ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles

[1]Dr. Syed Khasim,[2]M. Venu Gopal,[3]B. Venkatasubbaiah,[4]M. Chinna Raj,[5]M. Venkateswarulu,

[6]M. Sukumar Prasad

[1]Assistant Professor, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

[2,3,4,5,6]U. G Student, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

ABSTRACT- ***Cyber Security Operations Centers play a critical role in monitoring, detecting, and responding to cyber threats within modern organizations. With the rapid expansion of enterprise networks, cloud services, and digital platforms, the volume and complexity of cyberattacks have increased significantly. Traditional CSOC systems primarily rely on rule-based and signature-based detection mechanisms, generating large numbers of alerts, many of which are false positives. This results in alert fatigue among security analysts and delays in responding to genuine threats. Moreover, static rule-based systems struggle to detect advanced and unknown attacks, including zero-day exploits, highlighting the need for more intelligent, adaptive security solutions. To address these challenges, this project proposes a User-Centric Machine Learning Framework that enhances CSOC efficiency and accuracy. The system uses machine learning to analyze network traffic, system logs, and security event data in real time, detecting anomalies, classifying threats, and prioritizing alerts based on severity. Its user-centric design provides analysts with intuitive dashboards, actionable insights, and a feedback loop that improves model accuracy over time.***

KEYWORDS: Artificial Intelligence (AI), Cyber Threat Detection, ANN, Network Security, Threat Prediction.

INTRODUCTION

Cybersecurity has become one of the most critical concerns for modern organizations due to the rapid expansion of digital technologies, enterprise networks, and cloud-based infrastructures. As businesses increasingly rely on interconnected systems, the attack surface exposed to cybercriminals has grown significantly. Cyber Security Operations Centers (CSOCs) are specialized units responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity incidents. These centers operate around the clock to ensure organizational assets remain protected from threats. The complexity of cyberattacks has evolved dramatically over the past decade. Attackers now use sophisticated techniques such as advanced persistent threats, ransomware campaigns, phishing schemes, and zero-day exploits. Traditional security mechanisms are often insufficient to counter these evolving threats. Most CSOCs rely heavily on rule-based and signature-based detection systems. These systems compare incoming data against predefined threat patterns. While effective for known threats, they fail to detect new and unknown attack strategies. This limitation creates security gaps in enterprise environments. Additionally, rule-based systems generate an overwhelming number of alerts daily. Many of these alerts are false positives. Analysts must manually review and validate each alert. This process consumes valuable time and resources. Alert fatigue becomes a significant operational challenge. When analysts are overloaded, genuine threats may be overlooked. The increasing volume of security logs further complicates analysis. Manual monitoring becomes inefficient and error-prone. Organizations require intelligent solutions that can process large-scale data efficiently. Machine learning has emerged as a promising approach in cybersecurity. It enables systems to learn patterns from historical data. Unlike static systems, machine learning models can adapt over time. They can identify anomalies that deviate from normal behavior. This capability enhances the detection of unknown threats. Integrating machine learning into CSOC operations improves efficiency and accuracy. However, technical innovation alone is not sufficient. Security analysts must be able to interpret and interact with automated systems effectively. Therefore, a user-centric approach becomes essential. A user-friendly interface enhances situational awareness. Visual dashboards support faster decision-making. Feedback

mechanisms improve model performance over time. This project proposes a User-Centric Machine Learning Framework for CSOCs. The framework integrates anomaly detection, threat classification, and alert prioritization. It combines automation with human expertise. Real-time data processing ensures timely response to incidents. The architecture supports scalability for enterprise deployment. It also integrates seamlessly with existing security infrastructure. By balancing automation and analyst control, the framework aims to enhance operational resilience. Ultimately, this system strengthens cybersecurity posture while reducing analyst workload and improving response efficiency.

LITERATURESURVEY

Cybersecurity has become a major research area due to the increasing number of cyber threats affecting computer networks and digital systems. Traditional intrusion detection systems mainly depend on signature-based and rule-based techniques, which are effective for detecting known attacks but often fail to identify new and unknown threats. To overcome these limitations, researchers have widely adopted Support Vector Machine (SVM), a supervised machine learning algorithm known for its high classification accuracy and ability to handle complex datasets. SVM works by finding the optimal boundary that separates normal and malicious network traffic, making it highly effective for intrusion detection. Several studies have shown that SVM performs well in detecting attacks such as DDoS, brute force, and unauthorized access while reducing false-positive rates. It can efficiently classify network traffic using features such as source bytes, destination bytes, packet count, protocol type, and failed login attempts. Recent research has also integrated SVM into web-based cybersecurity platforms for automated threat detection and real-time analysis. Based on these studies, the proposed AI-Based Cyber Threat Detection and Prevention Platformutilizes theSupport Vector Machine (SVM) algorithm to accurately detect cyber threats, improve prediction performance, provide confidence scores and security recommendations, and enhance overall network security.

RELATED WORK

Several researchers have contributed to the development of AI-based cyber threat detection systems with the aim of improving network security, attack detection accuracy, and real-time threat prevention. Early

cybersecurity solutions mainly focused on signature-based and rule-based intrusion detection systems, where malicious activities were identified using predefined attack patterns and security rules. These traditional systems were effective in detecting known cyber threats but had limited capability to identify new or evolving attacks such as DDoS attacks, brute force attacks, malware, and unauthorized network access**.** As cyberattacks became more sophisticated, researchers introduced Machine Learning algorithms, particularly Support Vector Machine (SVM)**,** to automatically analyze network traffic, learn attack patterns, and accurately classify normal and malicious activities. AI-based approaches have significantly improved detection accuracy, reduced false alarms, minimized manual monitoring, and enabled faster response to cyber threats. These advancements have led to the development of intelligent cybersecurity platforms that provide real-time threat detection, confidence scores, risk assessment, and security recommendations, thereby enhancing the overall protection of computer networks and digital systems.

EXISTING SYSTEM

Cyber Security Operations Centers in many organizations currently operate using traditional rule-based and signature-based detection systems. These systems depend on predefined rules that match known attack signatures. When network traffic or system logs match these patterns, alerts are generated. This approach is effective for detecting previously identified threats. However, it is limited to known attack signatures stored in databases. As cyber threats evolve rapidly, new attack techniques emerge frequently. Traditional systems cannot detect zero-day vulnerabilities because they lack predefined rules. This creates significant security gaps. Another major limitation is the high volume of alerts generated daily. Security tools such as firewalls, intrusion detection systems, and antivirus software produce thousands of alerts. A large percentage of these alerts are false positives. Analysts must manually review and validate each alert. This process consumes significant time and effort. Alert fatigue becomes a serious operational challenge. Overloaded analysts may ignore or delay responses to critical alerts. The lack of automated prioritization mechanisms further worsens the situation. Many systems treat all alerts with similar priority levels. This makes it difficult to identify high-risk incidents quickly. Existing systems also struggle with data integration. Logs from

different sources are often stored separately. Lack of centralized correlation limits holistic analysis. Static rule updates require manual configuration. This slows down adaptation to emerging threats. The absence of adaptive learning capabilities prevents improvement over time. Traditional systems rely heavily on human expertise for configuration and tuning. This increases operational costs. Additionally, visualization tools in many CSOCs are complex and not user-friendly. Analysts may struggle to interpret raw log data. Limited contextual information reduces decision-making efficiency. Scalability is another concern in large enterprise environments. As data volume grows, system performance may degrade. Many traditional systems lack real-time processing capabilities. Delays in detection increase risk exposure. Integration with modern cloud infrastructures is often limited. Overall, the existing CSOC framework suffers from high false positive rates, limited adaptability, scalability challenges, inefficient alert management, and insufficient user-centric design, making it inadequate for addressing modern sophisticated cyber threats.

PROPOSED SYSTEM

To overcome the limitations of traditional CSOC systems, this project proposes a User-Centric Machine Learning Framework designed to enhance detection accuracy and operational efficiency. The proposed system integrates machine learning algorithms to analyze network traffic, system logs, and security event data in real time. Unlike static rule-based systems, machine learning models learn from historical data patterns. This enables detection of unknown and zero-day attacks. The system incorporates anomaly detection techniques to identify unusual behavior. It also includes supervised classification models for threat categorization. Real-time data processing ensures timely identification of suspicious activities. One major advantage is the reduction of false positives. By learning behavioral patterns, the system differentiates between normal and malicious activities more accurately. Alert prioritization mechanisms assign risk scores to incidents. High-severity threats are highlighted for immediate response. This reduces analyst workload and improves efficiency. The framework includes intuitive dashboards for better visualization. Graphical representations enhance situational awareness. Analysts can easily interpret system outputs. A feedback loop mechanism

allows analysts to label alerts. This feedback is used to retrain and refine models continuously. Continuous learning improves detection accuracy over time. The system supports integration with existing security tools such as SIEM platforms. Centralized data aggregation improves correlation analysis. Scalability is ensured through modular architecture. Cloud compatibility allows flexible deployment. Automated classification accelerates incident response. Reduced manual intervention lowers operational costs. The user-centric design enhances collaboration between automated tools and analysts. The framework promotes proactive threat hunting capabilities. Advanced analytics provide deeper insights into attack patterns. Data encryption and access control ensure security compliance. Performance optimization ensures real-time responsiveness. Overall, the proposed system provides adaptive intelligence, reduced false positives, efficient alert prioritization, improved visualization, scalability, and continuous learning capabilities, making it more suitable for modern cybersecurity environments.

SYSTEM ARCHITECTURE

The AI-Based Cyber Threat Detection and Prevention Platform follow a layered architecture that integrates data processing, machine learning, and a web-based user interface. The system is developed using Python and the Flask framework. The uploaded data is preprocessed by handling missing values, encoding categorical features, and scaling numerical data before being used for training. The Support Vector Machine (SVM) algorithm is then trained to build a cyber threat detection model. During prediction, users enter network traffic details, and the trained model analyzes the input to identify whether the traffic is normal or represents a cyber attack such as DDoS, Brute Force, or Port Scan. The system displays the prediction result, confidence score, risk level, and security recommendations, ensuring accurate, fast.

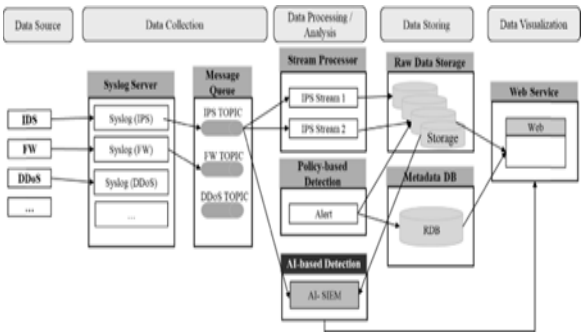

Fig1 : System Architecture

METHODLOGY DESCRIPTION

The proposed AI-Based Cyber Threat Detection and Prevention Platform follows a systematic methodology for detecting cyber

threats using Machine Learning. First, the user uploads a network traffic dataset in CSV format through the web interface. The processed data is then used to train the Support Vector Machine (SVM) algorithm to create a threat detection model. After training, the model analyzes input network traffic features and classifies them as normal or malicious. Finally, the system displays the predicted attack type, confidence score, risk level, and security recommendations for effective cyber threat prevention.

RESULTS AND DISCUSSION

Home Page:

The Home Page introduces the AI-Based Cyber Threat Detection & Prevention Platform and its purpose of detecting cyber threats using machine learning algorithms. It provides an overview of the supported models and allows users to begin the threat detection process by accessing the system through the Get Started option.

Fig2: Home page

Login Page:

The Login Page provides secure access to the AI-Based Cyber Threat Detection & Prevention Platform by authenticating authorized users. After successful login, users can upload datasets, train machine learning models, and perform cyber threat prediction.

Fig 3: Login Page

Dashboard Page:

The Dashboard Page provides an overview of the cyber threat detection workflow, including dataset upload, data preprocessing, model training, and threat prediction. It also displays the input features and threat

classification levels, allowing users to efficiently monitor and analyze network security.

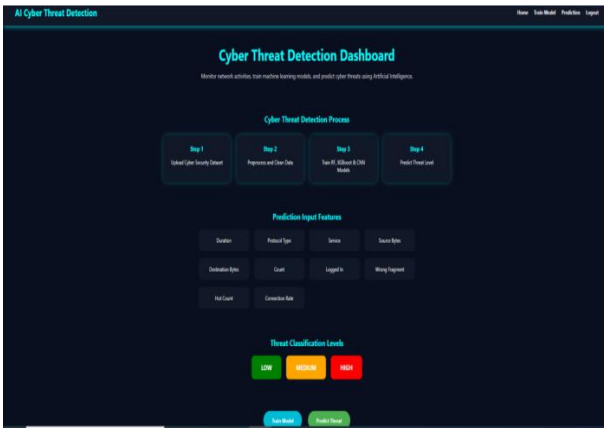

Fig 4: Dashboard Page

Train Model Page:

The Train Model Page enables users to upload a network traffic dataset and initiate the machine learning training process. It preprocesses the data, trains multiple algorithms, and selects the best-performing model for accurate cyber threat detection. Displays the accuracy of each algorithm and automatically selects the best model for prediction.

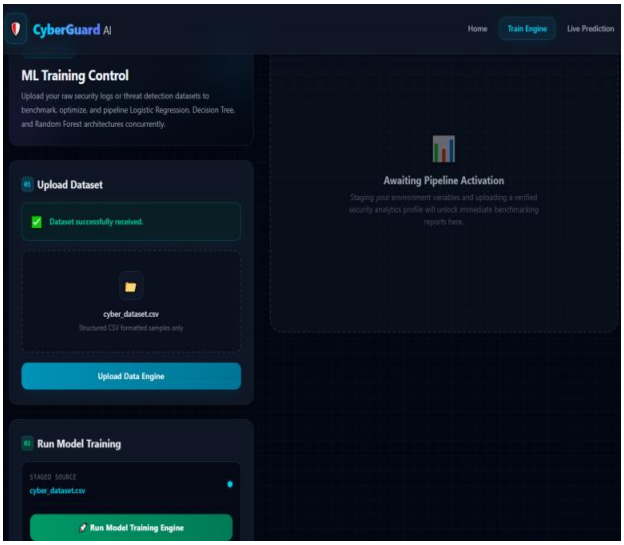

Fig 5: Train Model Page

Model Training Results:

This page displays the performance of all trained machine learning models and automatically selects the best-performing algorithm. It presents the evaluation metrics, comparison chart, and deploys the optimal model for live cyber threat prediction.

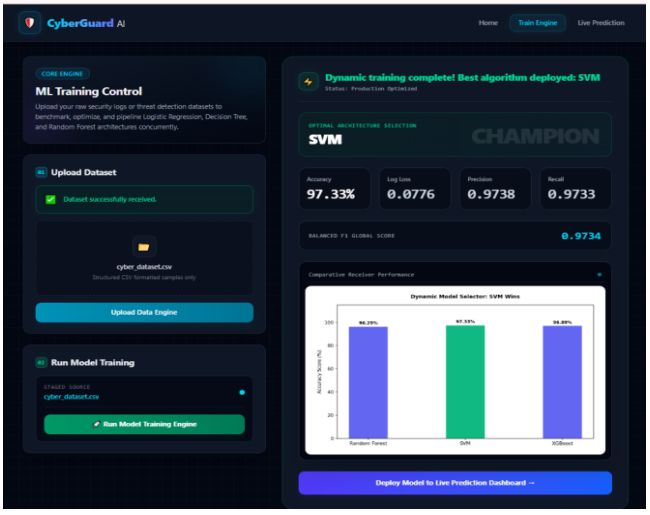

Fig 6: Model Training Results

Live Cyber Threat Prediction:

This page allows users to enter network traffic details and predict potential cyber threats in real time. The system identifies the attack type, displays the risk level, and recommends appropriate security measures.

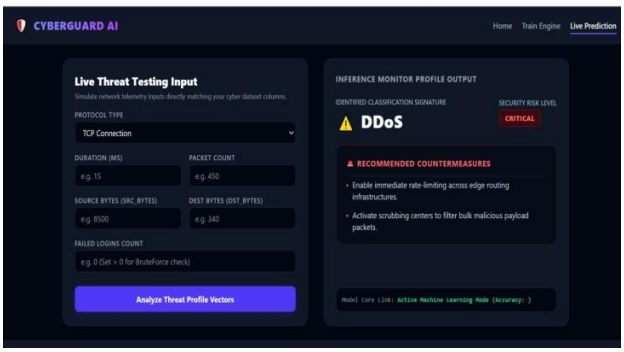

Fig 7: Live Cyber Threat Prediction

CONCLUSION

The rapid evolution of cyber threats has significantly transformed the security landscape of modern organizations. Cyber Security Operations Centers play a central role in safeguarding digital infrastructure against malicious attacks. However, traditional rule-based detection systems have proven inadequate in handling the growing complexity and sophistication of cyberattacks. Static signatures and predefined rules cannot effectively detect unknown threats or zero-day exploits. This limitation has resulted in excessive false positives, alert fatigue, and delayed incident response. To overcome these challenges, the proposed User-Centric Machine Learning Framework introduces an intelligent and adaptive solution designed specifically to enhance CSOC efficiency and effectiveness.

FUTURE SCOPE

Although the proposed framework demonstrates strong performance and reliability, continuous improvement is essential in the cybersecurity domain. Future enhancements can further expand the system's intelligence, automation, and adaptability. One important enhancement is the integration of advanced deep learning models such as transformer-based architectures for improved sequential log analysis. These models can better capture long-term dependencies in event data and enhance threat prediction accuracy.

REFERENCES

[1] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[2] C. C. Aggarwal, *Machine Learning for Text*. Cham, Switzerland: Springer, 2018.

[3] T. M. Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.

[4] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. Burlington, MA, USA: Morgan Kaufmann, 2012.

[5] F. Chollet, *Deep Learning with Python*, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021.

[6] D. Dua and C. Graff, "UCI Machine Learning Repository," University of California, Irvine, 2019.

[7] J. Brownlee, *Machine Learning Mastery with Python*. Melbourne, Australia: Machine Learning Mastery, 2020.

[8] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015.

[9] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Dataset," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1–6, 2009.

[10] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[11] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[12] J. R. Quinlan, *C4.5: Programs for Machine Learning*. San Mateo, CA, USA: Morgan Kaufmann, 1993.

[13] N. S. Altman, "An Introduction to Kernel and Nearest-Neighbor Nonparametric Regression," *The American Statistician*, vol. 46, no. 3, pp. 175–185, 1992.

[14] W. Stallings, *Network Security Essentials: Applications and Standards*, 7th ed. London, U.K.: Pearson, 2017.

[15] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. London, U.K.: Pearson, 2023.