iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IV Month of publication: April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68760

Cyber Threat Alert Detection

T.Ammannamma[1], I.Chandana[2], K.Keerthana[3], P.Greeshma[4]
[1]Assistant Professor, Department of IT, G.Narayanamma Institute of Technology and Science (For Women)
[2, 3, 4]Student, G. Narayanamma Institute of Technology and Science (For Women)

Abstract: Cyber threats are rapidly evolving, demanding sophisticated defense mechanisms. This paper presents a novel cyber threat detection system leveraging Artificial Neural Networks (ANNs) to enhance intrusion detection capabilities. The system incorporates data preprocessing techniques, including feature scaling, encoding, and dimensionality reduction, to optimize ANN performance. A state-of-the-art ANN model is employed to analyze network traffic, identify anomalies, and detect intrusions in real-time. The system integrates with MongoDB for efficient data storage and retrieval, facilitating further analysis and reporting. By harnessing the adaptability and learning capabilities of ANNs, the proposed system aims to provide a robust, scalable, and efficient solution for detecting emerging cyber threats while minimizing false positives. The results demonstrate significant improvements in detection accuracy and response time compared to traditional methods, contributing to the advancement of AI-powered cybersecurity solutions.

Keywords: Cyber threat, Intrusion detection, ANN, Anomalies detection.

I. INTRODUCTION

Traditional cybersecurity solutions can no longer keep up with the rapid evolution of cyber dangers, such as advanced persistent threats (APTs) and zero-day exploits. Although they work well against established threats, signature-based techniques[1] and heuristic approaches [2] have limitations when it comes to identifying new or quickly evolving attack patterns. In order to overcome these obstacles, this study presents an Artificial Neural Network (ANN)-based framework for intelligent and adaptive cyber threat identification. It works using machine learning to examine both historical and real-time network data.

In order to detect risks like Distributed Denial-of-Service (DDoS) assaults, illegal access, and data exfiltration—even in situations where attack signatures are unknown—the suggested approach trains an artificial neural network (ANN) to recognize unusual patterns in network traffic[3]. Over time, the framework increases detection accuracy and decreases false positives by continuously examining system activity and network data. Real-time warnings [4] and simplified analysis are made possible by integration with MongoDB, which guarantees effective data storage and retrieval.

By identifying complex patterns and adjusting to new threats, this scalable solution goes above and beyond conventional techniques to provide strong defense against known and unknown cyberthreats[5]. The framework offers a dynamic and intelligent method of protecting organizational networks in a threat landscape that is becoming more complicated by fusing cutting-edge machine learning [6]with effective data handling.

II. LITERATURE REVIEW

In [7] have proposed,All of the machine's usual activity data is collected on a server and then dispersed to all of the machines. This system integrates the data utilized for anomaly detection on each machine, increasing the detection accuracy. The majority method and the similarity algorithm are two enhanced algorithms that are included in the suggested system in addition to a simple integration algorithm. An existing system's behavior was experimentally contrasted with that of the suggested system, which was deployed on the Linux operating system.

In [8] they introduced the application of machine learning-based intrusion detection systems (IDS) using the UNSW-NB15 dataset demonstrates their potential to enhance cybersecurity. By improving accuracy and efficiency in detecting intrusions, these systems can play a crucial role in safeguarding networks and systems against evolving cyber threats.In [9] they have employed An intrusion detection and prevention system was built using a component-based approach. It involved analyzing requirements, designing a sequential architecture, selecting COTS products, and developing PHP adapters. The system was tested in a lab and future work includes refinements, real-time testing, online deployment, and incorporating data mining.

In [10] they proposed hybrid anomaly detection technique combining statistical filtering and a composite autoencoder to efficiently identify malicious activities to limit the danger of cyber attacks. The SWaT dataset was employed to evaluate the performance of the proposed hybrid detection scheme and the results indicate higher accuracy in detection of anomalies in ICS.

It also gained up to 0.008, 0.067, and 0.039 for precision, recall and F1 score while saving 8.03% of execution time in comparison to the autoencoder only approach. Such results substantiate its enhanced accuracy and efficiency in cyber threat detection.

In [11] this study it employs deep learning and anomaly detection techniques to enhance cybersecurity threat identification. The proposed RNN achieves a higher accuracy of 96% compared to 93% for the CNN algorithm. Practical testing confirms the framework's effectiveness in detecting and mitigating various cyber threats, including insider attacks and zero-day exploits. With high accuracy, low false positive rates, and rapid response times, the framework provides a proactive and adaptive solution, surpassing traditional systems and addressing the dynamic challenges of modern cybersecurity.

III. PROPOSED SYSTEM

The system aims at reducing false positives, detection of known as well as unknown threats, and the dynamic adaptation towards evolving attack vectors. At the core of it is a deep learning ANN model trained on the most comprehensive security event and network traffic datasets available. It could learn to spot very complex patterns and anomalies as indications of probable cyber threats. Such capability could easily distinguish between benign activities from those that are malicious and the dynamic nature of learning can allow the system to update attack techniques in an ever-evolving cyber space environment. When threats are identified, the system initiates automated response mechanisms, such as quarantining suspicious files, blocking IPs linked to malicious users, and logging critical data for further analysis. Another core objective of the proposed system is to enhance detection accuracy and reduce false positives. The system uses contextual analysis, which assesses user behavior, application usage, and network activity to tell the difference between normal deviations and actual threats.

The system also has a friendly interface that has been designed to make the threat management process easy for cyber experts. It has intuitive dashboards that give a real-time view of anomaly traffic, detected threats, and system responses. Such reports give security teams quick decision making on whatever has happened and detailed recommendations on the potential impact of each threat and ways of mitigation. Custom alerts and notifications can be directed .

Thus, the proposed system is a cutting-edge cyber threat detection and response system. A combination of power from ANN and anomaly detection technique, real-time monitoring, as well as providing an intuitive interface, makes for a comprehensive and adaptive solution toward modern cybersecurity issues. This provides a holistic network defense approach besides empowering security experts to stay at the forefront against evolving threats protecting critical systems and data.

A. System Architecture

The system architecture shows in Fig1. comprises four key layers:

1) The User Interface Layer provides a dashboard for user interaction, displaying real-time alerts, threat reports, and analytics results.

2) The Application Layer, the system's core, houses machine learning models that analyze network traffic for anomalies and known attack patterns.

3) The Data Layer stores raw data such as network traffic logs and threat intelligence data for analysis.

4) The Integration Layer interacts with external security systems and threat intelligence sources to enhance detection and response capabilities.

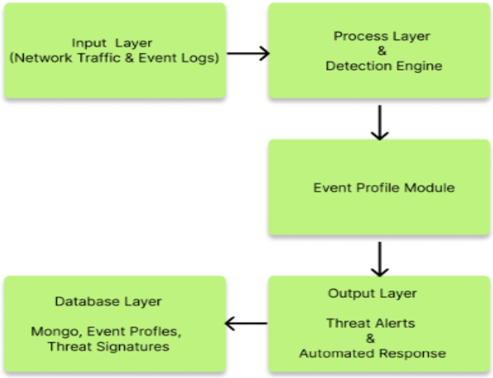


Fig1. System Architecture

IV. METHODOLOGY

The proposed cyber threat detection system is based on a robust and comprehensive framework that ensures smooth and efficient integration of different components to ensure better security. Now, some of the prominent attributes along with their methodologies are outlined in brief below:

1) *User Interface (UI)*

The user interface serves as the central hub for system interaction, enabling users to track system status, receive alerts, and generate reports. Key features include real-time threat detection alerts, visualization of system metrics and threat analyses, and customizable threat rules with adjustable thresholds. The UI will be developed using modern frontend frameworks like React.js or Angular, with basic structure and styling achieved through HTML5, CSS3, and JavaScript.

2) *Data Collection & Log Aggregation*

Data from all kinds of sources, including network traffic, system logs, and external threat intelligence feeds, will be aggregated for analysis. This feature supports multiple data sources like Syslog, SNMP traps, and network devices while also normalizing data for further processing. Technologies such as Logstash, Fluentd, or Filebeat will handle log forwarding, with external integrations like CVE databases and MITRE ATT&CK for enriched security feeds.

3) *Data Storage*

Processing and historical analysis require secure data storage. The system will store log data and alerts securely, allowing for large-scale data storage for forensic analysis. Structured and unstructured data will be managed using MongoDB or PostgreSQL, while Elasticsearch will facilitate the search and analysis of large data volumes. Distributed storage solutions like Hadoop or Apache Cassandra will handle scalability.

4) *Threat Detection Engine*

The threat detection engine uses advanced algorithms to process data for the identification of potential security breaches. It uses statistical models like Isolation Forest for anomaly detection, signature-based intrusion detection using tools like Snort and Suricata, and heuristic methods powered by machine learning models. Technologies such as TensorFlow and PyTorch support machine learning, ensuring accurate and efficient threat detection.

5) *Real-Time Data Processing*

This sub-module allows the real-time analysis of huge data, and the system will be in a position to detect threats immediately and respond promptly. The functionalities include stream processing on network traffic and system logs, suspicious pattern detection, and actual time notification for potential threats. Stream processing is handled by Apache Kafka, Flink, and Storm, and big data analytics will be done using Apache Spark.

6) *Alert Management & Notification System*

To ensure rapid threat response, the system tracks and alerts users to detected threats. Alerts can be set up with thresholds for specific event types, and real-time notifications through email, SMS, or messaging application will allow tools such as Twilio or SendGrid to do the work with slack or Microsoft Teams for effective communication.

7) *Reporting & Analytics*

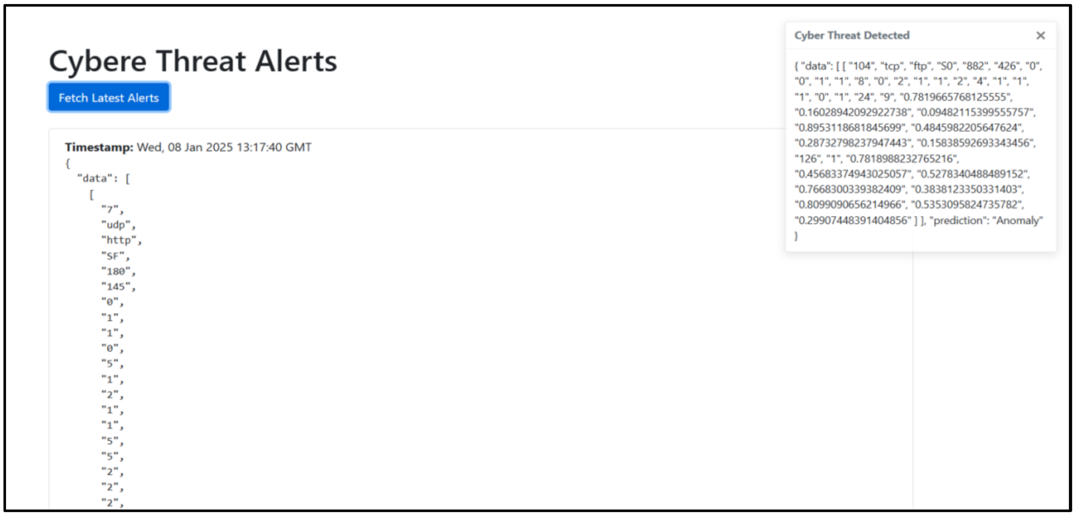
This module provides insights into system performance, detected threats, and incident response actions through periodic and on-demand reports. Reports can be customized with detailed data visualizations, offering visibility into trends, vulnerabilities, and threat patterns. Tools like Grafana, Kibana, and Tableau will handle data visualization and report generation.

8) *System Monitoring & Maintenance*

Continuous monitoring of systems ensures efficiency in operations and security. Features will include monitoring the usage of the CPU, memory, and disks, as well as alerting for system failure or performance issues. Scheduled updates to threat detection models and signatures will keep the system up-to-date. Tools like Nagios, Prometheus, and Zabbix will be used for monitoring, while Docker and Kubernetes will be used to ensure scalability and container-based deployment.

V. RESULTS AND ANALYSIS

Fig 2shows the detection of cyber threat using the trained dataset



Cybere Threat Alerts

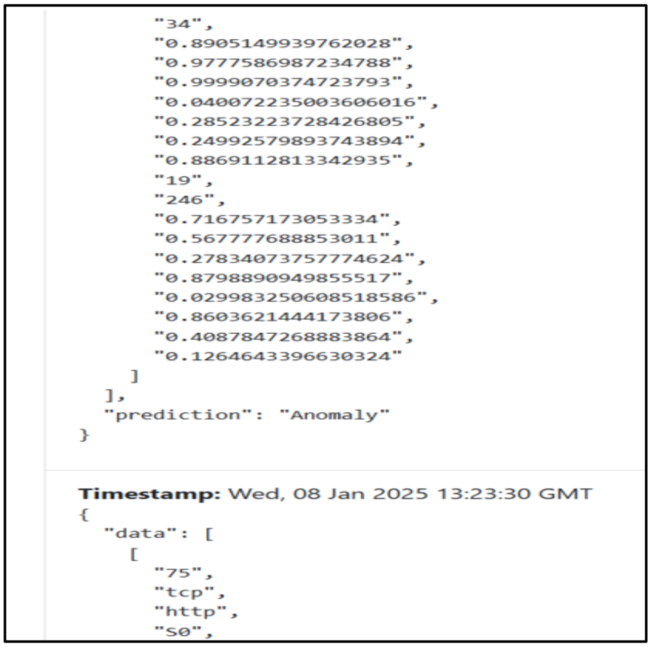
```
Timestamp: Wed, 08 Jan 2025 13:17:40 GMT
{
  "data": [
    [
      "7",
      "udp",
      "http",
      "SF",
      "180",
      "145",
      "0",
      "1",
      "1",
      "0",
      "5",
      "1",
      "2",
      "1",
      "1",
      "5",
      "5",
      "2",
      "2",
      "2",
```

Cyber Threat Detected ×

```
{ "data": [ [ "104", "tcp", "ftp", "S0", "882", "426", "0",
"0", "1", "1", "8", "0", "2", "1", "1", "2", "4", "1", "1",
"1", "0", "1", "24", "9", "0.7819665768125555",
"0.16028942092922738", "0.09482115399555757",
"0.8953118681845699", "0.4845982205647624",
"0.28732798237947443", "0.15838592693343456",
"126", "1", "0.7818988232765216",
"0.45683374943025057", "0.5278340488489152",
"0.7668300339382409", "0.3838123350331403",
"0.8099090656214966", "0.5353095824735782",
"0.29907448391404856" ] ], "prediction": "Anomaly"
}
```

Fig 2.Cyber threat detection

Fig 3shows the prediction of anomalies along with timestamp



```
        "34",
        "0.8905149939762028",
        "0.9777586987234788",
        "0.9999070374723793",
        "0.04007223500360601 6",
        "0.28523223728426805",
        "0.24992579893743894",
        "0.8869112813342935",
        "19",
        "246",
        "0.716757173053334",
        "0.567777688853011",
        "0.27834073757774624",
        "0.8798890949855517",
        "0.02998325060851858 6",
        "0.8603621444173806",
        "0.4087847268883864",
        "0.1264643396630324"
      ]
    ],
    "prediction": "Anomaly"
}

Timestamp: Wed, 08 Jan 2025 13:23:30 GMT
{
  "data": [
    [
      "75",
      "tcp",
      "http",
      "S0",
```

Fig 3. Prediction of Anomalies

VI. CONCLUSION

In conclusion the design and prototyping of Cyber Threat Detection System that aims to improve the security posture of organizations by identifying and countering threats as they occur. It utilizes a combination of network traffic captures, user activity recordings, and machine learning tools, to identify threats, anomalies, and then assigns a severity level to the threat. The integration of automatic mitigation methods such as isolation of a compromised network and sending alerts, allows appropriate actions to be done to the compromised network to limit further damage. The capability of the system to monitor computer networks in real time, analyze information, and make predictions about possible attacks enables a more robust style of cybersecurity. Visualization tools reduce the time security teams take to understand a problem and to address it. Although this substantial system provides an excellent basis for responding to threats in the cyberspace, future directions are to look for more advanced machine learning models, use a broader spectrum of security tools and improve the system's scalability to serve the needs of contemporary networks.

REFERENCES

[1] Rehman, F., Mushtaq, F., & Zaman, H. (2024, October). A Host-based Intrusion Detection: Using Signature-based and AI driven Anomaly Detection for Enhanced Cybersecurity.

[2] Sabar, N. R., Yi, X., & Song, A. (2018). A bi-objective hyper-heuristic support vector machines for big data cyber-security.

[3] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles.

[4] Danish, M. (2024). Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response.

[5] Greiman, V. (2023, June). Known unknowns: the inevitability of cyber attacks. In European Conference on Cyber Warfare and Security (Vol. 22, No. 1, pp. 223-231).

[6] Sivaraman, K. (2024, April). The Cutting-Edge Machine Learning Techniques for Seamless and Proactive Automation in Cybersecurity.

[7] Ohtahara, S., Kamiyama, T., & Oyama, Y. (2009, October). Anomaly-based Intrusion Detection System Sharing Normal Behavior Databases among Different Machines.

[8] Mohamed, A., Heilala, J., & Madonsela, N. S. (2023, August). Machine Learning-Based Intrusion Detection Systems for Enhancing Cybersecurity.

[9] Han, J., Beheshti, M., Kowalski, K., Ortiz, J., & Tomelden, J. (2009, April). Component-based Software architecture design for Network Intrusion detection and prevention system.

[10] Kwon, H. Y., Kim, T., & Lee, M. K. (2022). Advanced intrusion detection combining signature-based and behavior-based detection methods. Electronics, 11(6), 867.

[11] Rajendran, T., Imtiaz, N. M., Jagadeesh, K., & Sampathkumar, B. (2024, April). Cybersecurity Threat Detection Using Deep Learning and Anomaly Detection Techniques.