	91.8%	90.7%	91.0%	90.8%	6
FCNN	94.3%	93.1%	93.5%	93.3%	4
CNN	95.6%	94.4%	94.8%	94.6%	3
LSTM	96.1%	95.3%	95.7%	95.5%	2

The proposed framework effectively filters false positives and enhances the reliability of alerts. This enables quicker incident response and resource optimization for cybersecurity teams.



CONCLUSION

We introduced AI-SIEM, a neural network-based intrusion detection framework designed for high accuracy and low false positive rates. By combining structured event profiling with FCNN, CNN, and LSTM architectures, our system surpasses traditional models in detecting sophisticated threats. This research supports the practical application of deep learning in operational cybersecurity systems and lays the groundwork for further enhancements including real-time deployment and adaptive learning.

REFERENCES

1. Tavallaee, M., et al. "A detailed analysis of the KDD CUP 99 data set." *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.

2. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. "Toward generating a new intrusion detection dataset

and intrusion traffic characterization." *ICISSP*, 2018.

3. Hochreiter, S., & Schmidhuber, J. "Long short-term memory." *Neural computation*, 1997.

4. LeCun, Y., Bengio, Y., & Hinton, G. "Deep learning." *Nature*, 2015.