Cyber Threat Detection Based On Artificial Neural Network

[1] A.RASAN KUMAR, [2] A. LAXMIPRASANNA, [3] T. JANESWARI, [4] A. SRIVANI, [5] M. AKHILA REDDY, [6] PREMA LATHA

[1] Assistant Professor, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5,6] B. Tech Students, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

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. For 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.

I.INTRODUCTION

In the modern digital era, organizations and individuals are increasingly exposed to cyber threats such as malware, phishing, denial-of-service (DoS) attacks, and advanced persistent threats (APTs). With the rise in connectivity through the Internet of Things (IoT), cloud computing, and remote work, traditional security systems such as signature-based detection and firewalls have proven inadequate in identifying novel or evolving attacks. To tackle these dynamic threats, Artificial Neural Networks (ANNs) have emerged as a powerful tool due to their ability to learn from patterns, adapt to new data, and generalize from noisy or incomplete information.

Artificial Neural Networks mimic the way human brains process information. They can model complex, non-linear relationships, which makes them suitable for identifying suspicious behaviors or traffic patterns that are indicative of cyber attacks. This paper explores how ANNs can be trained using historical attack data to detect, classify, and respond to a wide range of cyber threats in real time, enhancing the proactiveness and intelligence of cybersecurity systems.

II.LITERATURE SURVEY

[1] The research conducted by A. SHABTAI, E. MENAHEM, AND Y. ELOVICI introduces a groundbreaking method called F-Sign, designed to automatically extract unique signatures from malware files. This method targets high-speed network traffic filtering devices that rely on deep-packet inspection. The analysis of malicious executables employs two approaches: disassembly with IDA-Pro and the application of a dedicated state machine to identify the executable's set of functions. The process of signature extraction in F-Sign involves comparing the executable's functions with those in a common function repository. By eliminating functions present in the repository from the list of potential signature candidates, F-Sign significantly reduces the risk of falsepositive detection errors. To further enhance the accuracy of detection, F-Sign introduces intelligent candidate selection using an entropy score to generate signatures. The effectiveness of F-Sign was thoroughly evaluated under various conditions. The results demonstrate that this proposed method is capable of automatically generating signatures that are both highly specific and sensitive to the presence of malware. The research not only highlights the potential of F-Sign in combating malware but also underscores its ability to minimize false-positive rates, making it a valuable tool in the field of cyber security. [2] The research paper authored by D. Kong, J. Gong, S. Zhu, P. Liu, and H. Xi introduces a pioneering approach named SAS (Semantics Aware Statistical) for the automatic generation of effective worm signatures in the presence of adversarial environments. While string extraction and matching techniques have been commonly employed for signature generation, dealing with the challenges posed by an adversarial setting remains a significant problem. In such environments, attackers possess the capability to manipulate byte distributions within attack payloads, allowing them to inject well-crafted noisy packets that contaminate the suspicious flow pool. To counteract these attacks, the SAS algorithm is proposed. When processing packets within

the suspicious flow pool, SAS utilizes data flow analysis techniques to remove non-critical bytes. Subsequently, a hidden Markov model (HMM) is applied to the refined data, enabling the generation of signatures based on state-transition graphs. Notably, this work represents the first endeavor to combine semantic analysis with statistical analysis to automatically generate worm signatures. Through extensive experiments, it was demonstrated that the proposed SAS technique exhibits accurate worm detection capabilities, utilizing concise signatures. Furthermore, the results indicate that SAS demonstrates enhanced resilience against changes in byte distribution and noise injection attacks when compared to existing approaches like Polygraph and Hamsa. This research contributes significantly to the field of worm detection by addressing the challenges posed by adversarial environments and offering a novel and robust approach for signature generation.

III.EXISTING SYSTEM

Existing cybersecurity solutions predominantly rely on signature-based and rule-based detection mechanisms, which compare incoming data with known patterns or heuristics. Tools like Snort, Suricata, and antivirus software use static rule databases that require constant updating. These methods are effective only against known threats and fail when encountering zero-day attacks, polymorphic malware, and encrypted payloads.

Deep learning have been used to analyze structured network logs. While these models perform well with pre-engineered features, they lack the ability to automatically extract hierarchical patterns and often struggle with large-scale or high-dimensional data. They are also less efficient in dynamic environments such as real-time monitoring of cloud servers or IoT ecosystems, where attack patterns constantly evolve.

Moreover, traditional systems often suffer from high false-positive rates, inflexible retraining, and manual feature engineering, making them unsuitable for real-world, real-time cyber defense.

IV.PROPOSED SYSTEM

The proposed system utilizes an Artificial Neural Network-based model for intelligent and real-time cyber threat detection. The architecture is designed with the following pipeline:

1. Data Collection: Collect raw network traffic, system logs, DNS queries, authentication logs, and other telemetry data.

2. Preprocessing: Clean the data, normalize features, and transform logs into numerical representations (using one-hot encoding, tokenization, etc.).
3. Feature Engineering: Automated using the ANN model, especially in deeper architectures (like CNN or LSTM) that can extract spatial and temporal patterns.
4. Model Training: A Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), or Recurrent Neural Network (RNN) is trained using labeled data from datasets like CICIDS2017 or custom enterprise logs.
5. Threat Classification: The trained ANN classifies traffic or events into multiple categories: benign, malware, DDoS, insider attack, ransomware, botnet, etc.

V. SYSTEM ARCHITECTURE

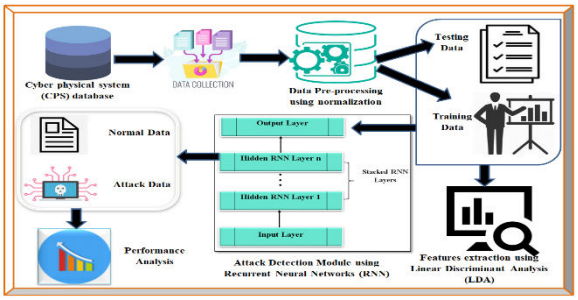

Fig 5.1 System Architecture

VI.IMPLEMENTATION

Fig 6.1 Main Page

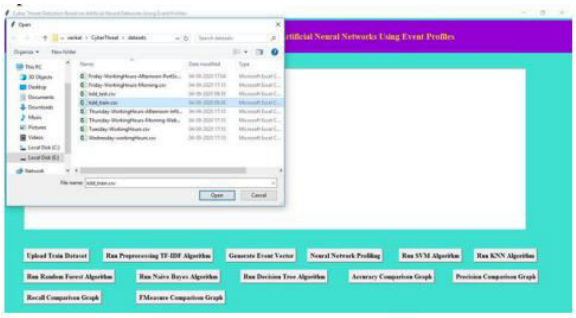

Fig 6.2 Upload file

Fig 6.3 Preprocess data

Fig 6.4 Run the Generate Event Vector Algorithm

Fig 6.5 Run Cnn And Lstm Algorithm

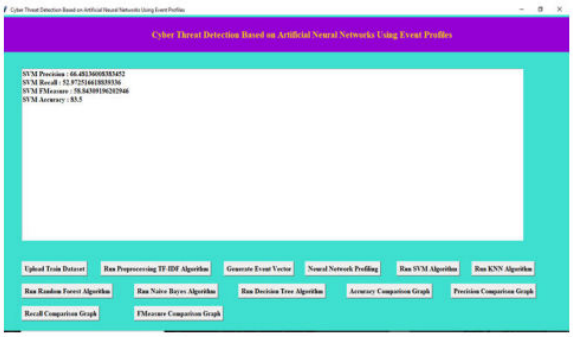

Fig 6.6 Run SVM Algorithm

Fig 6.7 Accuracy Comparison graph

VII.CONCLUSION

Artificial Neural Networks have revolutionized the field of cyber threat detection by offering adaptive, scalable, and intelligent solutions. Unlike traditional static methods, ANNs can model complex behaviors, detect anomalies, and generalize across varying environments. By leveraging deep learning capabilities, the system can significantly improve accuracy, speed, and proactivity in identifying and mitigating cyber threats. With appropriate training and real-time integration, ANN-based cybersecurity solutions represent a paradigm shift in modern digital defense. However, challenges like explainability, overfitting, and interpretability remain open areas of research.

VIII.FUTURE SCOPE

The integration of ANNs into cybersecurity is still evolving, and several areas offer rich potential for innovation:

- Federated Learning: To preserve data privacy while training across multiple decentralized clients (e.g., enterprises or IoT networks).
- Edge AI Integration: Real-time detection on edge devices for low-latency response in IoT and 5G environments.
- Adversarial Attack Defense: Making ANN models robust against data poisoning and adversarial evasion.
- XAI (Explainable AI): To provide human-understandable justifications for ANN decisions, critical for regulatory compliance.
- Hybrid Models: Combining ANN with unsupervised techniques like

autoencoders or GANs to detect unknown threats.

- Autonomous Threat Hunting Agents: AI-powered agents capable of autonomously investigating and responding to threats.
- Blockchain Integration: Using blockchain for secure, traceable threat intelligence sharing.
- Zero Trust Architecture: Enhancing ANN systems to support micro-segmentation and real-time behavioral profiling.
- Self-Healing Systems: Enabling systems to not only detect but recover from attacks autonomously.
- Application in National Cyber Defense: Deploying ANN-based systems to protect government infrastructure and defense networks.

IX.REFERENCES

1. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.
2. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
3. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference.
4. Kim, G., Lee, S., & Kim, S. (2020). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.
5. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. NDSS Symposium.
6. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. EAI International Conference on Bio-inspired Information and Communications Technologies.
7. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. Proceedings of the IEEE Symposium

on Computational Intelligence for Security and Defense Applications.

8. Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169–175.
9. Lashkari, A. H., Draper-Gil, G., Mamun, M. S. I., & Ghorbani, A. A. (2017). Characterization of Tor traffic using time-based features. ICISSP 2017.
10. Zhang, Y., & Paxson, V. (2021). Detecting and Analyzing Automated Cyber Attacks using Deep Learning Techniques. ACM Transactions on Privacy and Security, 24(4), Article 15.