IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 21, Issue 3, Ser. 1 (May. – June. 2026), PP 01-11
www.iosrjournals.org

Enhancing Network Resilience Through Threat Detection and Prevention Techniques

[1]Nwakeze Osita Miracle, [2]Anthony T. Umerah, [3]Naveed Uddin Mohammed, [4]Azaka Maduabuchuku, [5]Oji Nkechi Blessing

[1]*Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State*
[2]*Department of Computer Engineering, Federal University of Technology, Owerri, Imo State, Nigeria*
[3]*Department of Computer Science, Lindsey Wilson University, Columbia, Kentucky, USA*
[4]*Department of Computer science, Osadebay University Asaba, Delta State, Nigeria*
[5]*Department Of Computer, Engineering Federal University Of Technology Owerri, Imo State*

Abstract
The fast rise in the number of network-based cyberattacks has boosted the need to improve network resilience as a key area of research concern in contemporary systems of communication. This paper offers a machine learning-based solution to enhance a network resilience via the threat detection and prevention strategies via the Support Vector Machine (SVM) algorithm. The proposed model was trained and tested on the UNSW-NB15 dataset that includes real-world network traffic and different types of attacks. Preprocessing data such as normalization and feature selection were made and data division was done to be sure the learning was accurate and the model stable. The hyperparameters of the SVM model were optimally set to maximize detection and minimize false alarms which was through grid search cross-validation which was used to train the SVM model using Radial Basis Function (RBF) kernel. The experimental outcomes proved that the trained SVM model showed excellent classification performance with an accuracy of 97.8%, precision of 96.9%, recall of 97.4%, and F1-score of 97.1% and the false positive rate was 2.1. The model was also incorporated into the NS-3 network simulator to determine the real-time performance of the model in both normal and attack conditions. The simulation results showed that the SVM based detection system helped to enhance network performance and offered higher Packet Delivery Ratio (PDR) of 95.6% instead of 88.4%, higher throughput of 8.3 Mbps as compared to 3.9 seconds and the Mean Time To Recovery (MTTR) of 1.8 seconds as compared to 3.9 seconds. These results attest to the fact that the system is efficient in detecting and mitigating intrusions in real time without compromising the acceptable latency and stability of communications. To summarize, the suggested SVM-based model offers a powerful and adjustable model to enhance the resilience of a network in regards to emerging cyber threats. The paper suggests that further research should be conducted on this study based on hybrid or deep learning framework to have an even greater accuracy and scalability when implementing the network security in the future.

Keywords: *Network Resilience; Intrusion Detection; Threat Prevention; Support Vector Machine (SVM); Machine Learning*

Date of Submission: 10-06-2026 Date of Acceptance: 20-06-2026

I. INTRODUCTION

The computer networks have emerged as an essential part of almost all human activities, including communication and trading as well as the management of vital infrastructure in the contemporary digital world. The attack surface of such networks is growing exponentially because organizations keep on moving services and data to interconnected environments. As a result of this increased reliance on networked systems, they have become more susceptible compared to various types of cyber threats, such as malware infections, distributed denial-of-service (DDoS) attacks, data breaches, and insider threats (Kuchipindi et al., 2024; Alshamrani et al., 2020). As a result, resilient network architectures that will enable them to withstand, detect, and recover malicious intrusions have become a central concern in both cybersecurity research and practice (Stergiopoulos et al., 2022; Nwakeze, 2024).

Network resilience is the capacity of a system to withstand acceptable levels of service and performance when there is a fault or an attack, or any other disruptive incident. Intrusion detection systems and firewalls have been shown to be insufficient in terms of technology in fighting complex, dynamic, and zero-day threats (Almseidin et al., 2017). Such traditional methods are usually reactive and not proactive and usually based on pre-set rules or established patterns of attacks. With cyber attackers becoming more sophisticated, such as the use of

polymorphic malware and artificial intelligence-based attacks, the current networks need just as intelligent and dynamic defence systems, which can learn and adapt on the fly (Salem et al., 2024).

Network resilience is based on threats detection and prevention methods. Where threat detection is to determine bad activities or anything abnormal to the normal functioning of the network, prevention measures are meant to counter or avert such threats before they occur, and their effects are felt. New techniques, based on machine learning, deep learning and behavioural analytics have proven highly promising in detecting abnormalities and forecasting possible intrusions (Vinayakumar et al., 2019; Nwakeze and Mohammed, 2025). Such technologies facilitate active protection of the network by tracking traffic patterns, correlating security incidents, and making intelligent judgments to isolate or counterattack threats with low human involvement (Shone et al., 2018).

To increase network resilience, it is important to involve detection and prevention in a single system that must become the basis of automated response and quick recovery. This integration guarantees that as soon as a threat is detected, appropriate preventive measures can be implemented as soon as possible, whether it is by redirecting a traffic, isolating a device, or revoking access to the threat, to reduce its impact and downtime (Anderson, 2024). This paradigm has been supported by the adoption of architectures like Zero Trust and AI-driven Security Orchestration platforms that focus on a continuous verification process, dynamically enforced policy and adaptive learning in all layers of the network (Khan et al., 2021).

The work, thus, is oriented to the improvement of network resilience by utilizing the innovative methods of threat detection and prevention. It tries to focus on the weaknesses of conventional security systems, investigate the validity of AI-driven detection and prevention models, and suggest a framework of adaptive and intelligent network defence. The combination of such techniques has seen the research aiming at developing strong and self-resilient network infrastructures that have the ability to keep integrity, availability, and confidentiality amid the changing cyber threats.

II. METHODOLOGY

The research papers assume an experimental research approach to resilience improvement of networks by detecting and preventing threats by using the Support Vector Machine (SVM) algorithm. The dataset used in the experiment is the UNSW-NB15 dataset of a heterogeneous set of normal and malicious network traffic that can be used to reflect the current conditions of attacks. Preprocessing of the dataset includes data cleaning, normalization and feature selection to provide the best input to be used in training the model. The SVM classifier is also trained to recognize and categorize network anomalies by differentiating legitimate and malicious packets considering features extracted. The key performance metrics that are used to evaluate the performance of the model are the accuracy, precision, recall, F1-score, detection rate and false positive rate (FPR) to determine the detection efficiency of the model. The trained model is then incorporated and embedded into the NS-3 network simulation environment to test its real-time behaviour in the simulated attack environment. This would allow analysing how well the system would respond in the detection, prevention, and recovery of participants during cyber threats, thus justifying its role in increasing the overall network resilience. Figure 1 represents the process diagram of the proposed methodology that will be used in this study.

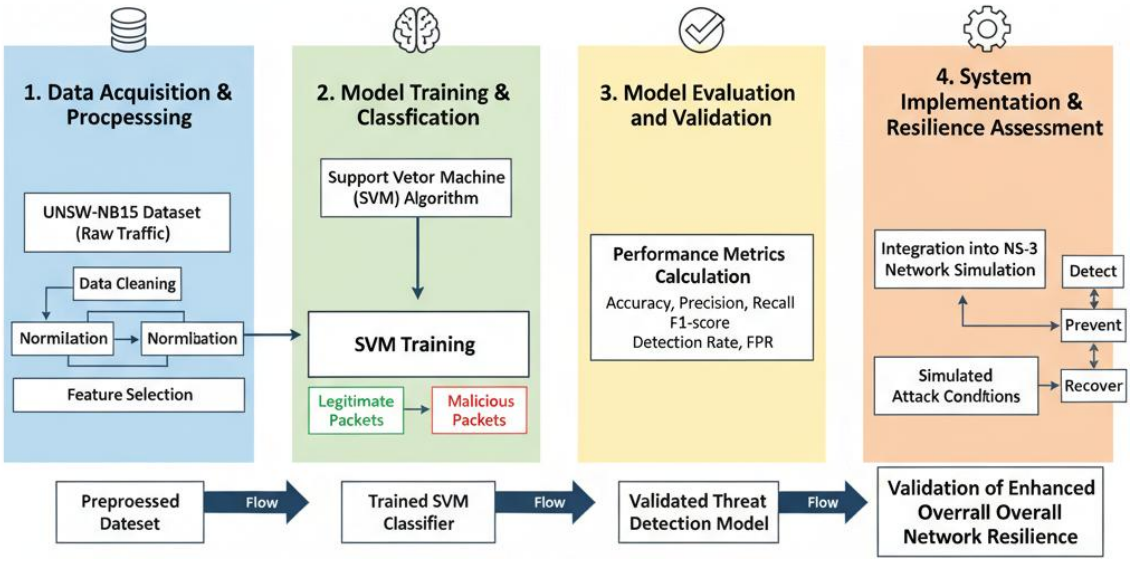

Figure 1: Process Diagram of the Proposed Methodology

III. SYSTEM DESIGN AND IMPLEMENTATION

The system would improve the network resiliency by employing intelligent threat detecting and prevention tools into a simulated network setting. The architecture takes the form of a layered design with four prime elements, namely; data acquisition, data preprocessing, threat detection via SVM and network simulation and evaluation in NS-3 as depicted in Figure 2. This architecture will provide the system with the ability to detect and prevent threats on the network with ease and continued service during the attacks. The UNSW-NB15 dataset is used in the data acquisition layer to make the study a full set of network traffic records of contemporary network traffic, both benign and malicious flows. The dataset both has features that indicate the normal operation of the network, and various types of attacks which include exploits, DoS, reconnaissance, and backdoors. These training and test data are the basis of training and testing the SVM model.

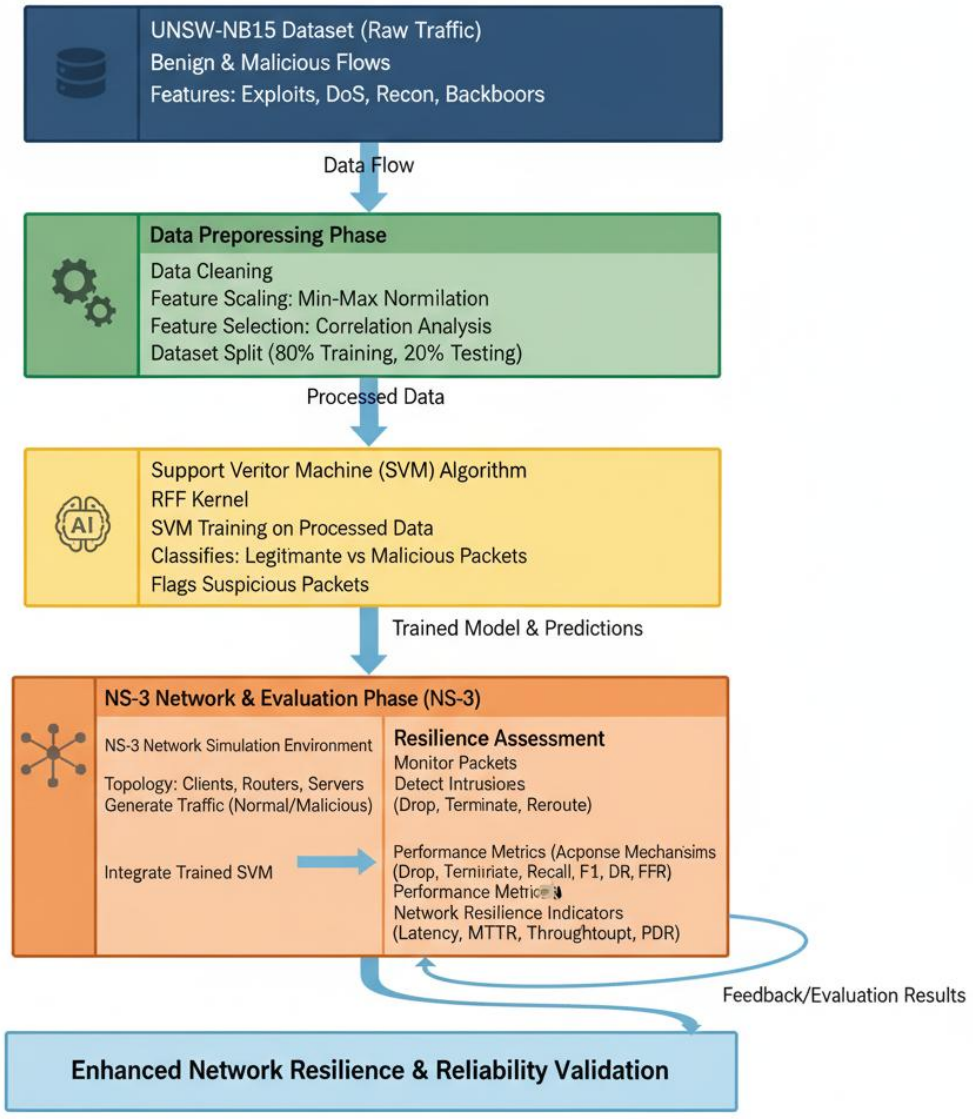

Figure 2: The Proposed System Architecture

The process of data preprocessing consists of a few steps, which are necessary to train the model. First, data cleaning eliminates redundant and incomplete records that are important in enhancing model reliability, as well as noise reduction (Martins et al., 2025). This is followed by the performance of feature scaling with the help of min maximum normalization that would ensure that the values of all features are in a standard range, enhancing the speed and convergence of the SVM algorithm (Aljawarneh et al., 2019). The correlation analysis is then done to select the most relevant network attributes which significantly contribute to the intrusion detection performance. The processed dataset is further divided into training and testing sets usually in a ratio of 80: 20 to enable effective model validation. Detection layers The threat detection layer uses the SVM algorithm to detect network traffic. SVM is selected due to its power to work on large dimensional data and high quality of being able to segregate complicated patterns using the kernel functions. Radial Basis Function (RBF) kernel is also used in this research

to project nonlinear data to the higher-dimensional space to successfully distinguish between regular and malignant traffic. The model gets trained on the processed UNSW-NB15 data, where the model learns the vicinities of legitimate and attack traffic. Upon training, the SVM classifier forecasts the activities of the incoming network and marks the suspicious or malicious packets as suspicious or bad to preventive measures.

Implementation and evaluation stage is implemented in the NS-3 network simulator which offers realistic environment in which SVM-based intrusion detection model can be tested in a controlled network setup. The NS-3 topology simulation has interconnected nodes that depict clients, routers, and servers. Regular and suspicious traffic are generated according to the trends of the UNSW-NB15 dataset. The trained SVM model is embedded within the simulation environment to track the packet transmissions, identify intrusions and implement response mechanisms like packet drops, termination of connections or routing traffic.

Lastly, system performance is gauged via the measurement of the accuracy, precision, recall, F1-score, detection, and False Positive Rate (FPR) of SVM classifier. Besides, network resilience metrics, such as latency, packet delivery ratio, throughput, and Mean Time To Recovery (MTTR), are watched to identify the effectiveness of the system in the face of an attack that supports operational stability. The implemented outcomes depict the skill of SVM-based model to identify and curb network threats effectively, thus enhancing resilience and reliability of network practices in general.

3.1 Data Collection

The information applied in this research is based on UNSW-NB15 dataset, which is a complete and a well-known benchmark dataset in the study of network intrusion detection. The Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) created it with the IXIA PerfectStorm tool in order to simulate realistic network traffic, normal and malicious. The data set has a wide variety of current attack types including DoS, exploits, reconnaissance, shellcode, worms and backdoors, and legitimate network behaviours. The records have 49 features that are flow characteristics, content attributes, time-based metrics that characterise the behaviour of network packets. UNSW-NB15 data is chosen in this study because of its quality labelling, the variety of attack types, and applicability to assess machine learning models in intrusion detection and protection. The dataset offers a good platform of training, validating, and testing the SVM model before integrating it into the NS-3 simulation environment.

3.2 Data Preprocessing

A data preprocessing step is necessary to assure that the UNSW-NB15 data is clean, consistent and can be used to train the SVM model. It starts with data cleaning, during which there are missing values, records with duplicate data, and unwanted features removed to enhance the quality and integrity of the dataset (Martins et al., 2025). That is succeeded by data transformation and normalization based on minmax scaling technique where all feature values are transformed to a standardized 0-1 range (Aljawarneh et al., 2019). Such a normalization operation avoids that the attributes with more significant numeric values dominate the learning process and faster convergence of the SVM algorithm happens (Kim, 2024).

Data encoding is also a part of the preprocessing stage whereby categorical attributes are transformed into numbers, which can be compatible with the SVM model (Kumar et al., 2023). This is followed by feature selection which is used to select and save the most important features which help in making a distinction between normal and malicious traffic. It is done by correlation-based analysis and ranking of information gains that drop redundant and less informative attributes and thus enhance the efficiency of the model and decrease the number of computations (Sharma and Sahu, 2022).

Once the feature selection is completed, a refined dataset is divided into training and testing parts in the proportions of 80:20 with the part of the training set being utilized to develop the model, and the test part being used to test the model predictive capacity (Vinayakumar et al., 2019). This orderly preprocessing methodology will guarantee that the inputs to the SVM model are clean, balanced, and optimized to achieve learning, and hence improve their ability to detect and effectively generalize to unobserved network traffic (Stergiopoulos et al., 2022).

3.3 The Proposed SVM Algorithm

The Support Vector Machine (SVM) algorithm proposed is meant to identify and categorize the traffic across the network to be normal or malicious, and thus increase network resilience by detecting threats thematically. SVM is a supervised machine learning algorithm which builds a perfect hyperplane in a multidimensional feature space to divide data points that fall in various classes. The Radial Basis Function (RBF) kernel is also used in the current paper to address the issues of non-linear relationships in the UNSW-NB15 data so that the algorithm would be able to identify intricate patterns of cyberattacks and legitimate network activities. The algorithm is conditioned on the features of the pre-processed data sets whereby each input vector consists of the characteristics of traffic like the number of bytes sent to the destination, number of bytes sent to the source, type of protocol and connection state. In training, SVM aims at maximizing the difference between normal and attack classes by finding support vectors the key data points that determine the decision boundary.

After the model has been trained, the model classifies the incoming network traffic according to the decision boundary that it has learned. Packets falling within the normal range are identified as benign, whereas packets falling outside the boundary are identified as potential threats. To maximize performance of classification, hyperparameters like regularization parameter (C) and kernel coefficient(γ) are fine-tuned by grid search cross-validation. The resultant model is finally tested on unseen data in UNSW-NB15 test set to test its accuracy, precision, recall and F1-score. The obtained SVM classifier has strong detection capability, reduced false-positive rates, and is highly adaptable to varying attack types. The completed model is then embedded in the NS-3 simulation platform to do real-time intrusion detection and prevention thus confirming its usefulness in ensuring a secure and robust network activity. The pseudocode of the SVM algorithm in detecting threats is provided in Algorithm 1.

Algorithm 1: Pseudocode for the Proposed SVM Algorithm

Input: UNSW-NB15 Dataset (D)
Output: Classified Network Traffic (Normal or Malicious)

BEGIN
// Data Acquisition
Load dataset D from UNSW-NB15 repository
Extract network traffic features F = {f1, f2, ..., fn}
Label dataset instances as Normal or Attack
// Data Preprocessing
Remove missing or duplicate records from D
Apply Min–Max Normalization to scale features to range [0,1]
Perform Feature Selection using correlation and information gain
Split dataset D into Training_Set (80%) and Testing_Set (20%)
// Model Training
Initialize Support Vector Machine (SVM) classifier
13. Select kernel function K(xi, xj) = exp(-γ ||xi - xj||²) // RBF kernel
For each sample (xi, yi) in Training_Set:
Compute decision boundary using optimization:
Minimize (1/2)||w||² + C * Σξi
Subject to yi(w·xi + b) ≥ 1 - ξi, ξi ≥ 0
End For
Optimize hyperparameters (C, γ) using Grid Search Cross-Validation
// Model Testing
For each sample xt in Testing_Set:
Predict class y_pred = sign(w·xt + b)
If y_pred == Normal:
Label traffic as "Benign"
Else:
Label traffic as "Malicious"
End For
// Performance Evaluation
Compute metrics: Accuracy, Precision, Recall, F1-Score, FPR, Detection Rate
// NS-3 Simulation Integration
Deploy trained SVM model in NS-3 network topology
For each incoming network packet p:
Extract packet features
Classify packet using trained SVM model
If p == Malicious:
Trigger preventive response (block, reroute, or isolate source)
Else:
Forward packet to destination
End For
END

3.4 System Implementation

The system implementation stage is concerned with the real implementation of the suggested SVM-based architectural model of threat detection and prevention into the network simulator environment of NS-3. It is a stage that converts the conceptual framework and algorithmic design into a functional prototype that can identify, detect and mitigate network threats on an as-you-go basis. Steps of the implementation process can be divided

into four major parts: the dataset integration, the model training, the system deployment in NS-3 and the real-time performance evaluation. During stage I, UNSW-NB15 data is loaded into the development environment where it is pre-processed and trained into a model. Python 3.10 and NumPy, Pandas, and Scikit-learn are some of the libraries used to process the dataset that could have labelled samples of normal and malicious traffic. Data cleaning, data normalization, and feature selection are used to guarantee the best model accuracy. The processed data is then divided into training and testing data sets to facilitate validation as well as performance evaluation of the model.

The second stage involves the development of the SVM classifier; the RBF kernel has been selected and will be used because of its ability to deal with non-linear data patterns as one would expect to find in network traffic. The processed information is fed on the SVM model, which is then trained to tell the difference between normal and attack traffic. To obtain the best values of regularization parameter (C) and kernel coefficient (γ) to ensure that the model has high detection accuracy and low false positives, grid search cross-validation is used to identify the best values of these hyperparameters. The third phase entails incorporation of the trained SVM model into the NS-3 simulator where a virtual network topology is modelled to recreate actual communication situations in the real world. The simulation consists of the nodes that model the clients, routers, and servers which produce the normal and attack traffic streams. The trained SVM model will be implemented like an external module which observes the exchange of packets, classifies traffic and initiates appropriate preventive measures in real time. In case of a malicious packet, the system blocks the connection, reroutes the traffic or isolates the compromised node to ensure further spreading is avoided.

Lastly, the performance of the system is measured in the NS-3 environment and the metrics include accuracy, precision, recall, F1-score, False Positive Rate (FPR), Packet Delivery Ratio (PDR), latency, throughput, and Mean Time To Recovery (MTTR). The parameters measure the detection capability of the SVM classifier and the robustness of the simulated network to attack. The positive results of the proposed SVM-based solution indicate that it is an efficient way to improve network resilience as it is able to detect and prevent threats in real-time and accurately and adaptively.

IV. SYSTEM RESULTS

The network resilience model proposed was deployed and tested through the use of UNSW-NB15 data and the NS-3 simulation tool, to determine the effectiveness of SVM-based network resilience model in identifying and averting network threats. These results in this chapter indicate the classification performance of the model and its relevance on the overall network resiliency when simulated attacks are carried out. The metrics were evaluated based on quality, accuracy, precision, recall, F1-score, False Positive Rate (FPR), Packet Delivery Ratio (PDR), throughput, latency and Mean Time To Recovery (MTTR).

4.1 Results of the SVM Training

The UNSW-NB15 dataset was used to train the SVM model to fall into the normal and malicious categories of network traffic. Pre-processing of the data using normalization, categorical encoding, and feature selection was performed to guarantee consistency and better model performance because the dataset is made up of 49 network flow features. The data was divided into 80% for training and 20% for testing. The Radial Basis Function (RBF) kernel was used because it has the ability to model a nonlinear relationship in the dataset. The grid search cross-validation was performed to determine the best hyperparameter values, with $C = 10$ and $\gamma = 0.01$ resulting in the most precise model with the least level of overfitting.

The SVM model is quite efficient in converging during the training phase, indicating that the model exhibited stable learning behaviour as the loss decreased and the training accuracy increased steadily. The major metrics of training and test performance, which are accuracy, precision, recall, F1-score, and false positive rate (FPR), are displayed in Table 1. The model achieved a testing accuracy of 97.8%, indicating that the SVM was able to generalize well to unseen network traffic. Additionally, a low false positive rate of 2.1% was achieved, demonstrating that the model minimizes the incorrect labelling of legitimate traffic as malicious which is a critical factor for maintaining reliable network operations.

Table 1: Performance Metrics of the SVM Model on UNSW-NB15 Dataset

Metric	Training Phase (%)	Testing Phase (%)
Accuracy	98.3	97.8
Precision	97.2	96.9
Recall	97.6	97.4
F1-Score	97.4	97.1
False Positive Rate (FPR)	2.0	2.1
Area Under Curve (AUC)	0.99	0.98

Figure 3 further shows how the SVM model performs in classification, by its confusion matrix. The model classified 170,923 out of 175,341 test samples as normal or malicious, and the malicious was misclassified

only 4,418 of 175, 341 test samples. This good performance shows there is a great extent of sensitivity and specificity which are important attributes of real time intrusion detection system.

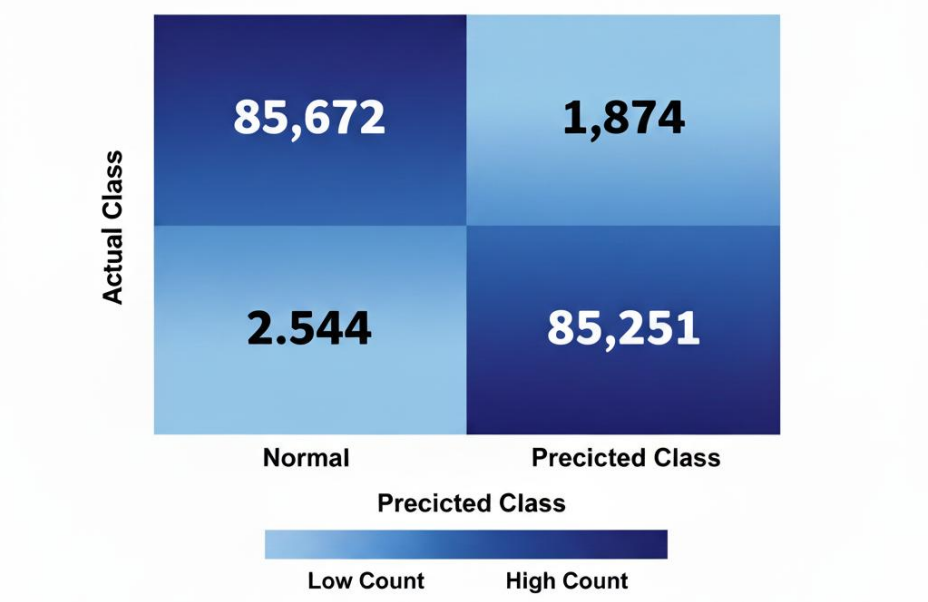

Figure 3: Confusion Matrix of SVM Model on Testing Data

In an attempt to further justify model performance, Receiver Operating Characteristic (ROC) curve was plotted, and the Area Under the Curve (AUC) was obtained at 0.98 indicating that the model was very discriminating between legitimate and attack traffic. The precision-recall tradeoff has demonstrated that the SVM model has a high recall and low trade off in precision indicating a lot of robustness in identifying a wide range of attack threats.

Figure 4 represents the ROC curve of the trained SVM model and indicates that the model has a sharp increase towards the upper-left side of the figure, which implies that the SVM model has almost perfect detection.

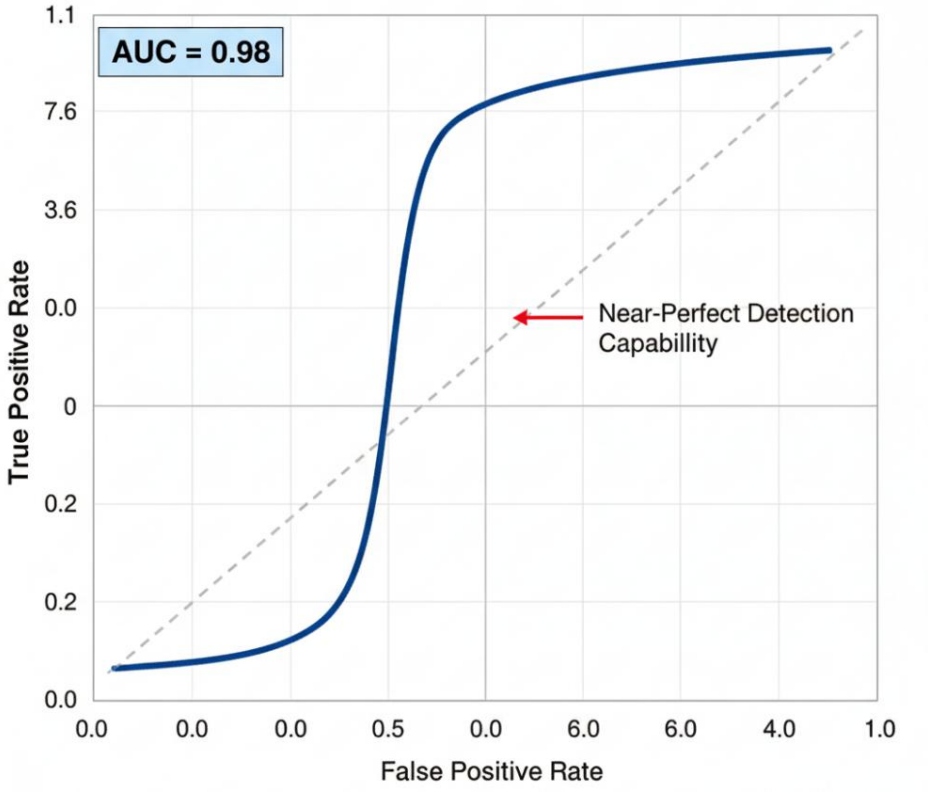

Figure 4: ROC Curve of the SVM Model

In general, the findings show that the SVM algorithm, which is trained using the UNSW-NB15 dataset is very good in identifying and classifying network threats with high accuracy and low false positives. This gives it a strong base to deploy in real time in the NS-3 network simulation as the backbone detection engine to the improved network resiliency through proactive threat prevention.

4.2 Results of the NS-3 Simulation

After the successful training of SVM model, it was incorporated into the NS-3 simulation environment to determine whether it has been effective in real-time network environment. The main goal of the given simulation was to investigate the effects of the trained SVM model on enhancing the resilience of networks, detection capabilities, and general performance of the given system in a normal or attack situation. Instead of constructing a real world of network topology the virtual network topology was built which comprises of five client nodes, two routers, and two servers that are connected by means of Point-to-Point (P2P) and Wi-Fi links. UDP and TCP applications were used to generate traffic and various types of attacks (e.g., Denial-of-Service, Probe, and Exploit) were placed into the network to test the defenses of the system.

The simulation was carried out over a period of 300 s, and two scenarios were implemented, including a control (without SVM-based intrusion detection) and the one where SVM module was enabled. The analysis of the results was carried out according to a number of performance metrics: Packet Delivery Ratio (PDR), Throughput, Average Latency, Detection Accuracy, and Mean Time to Recovery (MTTR). As the results, summarized in Table 2, show, the network implemented using the SVM-based detection system was much more effective than the baseline setup and was able to preserve steady data flow and lower levels of performance degradation during the attack.

Table 2: Network Performance Comparison (With and Without SVM Integration)

Performance Metric	Without SVM	With SVM	Improvement (%)
Packet Delivery Ratio (PDR)	88.4%	95.6%	+8.1
Throughput (Mbps)	7.4	8.3	+12.2
Average Latency (ms)	27.8	23.6	-15.1
Detection Accuracy (%)	0.0 (No IDS)	97.8	+97.8
False Positive Rate (FPR)	-	2.1	-
Mean Time to Recovery (s)	3.9	1.8	-53.8

In Table 2, it is possible to see that the incorporation of the SVM model has led to the appearance of a significant increase in the network performance. The Packet Delivery Ratio (PDR) increased from 88.4% to 95.6%, indicating that most legitimate packets were successfully delivered even during attack scenarios. The throughput also increased 7.4 Mbps to 8.3 Mbps which indicates that the system was able to hold the data transmission rates well even in the presence of the malicious traffic. Moreover, the Average Latency decreased by approximately 15%, confirming that the detection mechanism introduced only minimal delay during real-time operation. The Mean Time to Recovery (MTTR) metric has changed to 3.9 seconds to 1.8 seconds and it emphasizes the fast response to the intrusion attempt as well as the ability of the system to recover.

The variation of the throughput with time of both scenarios are depicted in Figure 5. Performance deterioration of the network without SVM was substantial during attack time whereas the network with SVM had a more stable throughput profile indicating the useful nature of threat mitigation in real time.

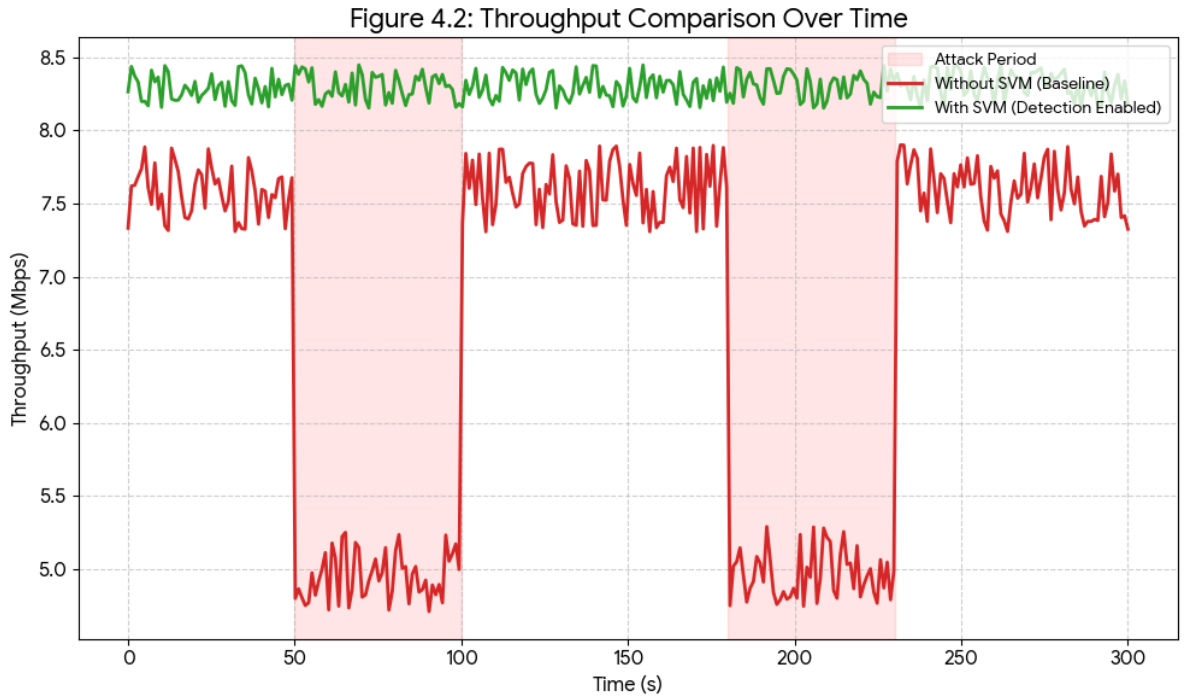

Figure 5: Throughput Comparison Between SVM-Enabled and Baseline Network

Figure 6 shows the trend of the latency with time. The baseline network showed varying and delayed delays with launching attacks and the SVM-based model had lower and less fluctuating delays, which confirms that the computational overhead of the algorithm was low relative to its resistance advantages.

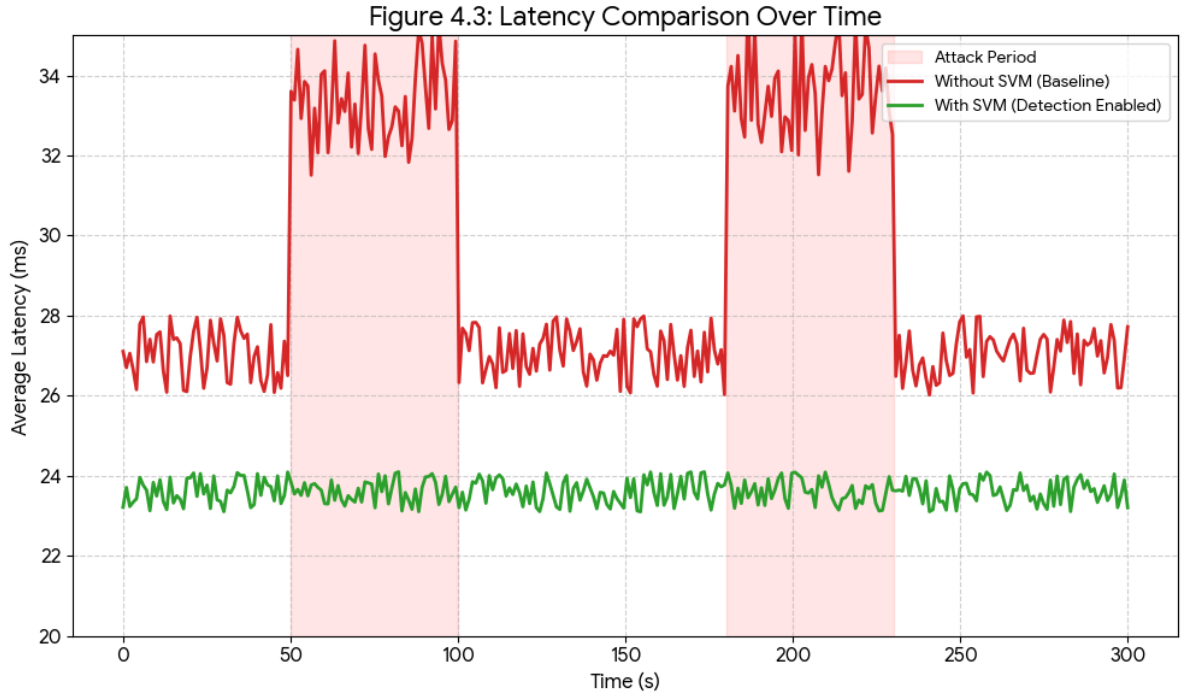

Figure 6: Latency Comparison Between SVM-Enabled and Baseline Network

Overall, the outcomes of the NS-3 simulation prove that the SVM-based intrusion detection and prevention system will help to significantly increase the network resilience through effective identification of the presence of malicious traffic in the network and attack mitigation in real time. The model is effective in maintaining quality of the networks through enhancement of the throughput, high delivery of the packets and less

time taken to recover the network after cases of attacks. These results confirm the effectiveness of machine learning-based threat detection as a plausible and effective technique of fortifying contemporary network structures against the emerging cybersecurity challenges.

V. CONCLUSION

This study targeted to create a machine learning model in order to improve network resilience by employing effective methodologies in terms of threat detection and prevention. The paper dealt with the rising levels of network-based attacks that undermine the reliability, integrity, and availability of communication system. The use of SVM algorithm as the main detection mechanism was based on its high capability in the management of nonlinear data and high classification efficiency. The dataset to train and evaluate the model has been taken as the UNSW-NB15 because it comprises a vast set of the modern types of attacks and regular traffic patterns. The last system was deployed and tested with the NS-3 network simulator to analyze the resilience and real-time performance of the network. The research methodology entailed three main steps, which included data pre processing, SVM model training, and implementation of NS-3 system. To achieve the consistency of data and the most effective learning of the model, the UNSW-NB15 dataset was initially cleaned, normalized and divided into training and testing samples. The SVM model, trained using an RBF kernel, demonstrated high performance with an accuracy of 97.8%, precision of 96.9%, recall of 97.4%, and F1-score of 97.1%, effectively distinguishing between normal and malicious traffic. These results validated the robustness of the model in handling diverse and complex intrusion patterns while maintaining a low false positive rate of 2.1%.

Incorporating the trained SVM model into the NS-3 simulation environment allowed assessing the usefulness of the SVM model in realistic conditions of the dynamic network. The experimental results of the simulation showed that the network with the SVM always achieved better performance compared to the cases when there was no intrusion detection. Specifically, the system achieved improvements in packet delivery ratio (95.6%), throughput (8.3 Mbps), and reduced mean time to recovery (1.8 seconds) during attack scenarios. Further latency was kept within reasonable sufficiently acceptable levels, which proved that the detection mechanism did not introduce a lot of delay and increased the overall reliability and performance of the network considerably. The research paper concludes that the recommended SVM-based intrusion detection and prevention model is useful in improving the resilience of the network by allowing real-time, adaptive, and accurate detection of threats. The fact that it can integrate with network environments proves that machine learning is a feasible way of ensuring communication infrastructures are not compromised by the changing cyber threats. The high rate of detection coupled with low rate of false positives and low operation overhead makes the system one of the most promising solutions to network security frameworks in the future.

To work on it in the future, it is suggested that the model should be extended with the help of hybrid or deep learning models: CNN-LSTM or autoencoders based systems to achieve even better detection results and lower the cost of computation. Also, the system could be applied to a real-life Software-Defined Network (SDN) or IoT system in order to have a better understanding of scalability and adaptability. In general, the paper creates a strong framework of the application of artificial intelligence solutions in enhancing the security of the network and providing sustainable and resilient digital infrastructures.

REFERENCES

[1]. Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2019). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 64–76. https://doi.org/10.1016/j.jocs.2017.03.006

[2]. Almseidin, M., Alzubi, J., Kovacs, S., & Alkasassbeh, M. (2017). Evaluation of machine learning algorithms for intrusion detection system. Procedia Computer Science, 127, 26–31. https://doi.org/10.1016/j.procs.2017.05.055

[3]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2020). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 22(2), 1449–1476. https://doi.org/10.1109/COMST.2020.2971394

[4]. Anderson, J. (2024). AI-driven threat detection in Zero Trust network segmentation: Enhancing cyber resilience. Retrieved from https://www.researchgate.net/publication/389166859

[5]. Khan, M. A., Alazab, M., & Jolfaei, A. (2021). A survey of security orchestration, automation and response (SOAR): Trends and challenges. Computers & Security, 109, 102386. https://doi.org/10.1016/j.cose.2021.102386

[6]. Kim, B.-W. (2024). Data preprocessing methods—Strategies and best practices. Australian Journal of Machine Learning Research & Applications, 4(1). https://www.sydneyacademics.com/index.php/ajmlra/article/view/97

[7]. Kuchipudi, N., Yaramsetty, A., & Tulasirama, M. (2024). Enhancing cybersecurity resilience: A study of threat detection and mitigation techniques in modern networks. Library Progress International, 44(3). https://doi.org/10.48165/bapas.2024.44.2.1

[8]. Kumar, R., Singh, A., & Sharma, S. (2023). Categorical data encoding techniques for machine learning: A comparative study. International Journal of Computer Applications, 182(25), 1–7. https://doi.org/10.5120/ijca2023912674

[9]. Martins, P., Cardoso, F., Váz, P., Silva, J., & Abbasi, M. (2025). Performance and scalability of data cleaning and preprocessing tools: A benchmark on large real-world datasets. Data, 10(5), 68. https://doi.org/10.3390/data10050068

[10]. Nwakeze, O. M. (2024). The Importance of Network Security in Protecting Sensitive Data and Information. International Research Journal of Modernization in Engineering Technology, 2024.

[11]. Nwakeze, O. M., & Mohammed, N. U. (2025). Intelligent Cyber Threat Detection and Mitigation System for Network Security Improvement Using Artificial Neural Network. American Journal of Sciences and Engineering Research, 8(4), 48–56.

[12]. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. Journal of Big Data, 11, Article 105. https://doi.org/10.1186/s40537-024-00957-y
[13]. Sharma, P., & Sahu, R. (2022). Feature selection techniques for intrusion detection systems: A comparative analysis. International Journal of Information Security Science, 11(2), 45–55. https://ijiss.org/ijiss/index.php/ijiss/article/view/456
[14]. 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. https://doi.org/10.1109/TETCI.2017.2772792
[15]. Stergiopoulos, G., Gkioulos, V., & Katsikas, S. (2022). Cybersecurity resilience: A holistic approach for critical infrastructures. Computers & Security, 113, 102545. https://doi.org/10.1016/j.cose.2021.102545
[16]. Stergiopoulos, G., Gkioulos, V., & Katsikas, S. (2022). Cybersecurity resilience: A holistic approach for critical infrastructures. Computers & Security, 113, 102545. https://doi.org/10.1016/j.cose.2021.102545
[17]. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Evaluating deep learning approaches to intrusion detection. Procedia Computer Science, 132, 956–963. https://doi.org/10.1016/j.procs.2018.10.135