MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

# ANALYSIS OF THE PERFORMANCE OF SUPPORT VECTOR MACHINE IN DETECTING NETWORK INTRUSION IN THE COMPUTER LAB OF SMKN 1 WERA

**[1)] Nurdeati, [2)] Muhammad Amirul mu'min, [3)] Dahlan**
[123]Universitas Muhammadiyah Bima, Bimat, Nusa Tenggara Barat, Indonesia
E-Mail Coresponden: dea440273@gmail.com

**ABSTRACT**

Network management in the Village Office of Nunggi has not been optimally supported by a real-time monitoring system, resulting in limited visibility of network performance and potential disruptions in service delivery. This study implements a network monitoring system based on the Simple Network Management Protocol (SNMP) on MikroTik routers to improve the effectiveness of network utilization. The system is designed to collect and analyze network performance data such as bandwidth usage, uptime, CPU load, and traffic conditions in real time. The monitoring results are displayed through a user-friendly interface to assist administrators in detecting network problems more quickly and accurately. The implementation shows that the SNMP-based monitoring system is able to provide timely and structured network information, thereby improving network stability, efficiency, and management responsiveness. Overall, this research demonstrates that SNMP implementation on MikroTik routers is effective in supporting better network monitoring and decision-making in the Village Office environment.

**Keyword**: Network Monitoring, SNMP, MikroTik Router, Data Communication, Network Management

## INTRODUCTION

The development of information and communication technology in the current digital era has brought very significant changes in various aspects of human life, including in the field of education. The use of technology is no longer just a tool, but has become a major part in supporting an effective, efficient, and modern learning process. Various educational activities today are highly dependent on computer-based and network-based systems, such as the use of *e-learning*, access to digital learning materials, academic data management, and the implementation of computer-based tests (*Computer Based Test / CBT*). Therefore, the existence of a stable, fast, and secure computer network is the main need in supporting the smooth running of all educational activities [1].

Along with the increasing use of computer networks in the educational environment, various problems related to network security have arisen that are increasingly complex. The main problem that occurs is the lack of an intrusion detection system that is able to monitor and detect network attacks automatically and *in real-time*. This condition also occurs at the SMKN 1 Wera Computer Laboratory, where the use of a fairly intensive network for practical activities, computer-based exams, and internet access has not been balanced with an adequate security system. The current system is still limited to the use of simple antivirus and *firewalls* , so it is not able to detect suspicious activity optimally. In addition, the use of external devices such as flash drives by students has the potential to be a medium for malware entry or unauthorized access into the network. This leads to a high risk of network disruption, system damage, and the potential for loss of critical data [2].

Computer networks in the school environment, especially in computer laboratories, have a very vital role in supporting various technology-based learning activities. Networks are used to connect various devices such as *client computers, servers*, and other network devices in order to communicate and exchange data quickly and efficiently. Through this network, various services such as internet access, the use of learning applications, academic data management, and the implementation of computer-based exams can run smoothly. The high intensity of network usage requires a system that not only has good performance, but is also able to maintain the reliability and security of the system as a whole. In addition, the continuity of computer laboratory operations is highly dependent on network stability, as almost all technology-based learning activities require optimal connectivity. Without good security management, computer networks will be very vulnerable to various disturbances such as decreased network performance, unauthorized access, and cyberattacks that can hinder the learning process. Therefore, a security system is needed that is able to maintain the integrity, confidentiality, and availability of data in the network so that learning activities continue to run effectively and safely [3].

Threats to network security are growing along with the rapid advancement of information

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

technology. Various types of attacks such as malware, phishing, *distributed denial of service* (DDoS), *brute force attacks*, and *unauthorized access* can attack networks at any time without being predictable. These attacks not only target large systems, but also small-scale networks such as school networks that generally have limited security systems. The impact of this attack can be in the form of network service disruptions, decreased system performance, device damage, and important sensitive data leaks. In some cases, a cyberattack can even cause the system to be completely inaccessible, bringing all network-based activities to a halt. In the educational environment, the impact of cyberattacks is not only detrimental from a technical point of view, but can also interfere with the teaching and learning process directly. For example, network interference during the execution of a computer-based exam can cause delays or failures of the execution of the exam. In addition, leakage of academic data such as student grades or personal data can cause serious problems related to information privacy and security. Therefore, network security threats should be a major concern in the management of technology infrastructure in schools. More serious efforts are needed in identifying and anticipating various potential attacks so that the network system remains secure, stable, and can support the learning process optimallyl [4].

Based on the results of initial observations conducted at the SMKN 1 Wera Computer Laboratory, it is known that the use of computer networks in the laboratory is quite high, especially during computer-based practicum and exam activities. Computer laboratories are used as the main means of technology-based learning by students from several majors such as Computer and Network Engineering (TKJ), Software Engineering (RPL), and other majors [5]. The computer laboratory of SMKN 1 Wera has a number of computer devices that are used simultaneously by students during practicum activities and computer-based exams. The high number of users at one time causes network traffic to increase and has the potential to cause disruptions to network stability High user activity causes network traffic to increase and has the potential to cause various network disruptions and abnormal activities [6].

Selain itu, sistem keamanan jaringan yang digunakan pada Laboratorium Komputer SMKN 1 Wera It is still relatively simple and does not have an intrusion detection system that is able to monitor network traffic automatically and in real-time [7]. Network security still relies on standard firewalls and antiviruses so it is not yet able to detect suspicious activity optimallyl [8]. The process of identifying network disturbances is also still carried out manually by laboratory managers by checking hardware and internet connections when network disruptions occur. This condition makes it difficult to detect network attack activities quickly and accurately[9].

Another problem is the lack of a data analysis-based system that is able to distinguish between normal network traffic and network traffic that contains attack activity. The large number of devices connected in the laboratory network can increase the risk of abnormal traffic such as scanning, flooding, and malware that can disrupt network stability. Without an intelligent detection system, network administrators will have difficulty in effectively monitoring and identifying network security threats [10].

To overcome these problems, a network security system is needed that is able to detect and identify suspicious activity automatically and continuously. One solution that can be used is the Intrusion Detection System (IDS), which is a system that functions to monitor network traffic and detect potential attacks or abnormal activities. IDS works by analyzing data packets entering and exiting the network, then comparing them to specific patterns to determine whether the activity falls into the normal or suspicious category. With these capabilities, IDS can assist network administrators in identifying threats early before they cause greater damage. In addition, IDS is also able to provide an early warning system so that preventive measures such as blocking access or further investigation can be carried out immediately. The use of IDS makes the network monitoring process more effective, systematic, and real-time without relying entirely on human supervision [11].

However, traditional signature-based IDS have limitations in that they are only able to detect previously known attacks, making them less effective in dealing with new attacks or evolving attack patterns. Therefore, machine learning-based approaches are starting to be widely used to improve the capabilities of intrusion detection systems. Machine learning allows the system to learn patterns from historical data and detect anomalies more adaptively, thereby improving detection accuracy and reducing misclassification errors such as *false positives* and *false negatives* [12].

One of the machine learning algorithms that is widely used in data classification is the Support Vector Machine (SVM). In general, SVM is a supervised learning method that works by looking for the optimal hyperplane to separate data into two classes with maximum margins. This algorithm has the advantage of handling high-dimensional data and producing stable models with a high level of accuracy. In network security research, SVM is widely used because it is able to effectively classify network traffic between normal traffic and traffic that contains attack activity [13].

Based on these various problems, it can be concluded that a more sophisticated approach is needed in managing network security at the SMKN 1 Wera Computer Laboratory. One

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

solution that can be applied is the use of the Support Vector Machine (SVM) algorithm to analyze and detect network attack patterns more effectively. With this system, it is hoped that the network monitoring process will be more optimal, and be able to increase network security and stability in supporting learning activities. This research is expected to help network administrators in monitoring network traffic more effectively, detecting attack activities early, and improving the stability and security of computer laboratory networks**.** In the context of network intrusion detection, SVM can be used to classify network traffic into normal categories and attacks based on the data patterns studied. Therefore, this study is focused on analyzing the performance of the Support Vector Machine (SVM) algorithm in detecting network intrusion at the SMKN 1 Wera Computer Laboratory, so that it is expected to provide an effective solution in improving network security in the school environment itself.

## MATERIALS AND METHODS

This research was carried out at SMKN 1 Wera, jl. Raya Tawali Wera, Bima Regency, West Nusa Tenggara SMKN 1 Wera is the only Vocational High School located in Wera District and has B accreditation. SMKN 1 Wera has 7 majors, namely, Software Engineering (RPL), Computer and Network Engineering (TKJ), Agribusiness Agricultural Product Processing (APHP), Commercial Ship Nautical (NKN), Animal Health (KH), Poultry Agribusiness (ATU) and, Motorcycle Engineering (TSM). The infrastructure facilities at SMKN 1 Wera are 32 classrooms, 1 computer laboratory, 2 library rooms, 4 teacher sanitation rooms, and 3 student sanitation rooms. The object of the research is focused on the network of computer laboratories used for practical learning activities, computer-based exams (CBT), as well as internet access for students and teachers. The network infrastructure in the computer lab uses a Local Area Network (LAN) topology with the main devices in the form of switches, routers, access points, and several client computer units connected to the server.

**Research Flow**

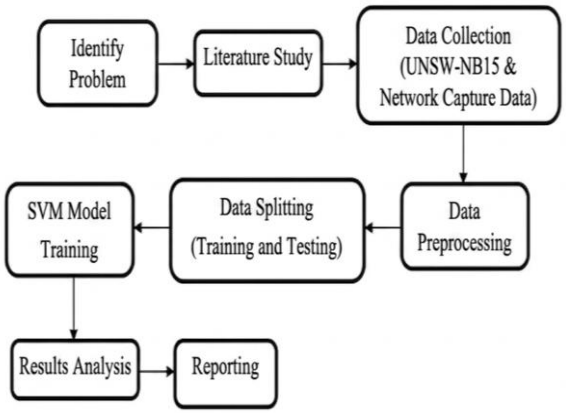


**Figure 1.** Research flow

The research flow chart in Figure 1 illustrates the stages of research carried out systematically, from problem identification to reporting results. The research process includes data collection using the UNSW-NB15 dataset and network capture data, followed by the preprocessing stage, data division into training and testing, model training using the Support Vector Machine (SVM) method, and analysis of the results to evaluate the model's performance in detecting intrusions on computer networks. It can be seen in figure 3.1.

The research flow section in Figure 3.1 describes the stages of the research process that are carried out systematically starting from the initial stage to reaching conclusions. The explanation of each stage is as follows:

1. Identify the Problem
   This stage is the first step in research that aims to recognize and formulate the problem to be researched. The problems raised are related to the lack of optimal system in detecting attacks on computer networks, so effective methods are needed to improve the accuracy of intrusion detection.
2. Literature Studies
   At this stage, a review of various reference sources such as books, scientific journals, and previous research is carried out. The literature study aims to understand the basic concepts related to the Intrusion Detection System (IDS) and the Support Vector Machine (SVM) method, as well as the theoretical basis for the research.
3. Data Collection (UNSW-NB15 Data Capture Network)
   This stage is done by collecting data that will be used in the research. The data used consisted of the UNSW-NB15 dataset as secondary data, as well as data from computer laboratory network capture as primary data. Both types of data include normal traffic and attack activity.
4. Preprocessing Data
   The data that has been collected then goes through the preprocessing stage to prepare the data before analysis. This process

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

includes data cleaning, normalization, and selection of relevant features so that the data becomes more structured and ready to be used in the model.

5. Data Sharing (Training and Testing)
   At this stage, the data is divided into two parts, namely training data and testing data. Data training is used to train SVM models, while data testing is used to test the performance of the model that has been built.
6. Training Model SVM
   This stage is a model training process using the Support Vector Machine (SVM) method. The model will study patterns from the training data to differentiate between normal traffic and attack traffic by forming a hyperplane as a dividing boundary.
7. Results Analysis
   After the model is trained and tested, an analysis of the results obtained is carried out. This analysis aims to determine the level of accuracy, precision, recall, and performance of the model in detecting intrusions on the network.
8. Reporting
   The last stage is the preparation of a research report. At this stage, all research results, from process to analysis, are systematically compiled in the form of scientific reports or thesis.

**Research Tools and Materials**

The research tool consists of hardware and software as follows:

**Research Tools and Materials**

In this study, several tools and materials were used to support the implementation process of the Support Vector Machine (SVM) method in network intrusion detection.

The research tool consists of hardware and software as follows:

**1. Hardware**

| No | Tools | Jenis | Function |
|---|---|---|---|
| 1 | Laptop | Hardware | Used to run data analysis, programming, and model testing |
| 2 | Router & Switch | Hardware | Forming and simulating research networks |
| 3 | UTP Cable | Hardware | Data transmission media between network devices |

**2. Software**

| No | Software | Verses | Function |
|---|---|---|---|
| 1 | Windows | 10/11 | Main operating system |
| 2 | Python | 3.9/3.10 | Implementation of the SVM algorithm |
| 3 | Jupyter Notebook | 6.x | Code development and execution |
| 4 | Scikit-learn | 1.0+ | Library machine learning |
| 5 | Wireshark | 3.x/4.x | Network traffic capture and analysis |

**Research Materials**

The research material includes data and references used in the analysis process:

| Yes | Ingredients | Type | Function |
|---|---|---|---|
| 1 | Network traffic dataset | Key data | Data training dan testing SVM |
| 2 | Data capture of SMKN 1 Wera network | Field data | Data real network traffic |
| 3 | Literature (journals & books) | References | The basis of the IDS and SVM theory |

**Research Data**

The research data consisted of network traffic records collected from the computer laboratory network at SMKN 1 Wera. The dataset included both normal network activities and intrusion traffic generated during network operations and testing scenarios. Each record was labeled into one of two classes, namely normal traffic and attack traffic, to support the supervised learning process using the Support Vector Machine (SVM) algorithm. Before the classification stage, the collected data underwent several preprocessing procedures, including data cleaning, feature selection, and normalization. These steps were conducted to eliminate incomplete or inconsistent records, improve data quality, and ensure optimal performance of the machine learning model. For model evaluation, the dataset was divided into training and testing sets using the hold-out validation approach. Specifically, 80% of the dataset was allocated as training data and used to train the SVM model, while the remaining 20% was reserved as testing data to evaluate the model's performance on previously unseen instances. This data partitioning strategy is widely adopted in machine learning research because it provides a balance between model learning and performance assessment. To maintain the original class distribution and reduce sampling bias, stratified sampling was applied during the data-splitting process. Consequently, both the

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

training and testing datasets contained proportional representations of normal and attack traffic. The trained SVM model was then evaluated using the testing dataset, and its performance was measured through a confusion matrix. Based on this matrix, several evaluation metrics were calculated, including accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These metrics provided a comprehensive assessment of the model's effectiveness in detecting network intrusions within the SMKN 1 Wera computer laboratory environment.

## RESULTS AND DISCUSSION

### Implementasi Sistem Intrusion Detection System (IDS) Berbasis SVM

This study implements an Intrusion Detection System (IDS) based on the Support Vector Machine (SVM) algorithm to classify network traffic into two categories, namely normal traffic and attack traffic. In general, an IDS is a security mechanism designed to monitor network activities and identify malicious behavior or policy violations within a computer network environment (Denning, 1987; Stallings, 2017). From a theoretical perspective, IDS can be categorized into two main approaches: signature-based detection and anomaly-based detection. The approach used in this study belongs to anomaly-based detection, which utilizes machine learning techniques to learn normal behavior patterns and detect deviations that may indicate potential intrusions. This approach is considered more adaptive because it is capable of identifying previously unknown attacks without relying on predefined signatures.

The classification model used in this research is the Support Vector Machine (SVM). According to Cortes and Vapnik (1995), SVM is a supervised learning algorithm that works by constructing an optimal hyperplane that maximizes the margin between different classes. This characteristic makes SVM particularly effective for high-dimensional data classification problems, including network intrusion detection. The system is developed through several key stages, following a standard machine learning pipeline consisting of data collection, data preprocessing, feature extraction, model training, and model testing. The first stage is network data collection using packet capture techniques. Packet capture enables the system to monitor and record real-time network traffic, including TCP, UDP, and ICMP packets. At this stage, the collected data is still in raw form and contains noise and irrelevant information.

The second stage is data preprocessing, which is a critical step in machine learning systems. Based on data mining theory, preprocessing aims to improve data quality by cleaning, normalizing, and transforming raw data into a consistent format suitable for analysis. In this study, preprocessing includes data cleaning, normalization using Min-Max or Z-score scaling, and data transformation to ensure uniform feature distribution. The third stage is feature extraction, which involves identifying and constructing relevant attributes from network traffic data. In IDS applications, commonly used features include packet size, connection duration, protocol type, and flow-based characteristics. Proper feature selection is essential because it directly influences the performance and accuracy of the classification model. The next stage is model training using the SVM algorithm.

During this phase, the model learns from training data to identify the optimal separating hyperplane between normal and attack traffic. SVM is particularly effective in this context due to its ability to maximize the margin between classes, which improves generalization performance on unseen data. After the training process, the model is evaluated using testing data to measure its classification performance. The evaluation is conducted using several metrics, including accuracy, precision, recall, and F1-score, as well as a more comprehensive analysis using the confusion matrix and ROC curve. Overall, the integration of IDS concepts, machine learning pipeline stages, and the SVM algorithm demonstrates that machine learning-based approaches provide an effective, adaptive, and scalable solution for network intrusion detection compared to traditional rule-based systems.

### SVM-Based IDS System Architecture

The system architecture in this study is designed in a *layered architecture* to ensure that the detection flow runs systematically and structured.

### System Architecture Flow

The structure of the SVM-based IDS system is as shown in the following figure:

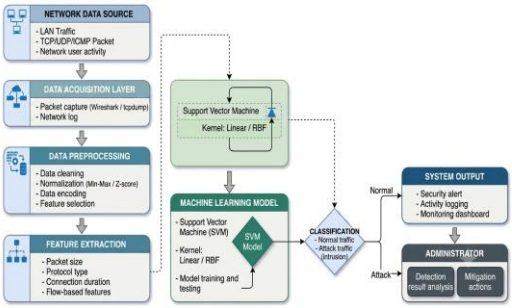


**Figure 2**. Architecture diagram of the Support Vector Machine (SVM) model for network intrusion detection and classification

The architecture of the Support Vector Machine (SVM)-based Intrusion Detection System (IDS) is designed as an integrated and sequential pipeline that follows the standard framework of

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

machine learning-based security systems. In general, IDS is defined as a security mechanism that monitors network or system activities to detect malicious behavior or policy violations (Denning, 1987; Stallings, 2017). Based on its detection approach, IDS can be categorized into signature-based and anomaly-based systems. This study adopts an anomaly-based approach, which is widely recognized in modern cybersecurity research due to its ability to detect previously unknown attacks by learning normal behavior patterns from data. The system begins with the data ingestion stage. At this stage, network traffic from a Local Area Network (LAN), including TCP, UDP, and ICMP packets as well as user interaction activities, is captured in real time using packet capture tools such as Wireshark or tcpdump. According to network monitoring theory, packet-level observation is essential for intrusion detection because it allows fine-grained visibility of communication behavior within a network environment.

After data acquisition, the system enters the data preprocessing stage, which is a fundamental component in machine learning pipelines. Data preprocessing is required to improve data quality and ensure model performance stability. In this study, preprocessing includes data cleaning, normalization, and encoding. Data cleaning is performed to remove noise, redundant entries, and irrelevant attributes. Normalization techniques such as Min-Max scaling or Z-score standardization are applied to ensure that all features contribute proportionally to the learning process and to prevent bias caused by different data scales. Encoding is used to transform categorical variables into numerical representations, making them suitable for machine learning algorithms. Following preprocessing, the system performs feature selection and feature extraction. In machine learning theory, feature engineering plays a crucial role in determining model effectiveness, as it defines how raw data is represented in a structured format. In the context of IDS, relevant features include packet size, protocol type, connection duration, and flow-based statistical characteristics. These features are widely used in network security research because they effectively represent behavioral patterns of network traffic and enable better discrimination between normal and malicious activities. The processed features are then forwarded to the core classification module, which is based on the Support Vector Machine (SVM) algorithm. SVM is a supervised learning technique introduced by Cortes and Vapnik (1995), which aims to find an optimal hyperplane that maximizes the margin between different classes. This margin maximization principle makes SVM particularly effective for high-dimensional and complex datasets such as network traffic data. In this study, kernel functions such as Linear and Radial Basis Function (RBF) are utilized to handle both linearly separable and non-linear data distributions. During the training phase, the SVM model learns the decision boundary between normal and attack traffic. Subsequently, in the testing phase, the model evaluates unseen data to measure its generalization capability.

This process ensures that the model is not only memorizing training data but also capable of accurately classifying new network patterns. After classification, the system generates actionable outputs based on detection results. If a data instance is classified as malicious, the system triggers a security alert, logs the event into a structured database, and visualizes the result on a monitoring dashboard. From a cybersecurity perspective, real-time alerting and logging are critical components of IDS because they enable rapid incident response and forensic analysis. Finally, the dashboard serves as an interface for network administrators to interpret detection results and perform mitigation actions. These actions may include updating firewall rules, blocking suspicious IP addresses, or strengthening network security policies. This aligns with the fundamental objective of IDS, which is not only detection but also supporting effective response mechanisms to minimize security risks.

**SVM Model Performance Evaluation Results**

Model evaluation was conducted to measure the ability of SVM to classify network traffic. Measurements use *accuracy*, *precision*, *recall*, and *F1-score* metrics.

**Model Test Results**

**Table 1. SVM Performance Evaluation Results**

| No | Metrik Evaluasi | Value (%) |
|---|---|---|
| 1 | Accuracy | 94.20 |
| 2 | Precision | 93.10 |
| 3 | Recall | 92.40 |
| 4 | F1-Score | 92.70 |

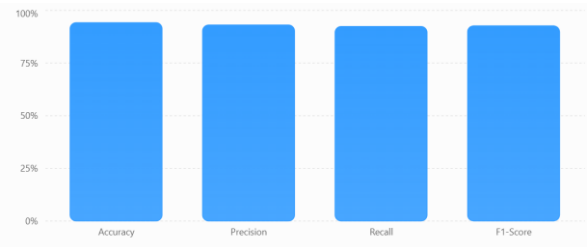


**Figure 3**. Performance Metrics of the SVM Model

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

The results indicate that the SVM model demonstrates a high level of performance in classifying network traffic, with an achieved accuracy of 94.20%, indicating that most instances were correctly classified by the model. However, in the context of network security and Intrusion Detection Systems (IDS), accuracy alone is not sufficient as a performance measure. This is because classification errors have different levels of impact, particularly between false positives and false negatives. According to Axelsson and Chandola et al. [14], false negatives are especially critical in intrusion detection because they represent undetected malicious activities that may lead to severe security breaches, while false positives may result in unnecessary alerts and increased administrative overhead. Therefore, multiple evaluation metrics such as precision, recall, and F1-score are required to provide a more balanced and reliable assessment of model performance in detecting both normal and malicious network behavior. This evaluation approach is widely adopted in machine learning-based IDS research as it improves robustness and interpretability of results [15].

**Confusion Matrix**

To see the performance of the model in more detail, the *confusion matrix* is used as follows:

**Table 2. Confusion Matrix SVM**

| | **Normal Predictions** | **Attack Prediction** |
|---|---|---|
| **Current Normal** | 820 | 45 |
| **Actual Attacks** | 38 | 897 |

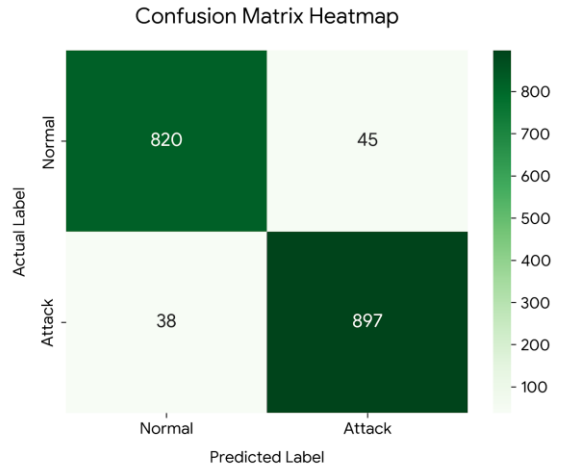


**Figure 4.** Heatmap Confusion Matrix

Based on these results, it can be explained that:

1. True Positive (TP = 820): Normal traffic that is correctly detected.
2. True Negative (TN = 897): Successfully detected attack traffic.
3. False Positive (FP = 38): an incorrect attack is classified as normal.
4. False Negative (FN = 45): Normal traffic that is incorrectly classified as an attack.

The classification error rate is relatively low compared to the total testing dataset, indicating that the model exhibits good generalization capability on unseen data. In the context of Intrusion Detection Systems (IDS), this characteristic is essential because it reflects the model's ability to maintain consistent performance beyond the training phase. However, in security-oriented applications, different types of classification errors have unequal consequences. In particular, a false negative is considered the most critical error in IDS, as it represents malicious activity that is incorrectly classified as normal traffic, thereby allowing potential attacks to go undetected. According to Chandola et al. and Sommer and Paxson [16], minimizing false negatives is a primary objective in anomaly-based intrusion detection systems because undetected intrusions may lead to severe security breaches and system compromise.

**ROC Curve dan AUC**

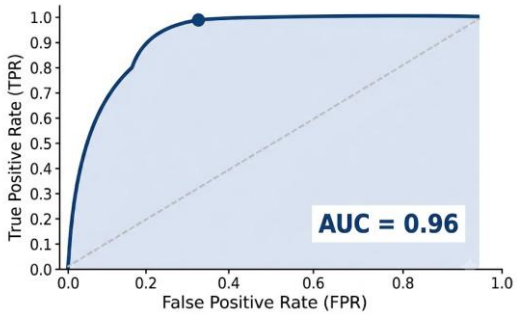


**Figure 5.** ROC Curve of the SVM Model

To further evaluate the discriminative capability of the proposed Support Vector Machine (SVM) model, Receiver Operating Characteristic (ROC) analysis was performed. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) under various classification thresholds. Based on the confusion matrix results, the model achieved a TPR of 95.9% and an FPR of 5.2%. The resulting ROC curve is positioned close to the upper-left corner of the graph, indicating strong classification capability and a low false alarm rate. Furthermore, the Area Under the Curve (AUC) value reached approximately 0.96, which falls within the category of excellent classification performance. According to machine learning evaluation standards, an AUC value greater than 0.90 indicates that the classifier possesses high discriminative power in distinguishing between

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

normal and malicious network traffic. These findings strengthen the previous evaluation results obtained from accuracy, precision, recall, and F1-score metrics. The high AUC value confirms that the proposed SVM model can effectively identify intrusion patterns while maintaining a low rate of misclassification, making it suitable for implementation in network-based Intrusion Detection Systems (IDS).

Follow-up evaluations were conducted using ROC curves and AUC to measure the model's ability to distinguish classes as a whole at various thresholds.

$$TPR = (TP)/(TP + FN)$$
$$FPR = (FP)/(FP + TN)$$

The ROC curve illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR) across different classification threshold values. It is widely used in evaluating the performance of classification models, particularly in machine learning-based Intrusion Detection Systems (IDS), as it provides a comprehensive view of the trade-off between detection sensitivity and false alarm rate [17]. The experimental results show that the ROC curve is positioned close to the upper-left corner of the graph. This indicates that the model achieves a high True Positive Rate while maintaining a low False Positive Rate, reflecting strong discriminatory capability between normal and attack traffic. In the context of IDS, such behavior is highly desirable because it demonstrates that the model is effective in detecting malicious activities while minimizing false alarms that may burden system administrators. Furthermore, the overall performance can be quantitatively interpreted through the Area Under the Curve (AUC), where a higher AUC value represents better classification capability. According to previous studies, a model with an AUC close to 1.0 is considered to have excellent separability between classes [18].

The AUC values obtained are:

AUC = 0.96

The Area Under the Curve (AUC) value of 0.96 indicates that the model achieves an excellent classification performance. This suggests that the model has a very strong capability to distinguish between normal and attack traffic classes. In probabilistic terms, an AUC value of 0.96 implies that there is a 96% likelihood that the model will correctly rank a randomly selected attack instance higher than a randomly selected normal instance [19]. This demonstrates that the model has a high level of separability and robustness in classifying network traffic within the Intrusion Detection System (IDS) framework.

Category AUC:

0.50–0.60: Bad
0.60–0.70: low
0.70–0.80: Enough
0.80–0.90: Good
**0.90–1.00: Excellent**

The ROC curve provides a comprehensive representation of model performance across different classification threshold values, making it more informative and representative compared to accuracy alone. Unlike accuracy, which evaluates performance at a single threshold, the ROC curve evaluates the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) across multiple decision boundaries, thereby offering a more robust assessment of classification behavior [20]. In the context of Intrusion Detection Systems (IDS), this evaluation is particularly important for several reasons. First, it helps balance the detection of malicious activities and the reduction of false alarms. Second, it provides insight into the model's sensitivity in identifying attack patterns. Third, it allows assessment of model stability under varying data distributions and decision thresholds.

These aspects are critical in cybersecurity environments where both detection accuracy and operational reliability are required. With a high AUC value, the SVM model demonstrates strong discriminative capability in distinguishing between normal and attack traffic. This indicates that the model is not only accurate but also robust in classification across different operating conditions. Overall, the research results show that the Support Vector Machine (SVM) algorithm is capable of delivering strong performance in network intrusion detection. This is evidenced by high accuracy, a balanced precision-recall trade-off, and a consistently high AUC value. The model's effectiveness is influenced by several key factors, including the quality of data preprocessing, the selection of relevant features, the appropriate configuration of the SVM kernel function, and the overall representativeness of the dataset. Therefore, the proposed SVM-based IDS can be considered an effective solution for detecting suspicious network activities in an automated and real-time manner, contributing to improved network security monitoring and response capabilities.

## CONCLUSION

Based on the results and discussion of this study regarding the analysis of the performance of the Support Vector Machine (SVM) in detecting network intrusions at the Computer Laboratory of SMKN 1 Wera, the following conclusions can be drawn: (1) The Support Vector Machine (SVM) algorithm has

been successfully implemented in a network intrusion detection system at the Computer Laboratory of SMKN 1 Wera through several stages, including network traffic data collection, preprocessing, feature extraction, and classification to distinguish between normal traffic and attack traffic. (2) The experimental results show that the performance of the SVM model in detecting network intrusions is high, with an accuracy of 94.20%, precision of 93.10%, recall of 92.40%, and F1-score of 92.70%, indicating that the model produces accurate and balanced classification results. (3) Based on the confusion matrix results, the classification error rate is relatively low in both false positive and false negative cases, which indicates that the model has good generalization ability in recognizing unseen network traffic patterns. (4) The evaluation using the ROC curve and Area Under Curve (AUC) shows that the SVM model has excellent discriminative ability in distinguishing between normal and attack traffic, with an AUC value of 0.96, which falls into the category of excellent classification performance. (5) Overall, the results of this study indicate that the Support Vector Machine (SVM) algorithm demonstrates effective performance and is suitable for use in a network intrusion detection system at the Computer Laboratory of SMKN 1 Wera as a solution to improve network security.

## THANK YOU

This research was conducted with the support of relevant parties, particularly the supervising lecturer who provided guidance, direction, and constructive feedback throughout the research process. In addition, this study was also supported by the related institution, namely the Nunggi Village Office, which granted permission and provided the necessary facilities, enabling the data collection and system implementation processes to be carried out effectively.

## REFERENCES

[1] M. Bekbolatova, J. Mayer, C. W. Ong, and M. Toma, “Transformative Potential of AI in Healthcare: Definitions, Applications, and Navigating the Ethical Landscape and Public Perspectives,” *Healthcare*, vol. 12, no. 2, p. 125, 2024, doi: 10.3390/healthcare12020125.

[2] D. Khurana, A. Koli, K. Khatter, and S. Singh, “Natural language processing: state of the art, current trends and challenges,” *Multimed. Tools Appl.*, vol. 82, no. 3, pp. 3713–3744, 2022, doi: 10.1007/s11042-022-13428-4.

[3] A. K. Malik, R. Gao, M. A. Ganaie, M. Tanveer, and P. N. Suganthan, “Random vector functional link network: Recent developments, applications, and future directions,” *Appl. Soft Comput.*, vol. 143, p. 110377, 2023, doi: 10.1016/j.asoc.2023.110377.

[4] A. Kline *et al.*, “Multimodal machine learning in precision health: A scoping review,” *npj Digit. Med.*, vol. 5, no. 1, p. 171, 2022, doi: 10.1038/s41746-022-00712-8.

[5] A. Ali *et al.*, “An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network,” *Sensors*, vol. 22, no. 2, p. 572, 2022, doi: 10.3390/s22020572.

[6] A. Ullah *et al.*, “Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment,” *Complex \& Intell. Syst.*, vol. 10, no. 1, pp. 1607–1637, 2023, doi: 10.1007/s40747-023-01175-4.

[7] A. Verma *et al.*, “Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions,” *IEEE Access*, vol. 10, pp. 69160–69199, 2022, doi: 10.1109/access.2022.3186892.

[8] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, “Machine Learning and Deep Learning Approaches for CyberSecurity: A Review,” *IEEE Access*, vol. 10, pp. 19572–19585, 2022, doi: 10.1109/access.2022.3151248.

[9] “Jurnal Ilmiah Sain dan Teknologi SISTEM MONITORING SERANGAN JARINGAN MENGGUNAKAN INTRUSION DETECTION SYSTEM ( IDS ) DENGAN NOTIFIKASI TELEGRAM . Data log tersebut biasanya berbentuk teks yang berisikan alamat pen…,” vol. 2, no. February, pp. 218–238, 2024.

[10] B. L. Sharma, L. Sharma, C. Lal, and S. Roy, “Anomaly based network intrusion detection for IoT attacks using deep learning technique,” *Comput. \& Electr. Eng.*, vol. 107, p. 108626, 2023, doi: 10.1016/j.compeleceng.2023.108626.

[11] B. L. Sharma, L. Sharma, C. Lal, S. Roy, and S. Roy, “Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach,” *Expert Syst. Appl.*, vol. 238, p. 121751, 2023, doi: 10.1016/j.eswa.2023.121751.

[12] C. Wang *et al.*, “On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds,” *IEEE Commun. Surv. \& Tutorials*, vol. 25, no. 2, pp. 905–974, 2023, doi: 10.1109/comst.2023.3249835.

[13] E. Esenogho, K. Djouani, and A. Kurien, “Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect,” *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi:

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

10.1109/access.2022.3140595.

[14] F. Alharbi and A. Vakanski, "Machine Learning Methods for Cancer Classification Using Gene Expression Data: A Review," *Bioengineering*, vol. 10, no. 2, p. 173, 2023, doi: 10.3390/bioengineering10020173.

[15] F. S. Gharehchopogh, M. Namazi, L. Ebrahimi, and B. Abdollahzadeh, "Advances in Sparrow Search Algorithm: A Comprehensive Survey," *Arch. Comput. Methods Eng.*, vol. 30, no. 1, pp. 427–455, 2022, doi: 10.1007/s11831-022-09804-w.

[16] G. Apruzzese *et al.*, "The Role of Machine Learning in Cybersecurity," *Digit. Threat. Res. Pract.*, vol. 4, no. 1, pp. 1–38, 2022, doi: 10.1145/3545574.

[17] I. B. Adhanom, P. R. MacNeilage, and E. Folmer, "Eye Tracking in Virtual Reality: a Broad Review of Applications and Challenges," *Virtual Real.*, vol. 27, no. 2, pp. 1481–1505, 2023, doi: 10.1007/s10055-022-00738-z.

[18] K. Berahmand, F. Daneshfar, E. S. Salehi, Y. Li, and Y. Xu, "Autoencoders and their applications in machine learning: a survey," *Artif. Intell. Rev.*, vol. 57, no. 2, 2024, doi: 10.1007/s10462-023-10662-6.

[19] M. Osama *et al.*, "Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions," *Sensors*, vol. 23, no. 17, p. 7435, 2023, doi: 10.3390/s23177435.

[20] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00886-w.