International Journal of Innovative Information Systems & Technology Research 14(3):453-460, July-Sept, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org ISSN: 2467-8562

DOI:10.5281/zenodo.23022588

A Perceptive Model for Cybersecurity Risk Management System

[1]N. A. Buba, *[2]E. O. Bennett, *[3]D. Matthias

Department of Computer Science, Rivers State University, Port-Harcourt, Nigeria
[1]Email: abdulqadir.njibbo@rsu.edu.ng, [2] Email: bennett.okoni@ust.edu.ng

ABSTRACT
This study developed an intelligent cybersecurity attack detection system for real-time identification and classification of network attacks using Support Vector Machine (SVM). Existing intrusion detection systems struggle to detect multiple attack types accurately with low false alarm rates. The proposed system classifies traffic into Normal, Man-in-the-Middle (MITM), DDoS_HTTP, and Ransomware. A labelled dataset was preprocessed through cleaning, encoding, normalization, and feature selection. An SVM with RBF kernel was trained on an 80:20 split and achieved 98.47% accuracy with high precision, recall, and F1-score. A real-time monitoring dashboard enabled efficient threat monitoring by security administrators.
Keywords: Perceptive Model, Risk Management, Support Vector Machine, Cybersecurity

1. INTRODUCTION
The increasing dependence on information systems, cloud computing, IoT, and interconnected networks has improved organizational efficiency and connectivity but has also increased exposure to sophisticated cyber threats such as ransomware, phishing, insider attacks, supply-chain breaches, and zero-day exploits [1]. Traditional reactive security approaches based on firewalls, periodic assessments, and signature-based detection have become less effective against rapidly changing threats, often identifying vulnerabilities only after attacks occur [2]. Dynamic risk assessment and continuous monitoring have therefore become important for maintaining current security awareness. By combining real-time data, threat intelligence, behavioral analysis, and predictive analytics, organizations can identify emerging threats and respond before significant damage occurs [3]. This approach is particularly important for managing risks associated with cloud services, third-party vendors, supply chains, and remote environments. The proposed system focused on perceptive cybersecurity risk management using Support Vector Machine (SVM) for threat detection and classification. The system monitored network, IoT, cloud, and application activities and classified events as normal or potentially malicious. Historical and real-time data were analyzed to support early threat detection, risk prioritization, and mitigation. SVM was selected because of its ability to handle high-dimensional data and complex network patterns. Existing cybersecurity systems were limited by reactive detection, weak integration of threat intelligence and behavioral analysis, and inadequate real-time decision support. These limitations created the need for a perceptive cybersecurity risk management approach that combined continuous monitoring, predictive analytics, and intelligent threat detection to improve organizational security and resilience.

2. Related Works

Cybersecurity underinvestment arising from information asymmetry and misaligned incentives has been examined in prior research, which showed that information sharing improved threat preparedness and reduced duplicated security efforts [4]. Although the findings support the value of threat intelligence and collaboration in proactive cybersecurity, the work focused mainly on economic investment decisions and did not provide a real-time machine-learning-based detection mechanism.

A structured cybersecurity risk assessment framework for cloud-based services was developed through threat analysis, asset prioritization, vulnerability assessment, and risk mitigation [5]. The framework offered a useful approach for managing risks in dynamic cloud environments; however, it did not sufficiently address continuous threat prediction or automated real-time attack detection.

Machine learning techniques including decision trees, K-means, and neural networks have been investigated for predictive cybersecurity, demonstrating value for anomaly detection and early threat identification [6]. That study, however, did not focus specifically on Support Vector Machine (SVM) or integrate predictive detection with comprehensive cybersecurity risk management.

Information security risk assessment has also been examined from a business perspective, emphasizing organizational objectives, operational continuity, and risk tolerance [7]. While the integration of cybersecurity with broader enterprise risk management is valuable, the study remained mainly business-oriented and provided limited technical mechanisms for real-time threat detection.

Analysis of cybercrime during the COVID-19 pandemic identified increased phishing, RDP exploitation, and supply-chain attacks, highlighting the need for agile and predictive cybersecurity measures [8]. The primary focus, however, was on analyzing pandemic-related cyber threats rather than developing an automated cybersecurity risk management system.

A probabilistic framework for security risk analysis using Bayesian networks has been proposed to support dynamic risk estimation and prioritization [9]. Although useful for risk scoring and threat ranking, the probabilistic approach did not directly provide machine-learning-based real-time classification of network threats.

The influence of organizational security culture has been studied, identifying leadership, awareness, employee engagement, and policy communication as important security factors [10]. Recognition of human behaviour as a major cybersecurity concern is valuable, yet the study did not provide technical solutions for automated threat detection and real-time risk response.

Cybersecurity threats affecting critical infrastructure have been reviewed with recommendations for layered protection using encryption, anomaly detection, firewalls, and contingency planning [11]. Support for defense-in-depth cybersecurity is noted; however, the review did not present an integrated predictive model capable of continuously detecting and classifying emerging threats.

3. METHODOLOGY

The development of the perceptive cybersecurity risk management system employed Object-Oriented Design (OOD) as its design methodology. OOD organizes software as a collection of discrete objects that encapsulate both data (state) and behavior (processes), modeled after real-world entities that interact within the system. The proposed system detects and classifies network attacks in real time, leveraging the capabilities of a Support Vector Machine (SVM) for accurate classification. The system continuously monitors network traffic and device behavior to identify patterns indicative of malicious activity. Once potential malicious activity is detected, the SVM algorithm classifies the traffic into Normal, MITM, DDoS_HTTP, or Ransomware categories, enabling precise identification of different attack vectors. By combining real-time detection with automated classification, the system provides an immediate response mechanism to mitigate threats before they can propagate or cause significant damage. The architecture of the proposed system defines the overall structure and interaction of its components to ensure efficient detection and prevention of cyber attacks in real time, as illustrated in Figure 1.

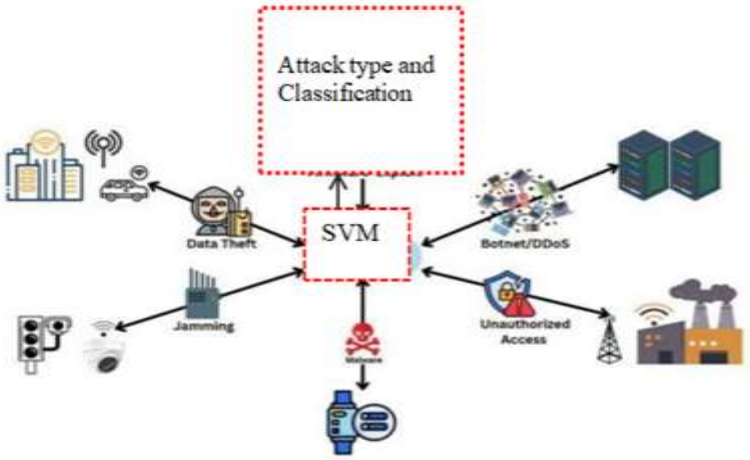

Figure 1: Architecture of the proposed system

Algorithm of the Proposed System

Real-Time Attack Detection and Classification using SVM

Step 1: Data Collection Continuously capture network traffic from connected devices.

Step 2: Data Preprocessing Extract relevant features ($X = \{x_1, x_2, \ldots, x_n\}$); normalize and clean data to remove noise.

Step 3: Attack Detection Input preprocessed data into the trained SVM model and evaluate the decision function.

Step 4: Classification If f(X) indicates a malicious pattern, classify the traffic as the corresponding attack type (MITM, DDoS_HTTP, or Ransomware); otherwise, classify the traffic as normal.

Step 5: Mitigation and Response If traffic is malicious, generate an alert to notify the network administrator and support timely response.

Step 6: Logging and Storage Store all detected events, classification results, and response actions in the database for future analysis and auditing.

Step 7: Repeat Continuously monitor network traffic in real time.

Mathematical Model of the Proposed System

The proposed system **models** botnet detection as a classification problem using a Support Vector Machine (SVM). Let the network traffic data be represented as a set of features:

X={x1,x2,x3,...,xn} Equ 1

Each input vector X **is associated** with a label y, which indicates whether the traffic is normal (y=0) or malicious (y=1):

Equ 2

$y \in \{0,1\}$

4. RESULTS AND DISCUSSIONS

System Setup

Implementation and Requirements

The system was developed and tested under the following environment and requirements:

i. Programming Language: Python 3
ii. Machine Learning Library: scikit-learn (SVM with RBF kernel)

iii. Data Processing: pandas, NumPy
iv. Visualization / Dashboard: Streamlit or equivalent real-time monitoring interface
v. Dataset: Labelled network traffic with Normal, MITM, DDoS_HTTP, and Ransomware classes

Evaluation Metrics: Accuracy, Precision, Recall, F1-score, Confusion Matrix, Classification Report

Hardware Requirements

The system was implemented on a computer equipped with a minimum Intel Core i3 processor, 4 GB RAM, and 500 GB storage capacity.

Software Requirements

The software environment consisted of the Windows 10 operating system, Python programming language, and Jupyter Notebook development environment.

Detection and Classification Results

The Support Vector Machine (SVM) model was utilized to detect, classify, and monitor attack activities in real time. The model analyzed network traffic features and classified traffic into normal activity or specific attack categories. When the calculated risk score exceeded the established threshold value, the system generated an alert and identified the corresponding attack type for immediate response. Table 1 presents the SVM threshold model used for real-time detection and classification.

Table 1: SVM Threshold Model for Real-Time Detection and Classification

Network Parameter	Threshold Value	Normal Traffic	Detected Attack Type
Packet Rate (packets/sec)	< 500	Normal	DDoS Botnet
Connection Requests	< 100/min	Normal	TCP SYN Flood Botnet
Failed Login Attempts	< 5	Normal	Brute Force Botnet
DNS Query Frequency	< 50/min	Normal	DNS Botnet Activity
Outbound Traffic Volume	< 100 MB/hr	Normal	Data Exfiltration Botnet
C&C Communication	Not Detected	Normal	C&C Botnet Communication
Network Anomaly Score	< 0.50	Normal	Suspicious Botnet Behavior
SVM Classification Score	< 0.70	Normal	Confirmed Botnet Attack

The system identifies abnormal HTTP traffic patterns, enabling rapid detection of denial-of-service attempts and supporting timely mitigation. Figure 2 demonstrates the detection of DDoS_HTTP attacks.

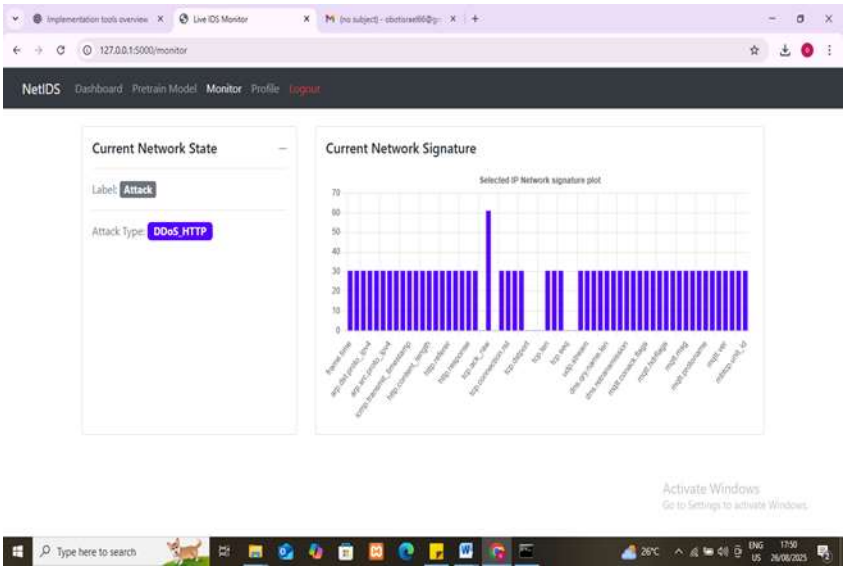

Figure 2: DDoS_HTTP attack detection

The system detects anomalies in network communication, enabling accurate identification of interception attempts and helping to preserve data confidentiality and integrity. Figure 3 illustrates the detection of MITM (Man-in-the-Middle) attacks.

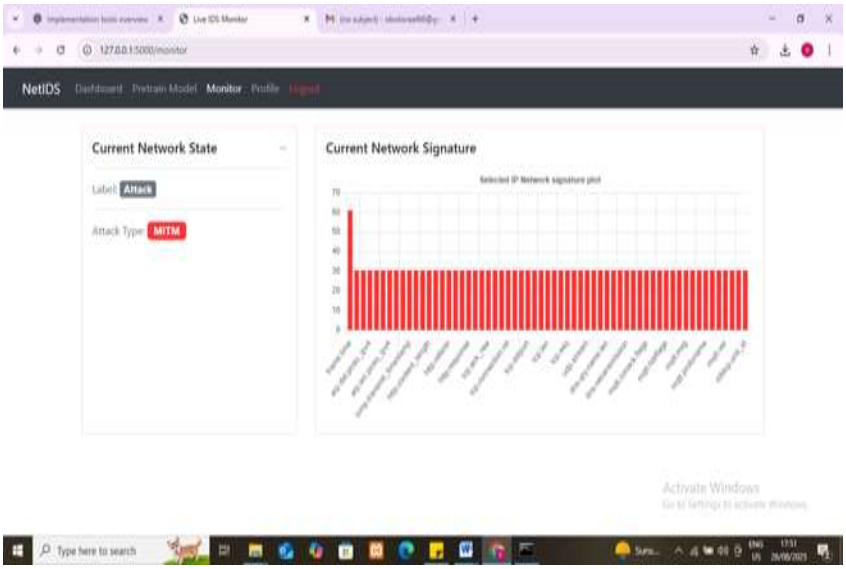

Figure 3: MITM attack detection

The system correctly distinguishes legitimate traffic from attacks, reducing false alarms and improving detection accuracy in real-world environments. Figure 4 shows normal network behavior.

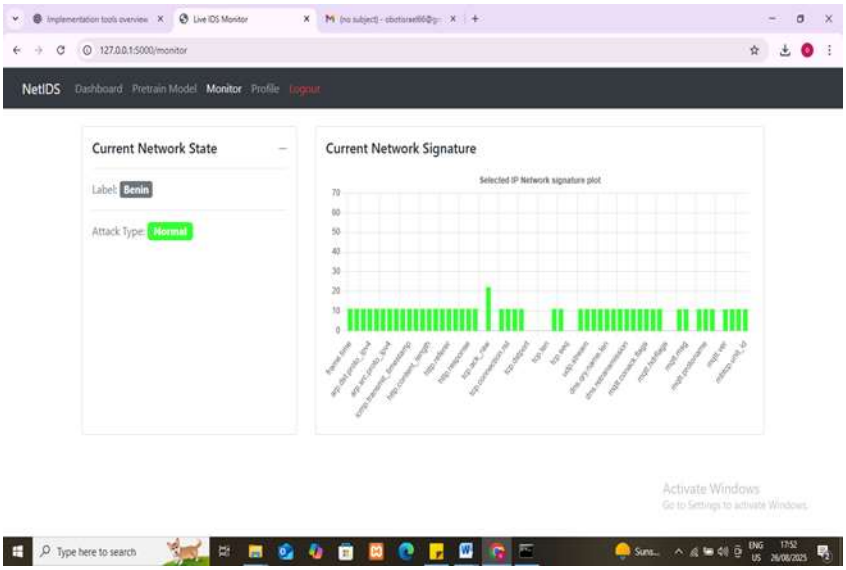

Figure 4: Normal network behavior

The dataset contains network and application-level features used to distinguish normal from malicious traffic, providing the foundation for feature engineering and attack detection. Figure 5 shows the dataset ingestion stage.

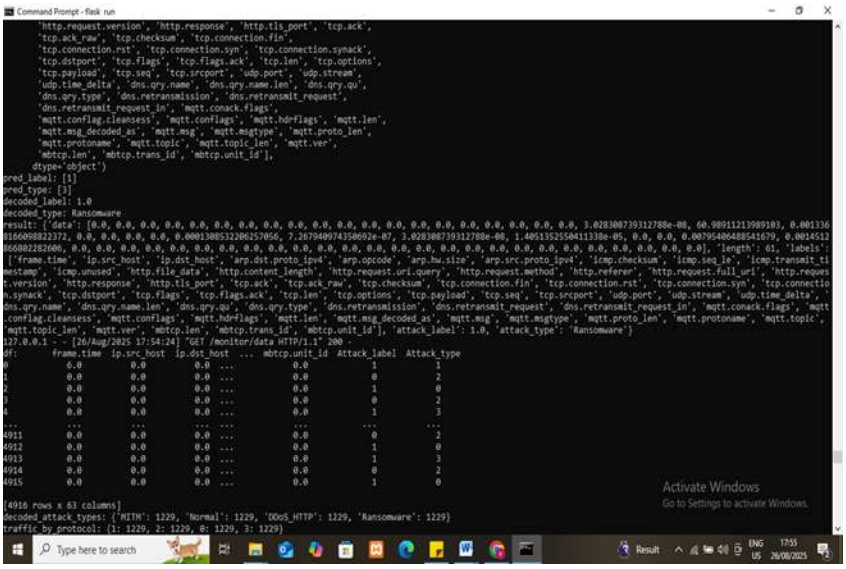

Figure 5: Dataset ingestion stage

The system achieved 98.47% accuracy with high precision, recall, and F1-score, demonstrating reliable and robust classification of normal and attack traffic. Figure 6 presents the model evaluation results.

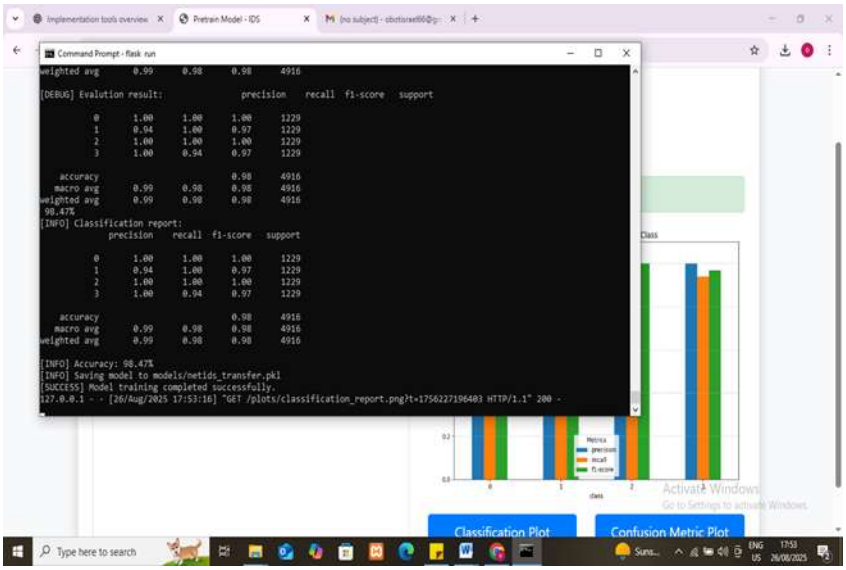

Figure 6: Model evaluation results (Accuracy)

The proposed cyberattack detection system was implemented using a labelled dataset containing Normal, MITM, DDoS_HTTP, and Ransomware traffic. The data were cleaned, encoded, normalized, and relevant features were selected to improve classification performance. The dataset was divided into training and testing sets using an 80:20 ratio. An SVM with an RBF kernel was trained to classify the four traffic categories. Incoming traffic was processed using the same preprocessing procedure before classification, and the results were displayed through the monitoring dashboard. The model successfully detected ransomware, DDoS_HTTP, MITM, and normal traffic by identifying their characteristic network behaviours. Performance evaluation showed an overall accuracy of 98.47%, with high precision, recall, and F1-scores across the traffic classes. The confusion matrix also showed that most samples were correctly classified, confirming the reliability and generalization capability of the model. The proposed system also outperformed the existing model, achieving improved accuracy compared with prior approaches. The improvement was attributed to effective preprocessing, feature selection, and the use of the RBF kernel, which improved traffic organization, classification performance, and scalability.

5. CONCLUSION

This study developed and evaluated a perceptive cybersecurity risk management system based on Support Vector Machine with an RBF kernel for real-time detection and classification of network attacks. The system successfully classified network traffic into Normal, MITM, DDoS_HTTP, and Ransomware categories with an overall accuracy of 98.47%, supported by high precision, recall, and F1-scores across all classes. A real-time monitoring dashboard enabled security administrators to view attack categories, detection logs, and network activity statistics for timely decision-making. The results demonstrate that the SVM-based approach provides an efficient and robust solution for modern cyberattack detection and network security monitoring. It is recommended that the developed system be deployed within organizational network infrastructures and periodically retrained using newly collected network traffic to maintain high detection accuracy against evolving cyber threats.

REFERENCES

[1] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management, 9*(12), 669–710.

[2] Munot, K. (2023). A comprehensive framework for managing cyber risks in cloud-based infrastructures. Journal of Cyber Defense and Digital Resilience, *7*(2), 45–62.

[3] Mahindrakar, V. (2022). Security governance and risk management approaches for digital transformation. *International Review of Cybersecurity Innovations, 5*(1), 77–94.

[4] Deshpande, A., Kulkarni, M., & Patil, R. (2022). Challenges and best practices in cyber risk management for large-scale organizations. *Asian Journal of Cybersecurity Research, 3*(2), 89–105.

[5] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy, 34*(5), 509–519.

[6] Sarker, I., Namin, A., & Arefin, M. (2019). Cybersecurity awareness and its influence on user behavior. *Journal of Cyber Research, 5*(3), 56–72.

[7] Jain, A., & Singh, R. (2020). Risk management in cybersecurity: An analytical approach.

[8] Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: Towards a business practice perspective. In *Proceedings of the 8th Australian Information Security Management Conference*. Edith Cowan University.

[9] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248.

[10] Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & Security, 29*(6), 659–679.

[11] AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575.