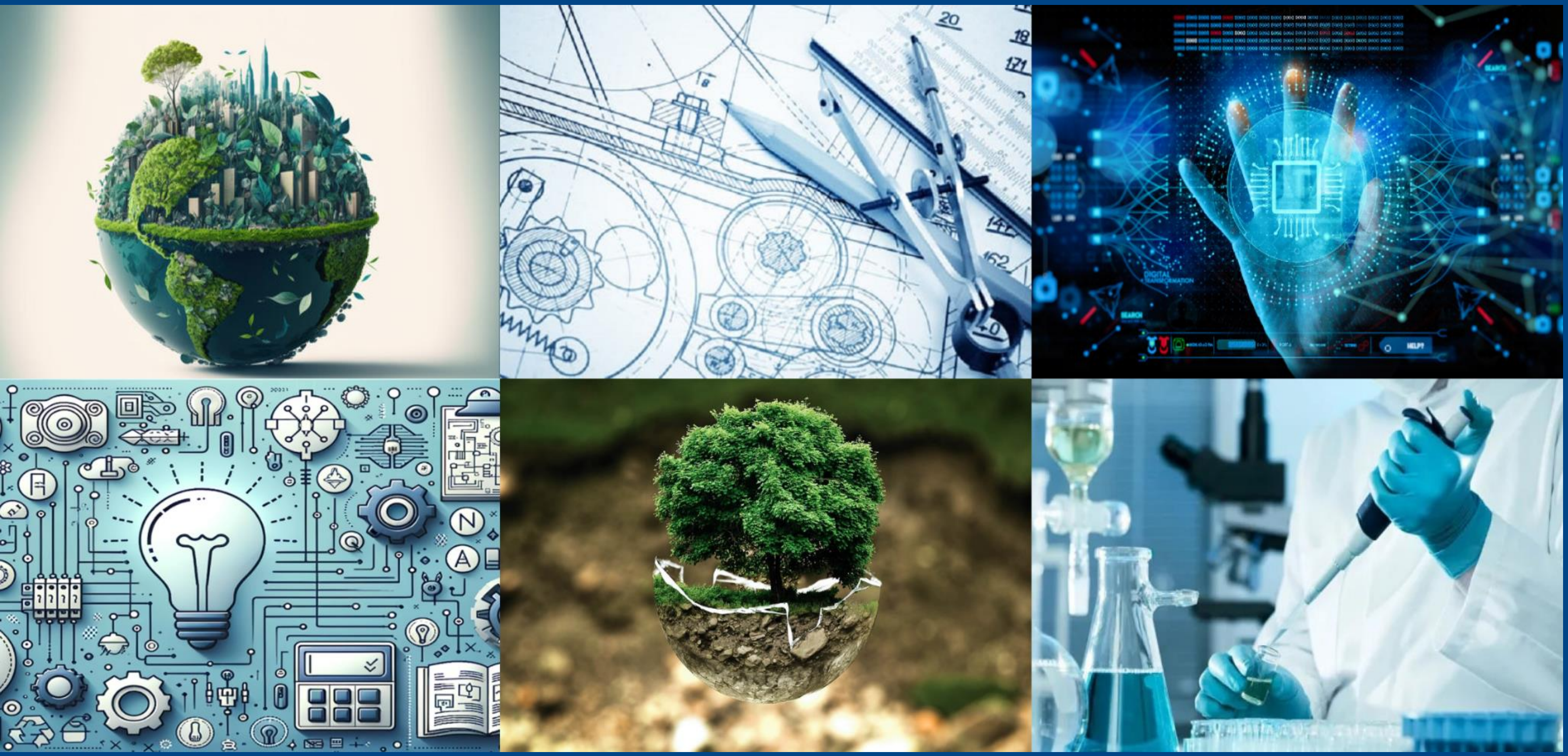
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Artificial Neural Networks for Detecting Cyber Threats using Event Profiles

Dr. D.J. Samatha Naidu, K. Venkata Ramya, P. Lakshmi Narasimha

Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

Assistant Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

PG Student, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, 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

With the emergence of artificial intelligence (AI) techniques, learning-based approaches for detecting cyber attacks, have become further improved, and they have achieved significant results in many studies. However, owing to constantly evolving cyber attacks, it is still highly challenging to protect IT systems against threats and malicious behaviors in networks. Because of various network intrusions and malicious activities, effective defenses and security considerations were given high priority for finding reliable solutions [1]–[4]. 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.

A learning-based method geared toward determining whether an attack occurred in a large amount of data can be useful to analysts who need to instantly analyze numerous events. According to [10], information security solutions generally fall into two categories: analyst-driven and machine learning-driven solutions. Analyst-driven solutions rely on rules determined by security experts called analysts. Meanwhile, machine learning-driven solutions used to detect rare or anomalous patterns can improve detection of new cyber threats [10]. Nevertheless, while learning-based approaches are useful in detecting cyber attacks in systems and networks, we observed that existing learning-based approaches have four main limitations.

II. SYSTEM ARCHITECTURE

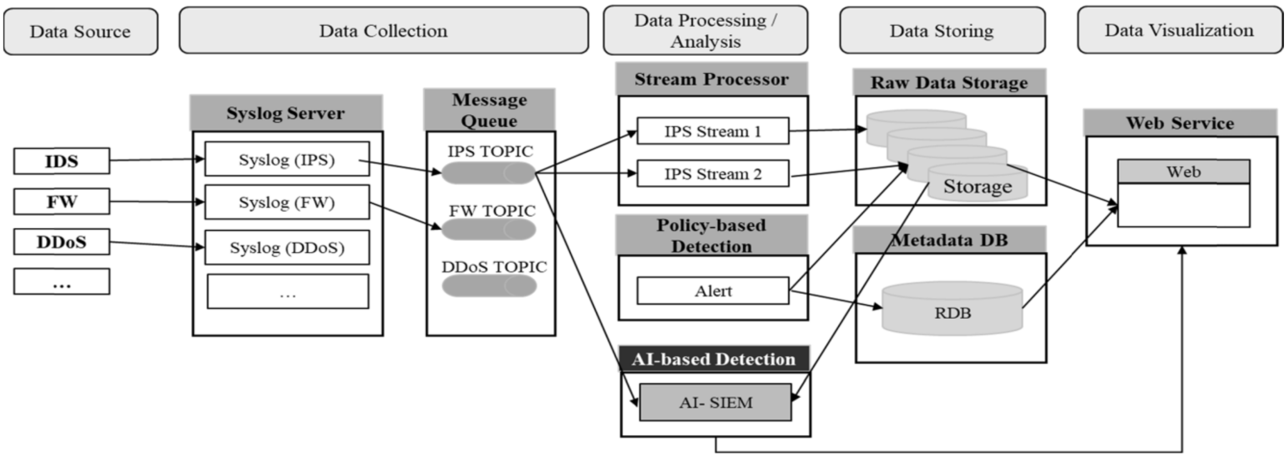


Figure 1: System Architecture.

III. LITERATURE REVIEW

Event profiles are representations of the behavior or activities of systems, users, or networks over time. These profiles are created by analyzing logs, system events, and user behavior to track patterns that may indicate malicious activity. ANNs can be trained on these profiles to identify patterns of normal and anomalous behavior, thus helping in detecting potential cyber threats. This review explores the research surrounding the use of ANNs for detecting cyber threats with an emphasis on the use of event profiles.

1. Artificial Neural Networks in Cyber Threat Detection

ANNs are computational models inspired by biological neural networks, and they have demonstrated significant success in various fields, including pattern recognition, classification, and anomaly detection. In the context of cybersecurity, ANNs are used to detect anomalies or threats by learning the patterns of network traffic, user behavior, or system events. The use of ANNs in cyber threat detection is driven by their ability to generalize patterns, adapt to new types of data, and provide robust performance in complex environments.

Several studies have demonstrated the capability of ANNs to detect malicious activities, including intrusion detection, malware detection, and phishing attacks. In general, ANNs can learn features from large and diverse datasets, which makes them ideal for detecting subtle or complex attack patterns that might be difficult to identify using conventional methods.

2. Event Profiles for Threat Detection

Event profiles represent the dynamic patterns of system, network, or user activity over time. These profiles are usually builtusing system logs, user actions, network traffic data, or event sequences. The idea is to capture normal and abnormal behavior by analyzing the temporal and spatial relationships between events.

- **User Event Profiles**: These profiles focus on the behavior patterns of users, tracking activities like login attempts, access to sensitive files, and unusual interactions with the system. Any deviation from these established behavior patterns might indicate a potential insider threat or account compromise.

Network Event Profiles: These profiles focus on monitoring network traffic and interactions. They can capture the normal flow of traffic, including IP addresses, protocols, data rates, and other characteristics. Sudden spikes, unusual

IV. METHODOLOGY OF PROPOSED SURVEY

This section outlines the methodology proposed for the survey of existing research on Artificial Neural Networks (ANNs) for detecting cyber threats using event profiles. The survey aims to analyze the various methods, models, and techniques used in the domain of cyber threat detection and provide a comprehensive overview of the current state-of-the-art research. The following steps outline the methodology for conducting this survey.

1. Literature Search and Data Collection

The first step in the proposed methodology is gathering relevant literature from various academic sources, journals, and conferences. This will include papers, articles, technical reports, and other scholarly publications related to the application of ANNs in detecting cyber threats using event profiles. The key sources for data collection will be:

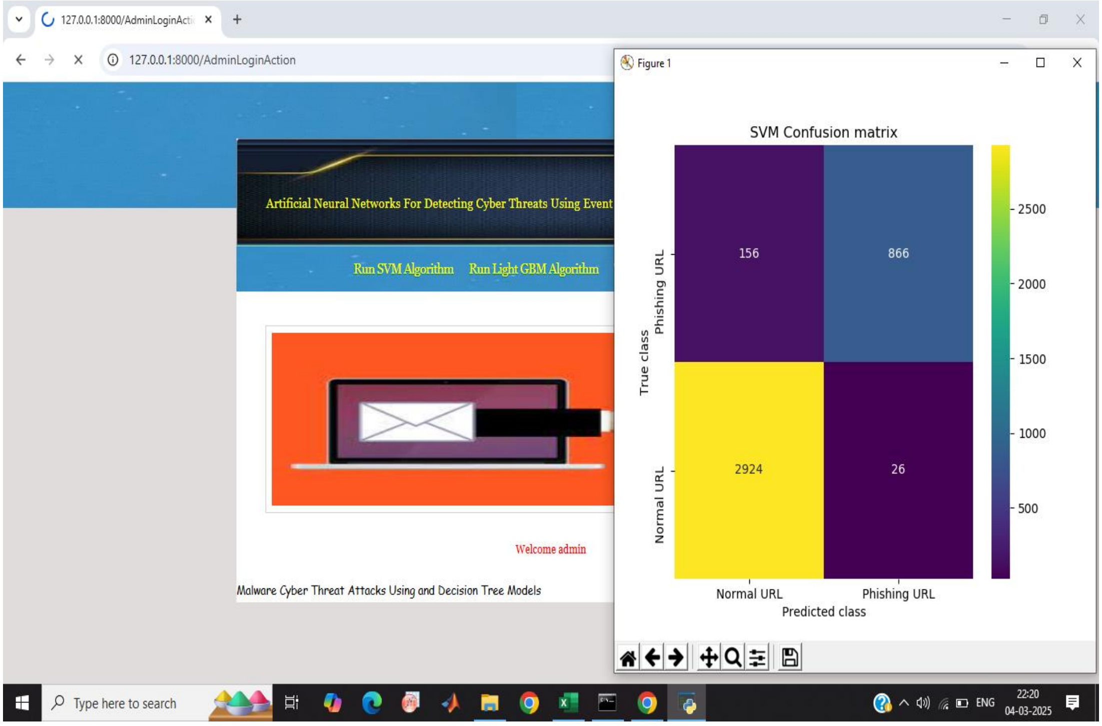
- **Digital Libraries and Databases**: IEEE Xplore, Google Scholar, SpringerLink, ScienceDirect, ACM Digital Library, and ResearchGate will be the primary platforms for retrieving peer-reviewed research papers.
- **Conference Proceedings**: Major cybersecurity and machine learning conferences such as IEEE S&P (Security and Privacy), ACM CCS (Computer and Communications Security), and NeurIPS (Conference on Neural Information Processing Systems) will be explored for relevant studies.
- **Books and Theses**: Relevant books and doctoral theses will also be analyzed to gather comprehensive insights into the methodologies used for cyber threat detection with ANNs and event profiles.

Search Keywords:

- "Artificial Neural Networks for Cyber Threat Detection"
- "Event Profiles in Cybersecurity"
- "Anomaly Detection in Cybersecurity"
- "Deep Learning for Intrusion Detection"
- "Neural Networks for Malware Detection"

V. RESULT AND DISCUSSION

It shows the tweet Datasets that are trained and tested results.



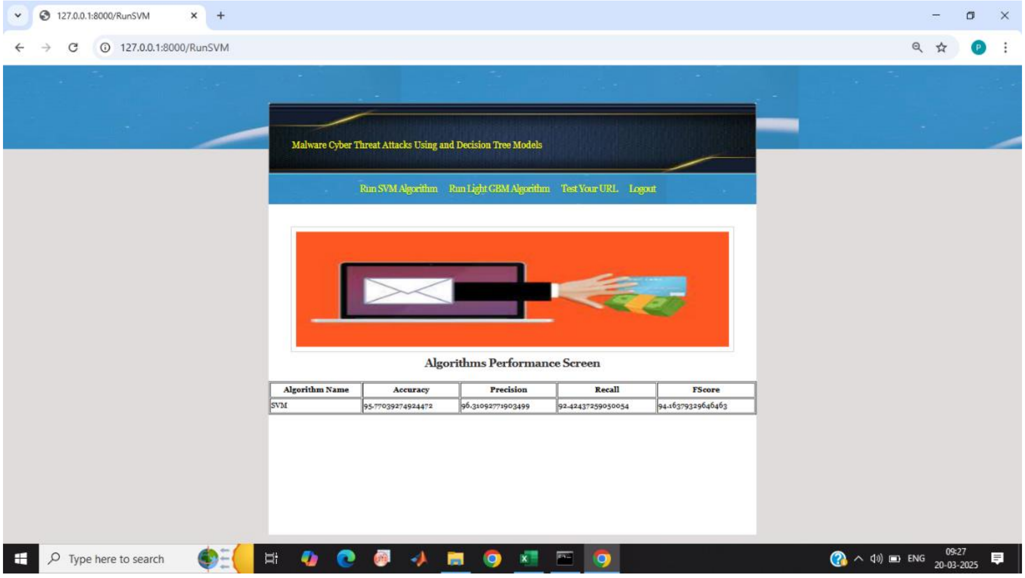
127.0.0.1:8000/AdminLoginAction

Artificial Neural Networks For Detecting Cyber Threats Using Event

Welcome admin

Malware Cyber Threat Attacks Using and Decision Tree Models

FIG:1 Run SVM Algorithm

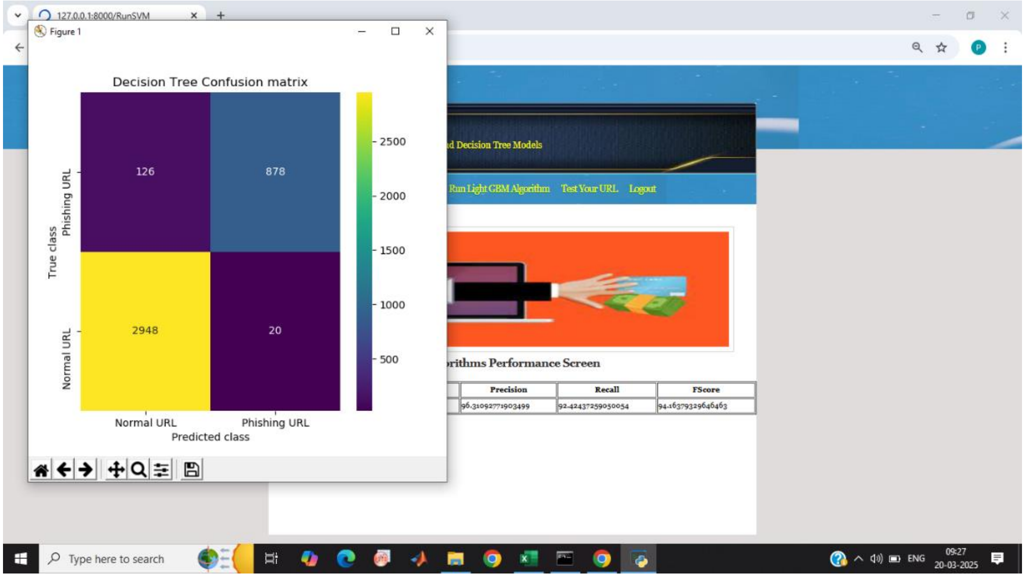


Algorithms Performance Screen

Algorithm Name	Accuracy	Precision	Recall	FScore
SVM	95.77039274924472	96.31092771903499	92.42437259050054	94.16379329646463

Fig. 2 Run SVM Algorithms Results

In the fig 2 It shows the Run SVM Algorithms Accuracy



Precision	Recall	FScore
96.31092771903499	92.42437259050054	94.16379329646463

Fig .3 Run Light GBM algorithm

In Fig 3, we can view the trained and tested tweet datasets Accuracy.

VI. CONCLUSION

Artificial Neural Networks have demonstrated significant potential in detecting cyber threats using event profiles. Their ability to model complex patterns in large, dynamic datasets makes them suitable for identifying both known and novel threats. However, challenges such as data quality, interpretability, and adversarial robustness remain, and future research

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

will likely focus on improving these aspects to ensure that ANNs can be used effectively in real-world cybersecurity applications.

REFERENCES

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, ‘‘Enhanced network anomaly detection based on deep neural networks,’’ IEEE Access, vol. 6, pp. 48231–48246, 2018.
[2] B.-C. Zhang, G.-Y. Hu, Z.-J. Zhou, Y.-M. Zhang, P.-L. Qiao, and L.-L. Chang, ‘‘Network intrusion detection based on directed acyclic graph and belief rule base,’’ Electron. Telecommun. Res. Inst. J., vol. 39, no. 4, pp. 592–604, Aug. 2017.
[3] W. Wang, Y. Sheng, and J. Wang, ‘‘HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,’’ IEEE Access, vol. 6, pp. 1792–1806, 2018.
[4] M. K. Hussein, N. Bin Zainal, and A. N. Jaber, ‘‘Data security analysis for DDoS defense of cloud based networks,’’ in Proc. IEEE Student Conf. Res. Develop. (SCOReD), Kuala Lumpur, Malaysia, Dec. 2015, pp. 305–310.
[5] S. S. Sekharan and K. Kandasamy, ‘‘Profiling SIEM tools and correlation engines for security analytics,’’ in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2017, pp. 717–721.
[6] N. Hubballi and V. Suryanarayanan, ‘‘False alarm minimization techniques in signature-based intrusion detection systems: A survey,’’ Comput. Commun., vol. 49, p. 1Â17, Aug. 2014.
[7] A. Naser, M. A. Majid, M. F. Zolkipli, and S. Anwar, ‘‘Trusting cloud computing for personal files,’’ in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Busan, South Korea, Oct. 2014, pp. 488–489.
[8] Y. Shen, E. Mariconti, P. A. Vervier, and G. Stringhini, ‘‘Tiresias: Predicting security events through deep learning,’’ in Proc. ACM CCS, Toronto, ON, Canada, Oct. 2018, pp. 592–605.
[9] K. Soska and N. Christin, ‘‘Automatically detecting vulnerable Websites before they turn malicious,’’ in Proc. USENIX Secur. Symp., San Diego, CA, USA, 2014, pp. 625–640.
[10] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, ‘‘AI2 : Training a big data machine to defend,’’ in Proc. IEEE BigDataSecurity HPSC IDS, New York, NY, USA, Apr. 2016, pp. 49–54.
[11] M. Tavallaee, E. Bagheri, W. Lu, and A. 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. 53–58.
[12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, ‘‘Toward generating a new intrusion detection dataset and intrusion traffic characterization,’’ in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), Jan. 2018, pp. 108–116.
[13] J. Song, H. Takakura, and Y. Okabe. (2006). Description of Kyoto University Benchmark Data. [Online]. Available: http://www. takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf
[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ‘‘A deep learning approach to network intrusion detection,’’ IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.
[15] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ‘‘Deep learning approach for intelligent intrusion detection system,’’ IEEE Access, vol. 7, pp. 41525–41550, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com