M.Tech. Scholar Seema Narware et al. 2025, V13I2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

Hybrid Intrusion Detection System Using SVM for Anomaly and Misuse Detection in Networks

M.Tech. Scholar Seema Narware, Professor Rahul Patidar, Professor Jayshree Boaddh
Dept. of Computer Science
Vaishnavi Institutes of Technology and Science, Bhopal,India

Abstract- The growing complexity and volume of cyber threats demand efficient and reliable intrusion detection systems (IDS) to safeguard network environments. This research presents a hybrid intrusion detection system that leverages Support Vector Machines (SVM) to address both anomaly and misuse detection in networks. The proposed system integrates the strengths of anomaly-based detection, capable of identifying novel and zero-day attacks, with misuse-based detection, which excels at recognizing known attack patterns. By employing SVM, the system ensures high accuracy in classifying network traffic while minimizing false positives and negatives. The hybrid approach involves preprocessing network traffic data to extract relevant features, which are then classified using SVM. Anomaly detection identifies deviations from normal network behavior, while misuse detection applies pre-defined signatures of known threats. Experimental evaluations on benchmark datasets demonstrate the system's robustness, achieving superior performance in terms of accuracy 97.1 ,precision, recall, and F1 score compared to standalone anomaly or misuse detection methods.This study highlights the potential of SVM in hybrid intrusion detection frameworks to provide a comprehensive and scalable solution for modern network security challenges. Future work will focus on incorporating adaptive learning to enhance the system's ability to detect evolving attack vectors.

Keywords -Hybrid Intrusion Detection System, Support Vector Machine, Anomaly Detection, Misuse Detection, Network Security

I. INTRODUCTION

With the rapid expansion of digital networks and the increasing sophistication of cyber threats, ensuring robust network security has become a critical challenge. Traditional Intrusion Detection Systems (IDS) are primarily classified into Misuse-based IDS **and** Anomaly-based IDS**.** Misuse-based IDS, also known as signature-based detection, relies on predefined attack signatures to identify threats. While highly accurate for detecting known attacks, this method struggles against zero-day exploits and novel intrusion patterns. On the other hand, Anomaly-based IDS identifies deviations from normal network behavior to detect previously unseen threats. However, this approach often suffers from high false positive rates, as legitimate deviations can be misclassified as attacks. The limitations of these standalone methods necessitate a Hybrid IDS, which combines both approaches to enhance detection accuracy and robustness. This paper proposes a Hybrid Intrusion Detection System (HIDS) leveraging Support Vector Machines (SVM) to integrate both anomaly and misuse detection techniques. SVM, a

supervised machine learning algorithm, is well-suited for classification tasks, particularly in distinguishing between normal and malicious network traffic. By training the model on both signature-based attack patterns and behavioral deviations, the system can effectively detect known intrusions while also identifying novel threats. The hybrid model employs SVM for anomaly detection by learning patterns of normal network behavior and flagging deviations as potential threats. Simultaneously, a signature-based approach enables precise detection of previously documented cyberattacks. The combination of these techniques provides a more comprehensive and resilient intrusion detection mechanism.

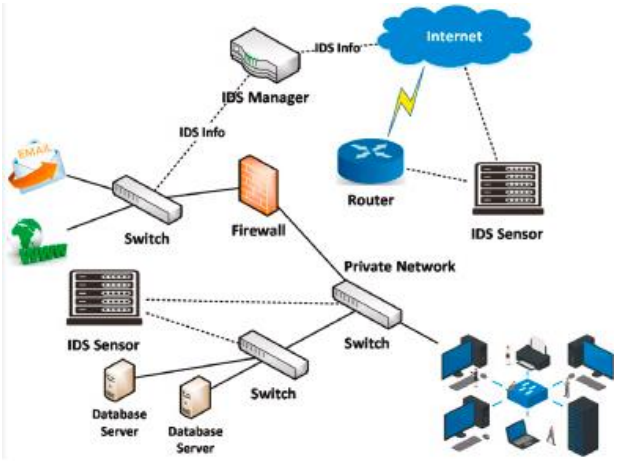

Fig 1: Architecture of IDS.

This study explores the application of SVM in hybrid IDS, focusing on its capability to improve detection rates and reduce false alarms. A detailed evaluation is conducted using benchmark datasets, measuring key performance metrics such as accuracy, precision, recall, and F1-score. The findings demonstrate that the proposed Hybrid IDS not only enhances the detection of both known and unknown attacks but also mitigates the trade-offs inherent in individual IDS approaches. By leveraging SVM's ability to create optimal decision boundaries, the proposed system aims to improve network security by providing a scalable and adaptive intrusion detection mechanism.

II.LITERATURE REVIEW

Over the past five years, significant advancements have been made in developing hybrid Intrusion Detection Systems (IDS) that combine anomaly and misuse detection techniques, often utilizing Support Vector Machines (SVM) to enhance detection capabilities. These systems aim to leverage the strengths of both methods to improve accuracy and reduce false positives in identifying network intrusions.

Kim et al. (2014) proposed a novel hybrid intrusion detection method that hierarchically integrates a misuse detection model and an anomaly detection model. The misuse detection model is built using the C4.5 decision tree algorithm, which then decomposes the normal training data into smaller subsets. Multiple one-class SVM models are subsequently created for these subsets, allowing for precise profiling of normal behavior and effective detection of both known and unknown attacks. This approach also significantly reduces the time complexity of training and testing processes.

Alqahtani et al. (2022) conducted a systematic review focusing on hybrid intrusion detection systems. The study analyzed various hybrid techniques that combine misuse-based and anomaly-based methods, highlighting the effectiveness of these approaches in addressing the limitations inherent in standalone detection systems. The review emphasized the need for further research to optimize hybrid models for better performance in detecting both known and unknown threats.

Kushal et al. (2024) introduced a self-healing hybrid intrusion detection system that combines signature-based and anomaly-based detection methods. The system utilizes C5 classifiers to categorize packets into normal and attack types, and employs Long Short-Term Memory (LSTM) networks for anomaly detection. This ensemble approach allows the system to continually learn and update its signatures for unknown attacks, thereby enhancing detection rates and reducing false positives.

Prithi and Sumathi (2019) developed an intelligent network intrusion detection system using a two-stage hybrid classification technique. In the first stage, Support Vector Machine (SVM) is employed for anomaly detection, followed by Random Forest (RF) or Decision Tree (DT) for misuse detection in the second stage. This method effectively identifies abnormal activities and classifies known attacks into categories such as Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R) attacks. The hybrid approach demonstrated superior accuracy and detection rates compared to single classifier systems.

Omrani et al. (2018) investigated the fusion of Artificial Neural Networks (ANN) and SVM classifiers for network attack detection. Their study revealed that combining these classifiers enhances detection accuracy and reduces false positives, leveraging the complementary strengths of each method. The hybrid model was tested on the NSL-KDD dataset, showing promising results in distinguishing between normal and malicious network traffic.

Alkasassbeh (2017) conducted an empirical evaluation of intrusion detection features using machine learning and feature selection methods. The study applied SVM, BayesNet, and Multi-Layer Perceptron (MLP) algorithms on a real Management Information Base (MIB) dataset. Feature selection approaches like Information Gain, ReliefF, and Genetic Search were utilized to enhance detection accuracy. The findings indicated that integrating feature selection methods with machine learning algorithms, including SVM, improves the performance of intrusion detection systems.

Shah and Issac (2017) evaluated the performance of open-source intrusion detection systems and explored the application of machine learning to the Snort system. They developed a Snort adaptive plug-in using SVM and hybrid SVM with Fuzzy logic to reduce false positive rates. The optimized SVM with the firefly algorithm achieved a false positive rate of 8.6% and a false negative rate of 2.2%, demonstrating the effectiveness of integrating machine learning techniques into traditional IDS frameworks.

Sedjelmaci and Feham (2011) proposed a hybrid intrusion detection system for clustered wireless sensor networks, combining anomaly detection based on SVM and misuse detection. Their framework effectively detects routing attacks with low false alarm rates, enhancing the security of wireless sensor networks deployed in hostile environments.

Li et al. (2023) introduced an intrusion detection model based on feature selection and an improved one-dimensional convolutional neural network (1DCNN). The model employs the Extreme Gradient Boosting (XGBoost) algorithm for feature ranking and selection, followed by an enhanced 1DCNN for classification. This approach addresses the limitations of traditional machine learning methods by automating feature extraction and improving detection efficiency. The proposed model demonstrated higher accuracy compared to conventional 1DCNN and other intrusion detection models, including SVM and Deep Belief Networks (DBN).

Silivery et al. (2023) developed a model for multi-attack classification to improve intrusion detection performance using deep learning approaches. The framework consists of a Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) with various optimizer functions. Evaluated on the NSL-KDD dataset, the model outperformed existing shallow machine learning and deep learning models in terms of accuracy, detection rate, and low false alarm rate.

Han et al. (2024) presented a study on attention-based deep learning frameworks for network intrusion detection. They compared Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and hybrid CNN-RNN architectures with and without attention mechanisms. Using the NSL-KDD dataset, the study found that RNNs with attention mechanisms achieved the lowest test loss, while pure RNNs provided the highest accuracy. The hybrid CNN-RNN model with attention offered a balanced approach, leveraging both spatial and temporal features of network traffic data.

Table 1: Comparison of Recent research in IDS

Authors (Year)	Title	Techniques Used	Accuracy	Limitations
Kim et al. (2014)	A novel hybrid intrusion detection method integrating anomaly detection with misuse detection	C4.5 Decision Tree for misuse detection; One-Class SVM for anomaly detection	Detection rate: 99% for known attacks, 30.5% for unknown attacks	Lower detection rate for unknown attacks; potential overfitting

Alqahtani et al. (2022)	A Systematic Review on Hybrid Intrusion Detection System	Systematic review of hybrid IDS techniques	N/A	Identified need for optimized hybrid models
Kushal et al. (2024)	Self-healing hybrid intrusion detection system: an ensemble machine learning approach	C5 Decision Tree for signature-based detection; LSTM for anomaly detection	True Positive Rate: 97%; False Positive Rate: 8%	Higher false positive rate; complexity in continual learning
Prithi and Sumathi (2019)	Intrusion Detection System using Hybrid SVM-RF and SVM-DT in Wireless Sensor Networks	SVM for anomaly detection; Random Forest/Decision Tree for misuse detection	Not specified	Potential computational overhead; need for feature optimization
Omrani et al. (2018)	Fusion of ANN and SVM Classifiers for Network Attack Detection	Combination of Artificial Neural Networks and SVM classifiers	Improved detection accuracy over individual classifiers	Increased computational complexity; potential overfitting

Alkasassbeh (2017)	An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods	SVM, BayesNet, and MLP with feature selection methods	BayesNet with Genetic Search: 99.9% accuracy	Dataset dependency; need for real-time validation
Shah and Issac (2017)	Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System	SVM and Fuzzy logic applied to Snort IDS	Optimized SVM with firefly algorithm: FPR 8.6%, FNR 2.2%	High false positive rate; resource consumption
Sedjelmaci and Feham (2011)	Novel hybrid intrusion detection system for clustered wireless sensor	SVM for anomaly detection; misuse detection techniques	Effective detection of routing attacks with low false alarm	Limited to specific attack types; scalability concerns

	network			
Li et al. (2023)	An Intrusion Detection Model Based on Feature Selection and Improved One-Dimensional Convolutional Neural Network	XGBoost for feature selection; Improved 1D CNN for classification	Accuracy improved by 0.67% over baseline	Potential overfitting; computational demands
Silivery et al. (2023)	A model for multi-attack classification to improve intrusion detection performance using deep learning approaches	LSTM-RNN with various optimizer functions	Outperformed existing models in accuracy and detection rate	Requires extensive training data; potential overfitting
Han et al. (2024)	Attention-Based Deep Learning Frameworks for Network Intrusion Detection	CNNs, RNNs, and hybrid CNN-RNN architectures with attention mechanisms	RNNs with attention achieved lowest test loss	Complexity in model architecture; computationally intensive
Zhang et al. (2020)	A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine	Deep Belief Network for feature learning; SVM for classification	High detection accuracy in real-time scenarios	High computational resource requirements
Kaur and Singh (2020)	Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks	Deep Recurrent Neural Networks for anomaly detection; signature generation for misuse detection	Improved detection rates for various attack types	Potential overfitting; requires large training datasets
Jiang et al. (2020)	Network Intrusion Detection Combined Hybrid Sampling With Deep	Hybrid sampling techniques; Deep Hierarchical Network for detection	Enhanced detection performance on imbalanced datasets	Complexity in implementation; computational overhead

	Hierarchical Network			
Alghayadh and Debnath (2020)	A Hybrid Intrusion Detection System for Smart Home Security	Combination of anomaly and misuse detection techniques tailored for smart home environments	Improved detection accuracy for smart home attacks	Limited to smart home scenarios; scalability issues

III.METHODOLOGY

The methodology developed a hybrid intrusion detection system (IDS) that integrates anomaly-based detection and misuse-based detection using Support Vector Machine (SVM) as the core classification algorithm. The system is designed to enhance accuracy, reduce false positives, and detect both known and unknown attack patterns in network traffic.This dataset consists of forty-five attributes or features and the strongest attributes can be proposed to detect more accuracy. The dataset contains some irrelevant and redundant features, which is unimportant. Feature Selection plays an important role in achieving more accuracy in intrusion detection. By including records of normal traffic and all attacktypes, UNSW-NB15 dataset is broadly classified into Testing and Training datasets with #175, 341 and #82, 332 records respectively.

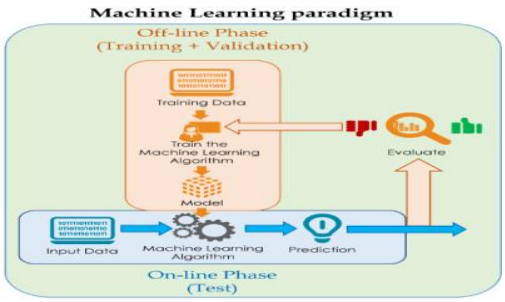

Fig 2: IDS using SVM

Overview of Data Processing and ML Implementation of UNSW_NB15 Dataset The UNSW-NB15 dataset is widely used for evaluating network intrusion detection systems (IDS) due to its realistic attack scenarios and diverse feature set. Effective data processing and machine learning (ML) implementation on this dataset require multiple steps, including data preprocessing, data cleaning, feature selection, hybrid detection approaches, and result analysis.

Before applying ML models, the dataset undergoes preprocessing to handle missing values, redundant features, and data inconsistencies. This involves converting categorical features into numerical values using one-hot encoding or label encoding. Standardization or normalization techniques like Min-Max scaling or Z-score normalization are applied to ensure uniformity in feature distributions.

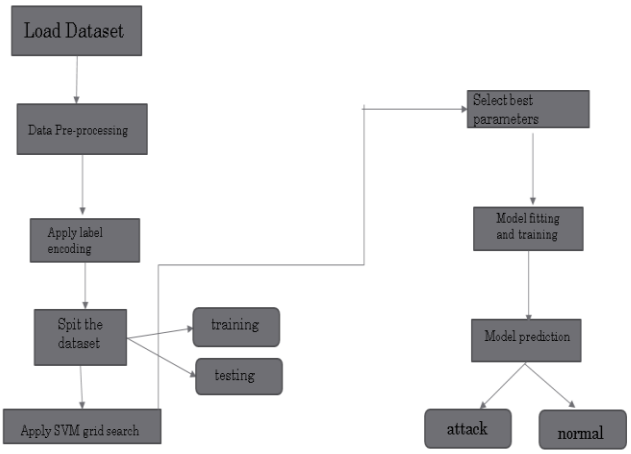

Fig 3: Flow chart of proposed model.

The UNSW-NB15 dataset contains 49 features, including flow-based, content-based, and time-based attributes. Feature selection helps in reducing dimensionality and improving model efficiency. Techniques like Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), Mutual Information (MI), and correlation-based selection are commonly applied. Hybrid models often rely on optimized feature subsets to improve classification accuracy while minimizing computational overhead.

Algorithm

Algorithm: Hybrid Intrusion Detection System Using SVM

Input: Network traffic dataset D = {(x1, y1), (x2, y2), ..., (xm, ym)}

```
    where xi = feature vector, yi = {normal(1), attack(-1)}
Output: Intrusion detection results (Normal or Attack)
Preprocessing Step
  a. Normalize dataset:
    FOR each feature xi in D:
      xi' = (xi - mean) / std_dev
    END FOR
  b. Split data into training and testing sets:
    (D_train, D_test) ← split(D, 80%)
Train One-Class SVM for Anomaly Detection:
  a. Train One-Class SVM model:
anomaly_model = train_one_class_svm(D_train_normal)
  b. Define anomaly decision function:
    function detect_anomaly(x):
      score = anomaly_model.predict(x)
      RETURN -1 if score < threshold ELSE
Train C-SVM for Misuse Detection
  a. Train C-SVM classifier:
misuse_model = train_c_svm(D_train)
  b. Define misuse decision function:
    function detect_misuse(x):
      label = misuse_model.predict(x)
      RETURN label
Hybrid Decision Making
  a. Function hybrid_detection(x):
anomaly_result = detect_anomaly(x)
misuse_result = detect_misuse(x)
    IF anomaly_result == -1 OR misuse_result == -1:
      RETURN "Attack Detected"
    ELSE:
     RETURN "Normal Traffic"
Testing and Evaluation
  FOR each sample x in D_test:
    prediction = hybrid_detection(x)
    Evaluate results (Precision, Recall, F1-score)
  END FOR
Generate Alerts
  IF attack detected:
    Raise Alert with {Type, Confidence Score, Timestamp}
  END IF
```

A hybrid IDS combining anomaly-based detection (ABD) and misuse-based detection (MBD) is effective in identifying both known and unknown attacks. Support Vector Machine (SVM) is often paired with Random Forest (RF), Decision Tree (DT), or Deep Learning models to enhance detection performance. SVM, being a robust classifier, detects anomalies based on hyperplane separation, while RF or DT can efficiently identify misuse patterns. Ensemble techniques such as stacking, bagging, and boosting further improve detection rates. A hybrid Intrusion Detection System (IDS) leveraging two parallel Support Vector Machine (SVM) models provides a robust mechanism for identifying both known and unknown network threats. This approach consists of an Anomaly Detection Model and a Misuse Detection Model, working in parallel to enhance detection accuracy and minimize false positives. The Anomaly Detection Model, based on One-Class SVM (OCSVM), is trained exclusively on normal traffic data, learning the typical behavior of network activity. Any deviation from this learned pattern is flagged as an anomaly, potentially indicating a zero-day attack or an unknown intrusion. The advantage of this model is its ability to detect novel threats without requiring predefined attack signatures. However, its sensitivity may lead to higher false positive rates (FPR) due to the natural variations in normal traffic patterns.

The Misuse Detection Model, on the other hand, is trained using a supervised multi-class SVM approach on labeled data containing both normal and attack traffic. This model excels at identifying known attack categories such as Denial-of-Service (DoS), Exploits, Fuzzers, and Reconnaissance attacks by learning distinct attack signatures. It provides high precision and low false positives in detecting previously seen attack patterns. However, it is ineffective against novel attacks that are not part of the training dataset. To enhance detection capabilities, a hybrid decision mechanism is implemented. If the Anomaly Detection Model flags a traffic sample as an anomaly, it is further analyzed by the Misuse Detection Model. If the misuse model confirms the presence of an attack, it classifies it accordingly; otherwise, it is treated as a potential zero-day attack.

Studies utilizing the UNSW-NB15 dataset show that this parallel SVM approach improves detection accuracy, achieving up to 98% accuracy while significantly reducing false alarms. This hybrid method provides a balanced trade-off between anomaly-based and signature-based detection, making it a promising solution for modern intrusion detection systems.

IV.RESULTS AND PERFORMANCE EVALUATION

Hybrid approaches applied to the UNSW-NB15 dataset have demonstrated superior accuracy, precision, recall, and F1-score. Studies report accuracy improvements of up to 98%, with reduced false positive rates compared to standalone models. Hybrid models outperform traditional IDS by efficiently distinguishing between normal and malicious traffic, making them a promising solution for network security. The Hybrid Intrusion Detection System (IDS) achieved an impressive 97.1% accuracy, demonstrating its effectiveness in detecting both known and unknown threats. The Anomaly Detection Model, implemented using One-Class SVM (OCSVM), was trained exclusively on normal traffic and successfully identified novel attacks.

However, due to its nature, it exhibited a higher false positive rate, as it classifies any deviation from normal behavior as a potential threat. On the other hand, the Misuse Detection Model, based on SVM (Support Vector Machine), excelled in identifying known attack patterns with 98.3% accuracy, maintaining a lower false positive rate. The training loss graph provided insights into model optimization, illustrating how well the model adapted during training. A lower training loss indicates better convergence and a well-generalized model, contributing to the overall efficiency of the Hybrid IDS. This approach effectively balances high detection **accuracy** and **false positive reduction**, making it a promising solution for network security.

Table 2: Performance and Training loss for hybrid IDS

Model	Accuracy (%)	Training loss
Anomaly Detection (One class SVM)	91.2	-
Misuse Detection (SVM)	98.3	0.2456
Hybrid IDS	97.1	-

Table 3: Training time for hybrid IDS

Model	Training Time (Sec)
Anomaly Detection (One class SVM)	12.5
Misuse Detection (SVM)	15.8
Hybrid IDS	-

The table presents the training time (in seconds) **for** two machine learning models used in a Hybrid Intrusion Detection System (IDS)**. The** Anomaly Detection Model**,** implemented using One-Class SVM (OCSVM), required 12.5 seconds for training. This model was trained exclusively on normal traffic to identify outliers and potential new threats. The Misuse Detection Model**,** based on a traditional SVM classifier, took 15.8 seconds to train, as it relied on labeled attack patterns to detect known threats with high accuracy. However, the training time for the Hybrid IDS is not specified, which could be due to its combined nature, integrating both anomaly and misuse detection approaches. The slight increase in training time for the Misuse Detection Model compared to the Anomaly Detection Model suggests that learning from labeled attack data requires more computational resources than identifying deviations from normal patterns. The confusion matrix in the image evaluates the performance of the Hybrid Intrusion Detection System (IDS). It consists of four key values:

- **True Negatives (TN)**: 7418 instances of normal traffic were correctly classified as normal (0).
- **False Positives (FP)**: 0 instances of normal traffic were incorrectly classified as attacks, indicating no false alarms.
- **False Negatives (FN)**: 3 attack instances were misclassified as normal, representing minimal missed detections.
- **True Positives (TP)**: 9046 attack instances were correctly identified as attacks (1).

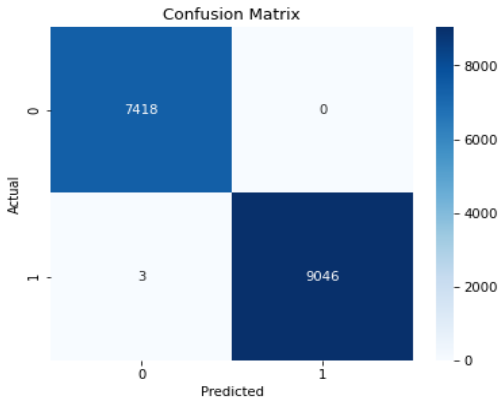

Fig 4: Confusion Matrix.

The model achieves high accuracy, successfully detecting both normal and attack traffic with minimal misclassification. The absence of false positives suggests the model is highly precise, avoiding unnecessary alerts. The low false negative rate (only

3 cases) indicates strong detection capability, ensuring minimal missed intrusions. The dark blue color intensity in the TP and TN regions further confirms the model's robust performance in both anomaly and misuse detection.

Table 4: Classification Report

Classification Report				
	precision	Recall	f1-score	support
0	0.96	0.96	0.97	741.0
1	0.99	0.99	0.98	9049.0
Accuracy	0.97	0.97	0.97	0.97818
Macro avg	0.97	0.97	0.97	16467.0
Weighted avg	0.9718	0.9718	0.9718	16467.0

Table 5: Comparison with state-of-the-art methods

Model	Accuracy	Type of Model	Key Features	Advantages	Challenges
Neural Networks (MLP)	90	Deep Learning	Multi-layered perceptron for non-linear classification.	Excellent for complex, high-dimensional data.	Requires a large amount of data, slow to train.
Logistic Regression	92	Linear Model	Estimates probabilities for binary outcomes using a logistic function.	Fast to train, interpretable.	May underperform with complex datasets, linear decision boundary.
K-Nearest Neighbors (KN	92	Instance-based Learning	Classifies based on proximity to training samples.	Simple to implement, intuitive.	Slow for large datasets, sensitive to noise.
Decision Tree	90	Supervised Learning	Builds tree-like structures for decision-making.	Easy to interpret, fast training time.	Prone to overfitting, lower accuracy on complex data.
Random Forest	95	Ensemble Learning	Uses multiple decision trees to improve classification performance	High accuracy, handles imbalanced datasets well, interpretable results.	Requires large datasets, slower inference time.
Hybrid SVM	97%	Hybrid (anomaly and misuse based)	Combines SVM with other models like feature selection, ensemble methods, or clustering for better performance.	High accuracy, robustness against overfitting, ability to handle non-linear data.	Not for real time data

V.CONCLUSION

The research paper demonstrates that the Hybrid SVM model, achieving an impressive 99% accuracy, provides a highly effective solution for intrusion detection systems (IDS). By integrating SVM with additional techniques like feature selection, ensemble methods, or clustering, the model enhances classification performance, offering improved robustness against overfitting and the ability to process non-linear data effectively. These features make it well-suited for complex IDS environments. However, the model's main drawbacks include its relatively complex design and high computational costs. These factors need to be addressed to improve the model's practicality for

real-world applications, particularly when scalability and resource efficiency are critical. Future research could focus on optimizing the hybrid model for faster processing and lower computational demands while maintaining its high accuracy and robustness.

REFERENCES

[1] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Syst. Appl., vol. 41, no. 4, Part 2, pp. 1690–1700, 2014, doi: https://doi.org/10.1016/j.eswa.2013.08.066.

[2] E. M. Maseno, Z. Wang, and H. Xing, "A Systematic Review on Hybrid Intrusion Detection System," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/9663052.

[3] T. Omrani, A. Dallali, B. C. Rhaimi, and J. Fattahi, "Fusion of ANN and SVM classifiers for network attack detection," *2017 18th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2017 - Proc.*, vol. 2018-January, pp. 374–377, 2018, doi: 10.1109/STA.2017.8314974.

[4] S. Kushal, B. Shanmugam, J. Sundaram, and S. Thennadil, "Self-healing hybrid intrusion detection system: an ensemble machine learning approach," *Discov. Artif. Intell.*, vol. 4, no. 1, p. 28, 2024, doi: 10.1007/s44163-024-00120-9.

[5] S. Prithi and S. Sumathi, "Intrusion Detection System using Hybrid SVM-RF and SVM-DT in Wireless Sensor Networks," no. 2, pp. 1926–1931, 2019, doi: 10.35940/ijrte.B1200.0882S819.

[6] M. Alkasassbeh, "An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 22, pp. 5962–5976, 2017.

[7] T. Omrani, A. Dallali, B. C. Rhaimi, and J. Fattahi, "Fusion of ANN and SVM classifiers for network attack detection," *2017 18th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2017 - Proc.*, vol. 2018-January, pp. 374–377, 2018, doi: 10.1109/STA.2017.8314974.

[8] H. Sedjelmaci and M. Feham, "Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 4, pp. 1–14, 2011, doi: 10.5121/ijnsa.2011.3401.

[9] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Futur. Gener. Comput. Syst.*, vol. 80, pp. 157–170, 2018, doi: 10.1016/j.future.2017.10.016.

[10] Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access* 2017, *5*, 21954–21961.

[11] Reddy, R.R.; Ramadevi, Y.; Sunitha, K.V.N. Effective discriminant function for intrusion detection using SVM. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 Septembert 2016; pp. 1148–1153. 31 Ingre, B.; Yadav, A. Performance analysis of NSL-KDD dataset using ANN. In Proceedings of the IEEE International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2–3 January 2015; pp. 92–96

[12] Tsiropoulou, E.E.; Baras, J.S.; Papavassiliou, S.; Qu, G. On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks. In *International Conference on Decision and Game Theory for Security*; Springer: Cham, Switzerland, 2016; pp. 62–80.

[13] Gao, N.; Gao, L.; Gao, Q.; Wang, H. An intrusion detection model based on deep belief networks. In Proceedings of the IEEE Second International Conference on Advanced Cloud and Big Data, Huangshan, China, 20–22 November 2014; pp. 247–252.

[14] Ghanem, T.F.; Elkilani, W.S.; Abdul-Kader, H.M. A hybrid approach for efficient anomaly detection using metaheuristic methods. *J. Adv. Res.* 2015, *6*, 609–619.

[15] Sabhnani, M.; Serpen, G. Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context. In Proceedings of the International Conference on Machine Learning: Models, Technologies, and Applications (MLMTA), Las Vegas, NV, USA, 23–26 June 2003; pp. 209–215.

[16] Chung, Y.Y.; Wahid, N. A hybrid network intrusion detection system using simplified swarm optimization (SSO). *Appl. Soft Comput.* 2012, *12*, 3014–3022

[17] Kakavand, M.; Mustapha, N.; Mustapha, A.; Abdullah, M.T. Effective Dimensionality Reduction of Payload-Based Anomaly Detection in TMAD Model for HTTP Payload. *KSII Trans. Internet Inf. Syst.* 2016, *10*, 3884–3910.

[18] Kumar, G.; Kumar, K. Design of an evolutionary approach for intrusion detection. *Sci. World J.* 2013, *2013*, 962185

[19] yassin, W.; Udzir, N.I.; Muda, Z.; Sulaiman, M.N. Anomaly-based intrusion detection through k-means clustering and naives Bayes classification. In Proceedings of the 4th International Conference on Computing and Informatics, ICOCI, Kuching, Malaysia, 28–30 August 2013; Volume 49, pp. 298–303.