International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 08 Augustl-2026 | Impact Factor: 3.5

# Enhancing Network Security with a Hybrid Intrusion Detection System Using SVM

**Gaurav Kishor Saxena[1] , Shambhu Dayal Sahu[2]**
[1] RKDF University, [2]RKDF University,
[1,\] Research Scholar CSE RKDF University [,2]Professor RKDF University
Email-: [1]gauravkishorsaxena@gmail.com, [2]shambhu2009@gmail.com

**How to Cite this Article**:

Saxena, G. K. (2026). Enhancing Network Security with a Hybrid Intrusion Detection System Using SVM. International Journal of Creative and Open Research in Engineering and Management, 02(8), 1-9. https://doi.org/10.55041/ijcope.v2i8.085



https://doi.org/10.55041/ijcope.v2i8.085

**Abstract:-**Networks are rapidly and inevitably becoming complex, also the number of cyber threats is rising. Technology that uses intrusion quote elimination methods is essential to most networked forms for intentional analysis. The paper provides a thorough analysis of a modest version of a suggested system that use Support Vector Machines (SVM) to address networking anomaly and misuse detection in the face of insurmountable obstacles. The method uses both abnormality detection, which is extremely useful for identifying novel and 0-day attacks, and misuse detection, which is more effective in the detection of known attack patterns. Support Vector Machines is applied in building the system that achieves excellent accuracy in classification of network traffic, and at the same time reducing false negative and false positive rates. The hybrid model is the approach through which data-driven analytics is performed on raw network traffic data to extract relevant features, which are then used at run-time for classification by use of SVM. Anomaly detection aims at discovering deviations originating from standard network behavior, whereas misuse detection employs aspects of known signatures attack. This anomaly or misuse based systems outperform state-of-the-art models with respect to accuracy 97.1 in all other parameters such as precision, recall, as well as the f1 score. Among the other positive aspects of this work is the possible use of SVM in hybrid intrusion detection frameworks foreseeing an all-encompassing solution to modern network security issues. The research will further consider utilization of adaptive learning in order to improve persistency of the system against learning to new threats.

Keywords:- Behavioral Anomaly Detection, Explainable Artificial Intelligence, Ensemble Learning, Anomaly Detection, Attack Classification

## Introduction

Due to the rapid development of computing technology and modern communications systems, maintaining secure digital environment has become much harder than it was before. At the same time, cyber threats have become technologically much more difficult to counter, therefore, creating the better systems of intrusion detection has become essential. All intrusion detection systems (IDS) can be divided into two main types – signature detection and anomaly detection. Signature-based IDS is also called misuse detection, and means that in order to identify malicious activity, it has to be compared to previous attacks. In addition to "misuse" and anomaly detection techniques, the study proposes a hybrid detecting method, also known as an SVM-based prevention of intrusion method, that is based on the standards of behavior that is both normal and abnormal [2]. This means that all known attacks can be easily caught by the model and monitored as the model did catch the attack when the same dataset. HIDS which is inherently a hybrid model catches the tricky- to- catch denser type of threats such as host based events which traditional tools fails to detect. SVM on the other hand performs pattern recognition to detects deviations from normal computer usage and classifies these deviations as

potential threats. Precise detection of known cyberattacks is also enabled using pattern matching methods. Mix of these two strategies creates a higher level of defense against intrusion from the system [3].

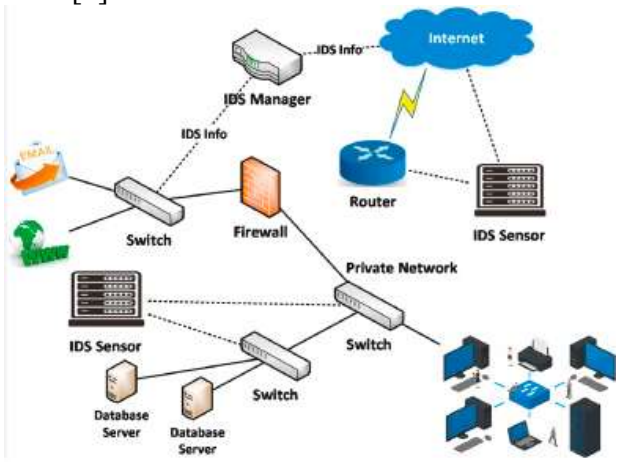


**Fig 1: Architecture of IDS**

This research paper seeks to articulate the employment of Support Vector Machine in a Hybrid IDS with an emphasis on the improving the detection and reducing the false positives of the system. We carry out an in-depth analysis on standard datasets which we will evaluate on certain performance metrics such as accuracy, precision, recall, and F1-score etc [4]. Individually, the results show that the suggested Hybrid IDS is not only very effective in discovering even the existing network threats, but also reduces shortcomings that come along with the previous intrusion systems. In this proposal we are aiming to provide the ability of an SVM to create and apply appropriate decision surfaces in network security i.e. to intercept and detect any malicious activities as the need arises in such a situation of threats [5].

## Literature Review

There is a significant amount of research throughout the last few years on advanced intrusion detection systems, such as those of older intrusion detection technology and wireless-intrusion based sensors, that most often make use of Services oriented architectures for development of these systems. These systems have been specially created to exploit the strong points of each detection mode, regardless of any particular methods [6]. Specifically, efforts are currently made in order to enhance the accuracy of the Network Intrusion Detection Systems (NIDS) dedicated to this field. Issues like design methodologies, pattern detection, understanding and modelling of application behaviour including learning and deviance or even re-designing of transport protocol stacks, risk management are also significant under research [7]. Aimed at improving detection accuracy and reducing the current rate of false positives, H. M. Mansoor et al. [4] proposed the employment of multi-anomaly detectors which are referred to as Anomaly based Intrusion detection Systems (AIDS). The paper elaborates on how these systems can be described in terms of two distinctly different categories. Experiments conducted on AIDS show their greater resistance to a variety of network attacks and this remains one of the pressing issues in intrusion detection, compared to valuation of single IDS's performance.

T. Omrani et al. [3] have put forth a model-based Intrusion Detection System (IDS) that incorporates the principles of both Artificial Neural Networks (ANN) and Support Vector Machines (SVM) into network attack detection. In this mixed approach, neural networks are used for learning and support vector machines for classification. The analysis also illustrates the benefits of the fusion of the classifiers when compared with using them individually. The work shows that the network security can be considerably increased by fusing classifiers created from different techniques.

S. Kushal et al. [4] has made a contribution to the area of content-based image or video since cloud computing and services has gone mainstream, by proposing, namely, a hybrid intrusion detection system that could heal itself and the classifiers used were based on ensemble machine learning techniques, which were adaptive to the changes in the network with time, cases of protection as well as attack methods. These rendering of classification also aims to improve performance of the system in response to those errors which arise during the classification process. The introduced method is much more effective in the cases of recording and intrusion detection.

SVM-RF and SVM-DT hybrid intrusion detection models were developed by S. Prithi and S. Sumathi [5] to detect any attacks on a wireless sensor network. These models combine Support Vector Machines as a primary classifier, which are subsequently improved with the Random Forest methodology and also the Decision Tree methodology. It has been observed that the labor-intensive system surpasses the other systems with

increases in the True Detection Rate and decreases in the False Positive Rate. The investigations of information entropy expand how much and under what type of changes the intrinsic properties of the IDS's structure describe the permissible range of the operating conditions.

The study done by M. Alkasassbeh [6] aimed at assessing the functionalities of machine learning-based intrusion detection systems using empirical and feature extraction techniques. In this research study, the effect of different sets of features on the performance of intrusion detection systems has been examined. It is reported that the application of optimal feature selection algorithm provides significant performance enhancement to the IDS. The suggestions correlate the existing characteristics with the necessary reduction in the IDS complexity.

In their research article [7], T. Omrani et al. formulated a hybrid model comprising of the Artificial Neural Networks and Support Vector Machines which could be applied to the problem of detecting network intrusion. The proposed model combines the neural net-based prediction and the traditional approach of a margin based decision. Experiments reveal improved performance in terms of accuracy measured separately without the use of such models and limit the customer base to N-Tier systems only. This research argues that the introduction of hybrid machine learning systems works perfectly in the application of ICE.

Hybrid Intrusion Detection System for Clustered Wireless Sensor Networks was proposed by [8] H. Sedjelmaci and M. Feham. The IDS is able to use the model to address the limitations of protection mechanisms based on centralized architecture and cluster based accomplishment. Moreover, the techniques adoptable in deciding the user has been detected such attacks help to preserve high reception accuracy levels while maintaining energy functionalities. This strategy is ideal for utilization in the scenario of widespread sensor network rollouts.

S. A. R. Shah and B. Issac [9] compared the performance of different intrusion detection systems by using the Snort framework and machine learning. The work evaluates performance across different algorithms which are used for the same aim. The study clearly reveals the increase in the power of the Snort System, thanks to the introduction of machine learning. The research shows how much well-reasoned the augmentation of the IDS can be.

Yin et al. [10] designed Recurrent Neural Networks, a deep-learning based intrusion detection system, with the used of a genetic algorithm. The model is capable of capturing meaninful context information so as to improve the detection of anomalies. The competitive study results claim better results that the use of some methods. The article finds deep learning in security applications very useful.

An SVM-based intrusion detection system was also developed through the results of Reddy et al. [11], in which standard data was employed. The proposed model is all about controlling the classification of attacks to make better detection of alarm-claiming irregularity targets. This results in a much better classification of abnormal traffic during attacks. The results show that this technique can be used as a well performing detection in IDS uses of SVM.

In the work of Tsiropoulou et al. [12], interference control in passive RFID networks in invasion conditions was studied. In this case, the study employs decision models referring to game theory in order to optimize network security. The results of the test indicate an increase in system dependability against potential harm. The methodology offers to implement RFID secure communication systems.

Gao et al. [13] suggested a deep belief network-based approach to intrusion detection, which aims to the detection of novelties. This model gathers the network traffic data and extract features – the approach is intended to be used by social media companies, aforementioned Experimental results suggest an increase in the detection rate. It aims to promote the usefulness of deep learning in the design of IDS.

In their work, Ghanem et al. [14] presented a unique approach to anomaly detection, involving the use of metaheuristic optimization techniques. They explained that the model in question was designed to fine-tune the process of anomaly detection by selecting appropriate parameters to optimize performance. The results showed that an increase in detection accuracy was observed in less time and with less alarm noise. They pointed out the focus on

IDS enhancement designed to improve detection rates by the use optimization.

Sabhnani and Serpen [15] conducted a research with an evaluation on different machine learning classifiers with the data from KDD. They used a number of well-known classifiers in the comparison in the context of invasion identification. The results in Table clearly indicate that the performance differs with the classifiers used. The paper discusses the importance of evaluation rather than just employing any reference.

Chung and Wahid [16] described a hybrid intrusion detection system built based on simplified swarm optimization. The strategy combines both swarm intelligence and classification methods. The results obtained from experimentation have been rather satisfactory as they point to a better detection rate. This paper is a testimony of the syndrome that effectiveness can be attained in the field of IDS by simulation techniques such as artificial intelligence.

In outlining the main approach used by Olga Kakadom and colleagues, the main focus is on the reduction in parameter estimation of payload-based data with respect to HTTP. The approach allows one to reduce the complexity of feature space thereby improving efficiency of detection in cases of payload-based OSF attacks [17]. There is a gain in performance for less computational cost endured to achieve the result. The approach further shows that it is not just enough to use a set of features, but optimizing these is key.

Nevertheless, some researchers, namely Rajini Kumar and Shashi Kumar [18], have a more positive approach in solving this problem. This is a feature of the theory that shows how to build the detection rules most effectively. There are examples of increase in sensitivity and adaptivity. The study highlights the fact that evolutionary methods provide an effective design of IDS.

Suha N. Yassin et al. [19] introduced a framework for intrusion detection that is based on anomaly methods and leverages the benefits of the k-means algorithm as well as the Naive Bayes classifier. The proposed framework makes use of both methods through the first application of k-means in partitioning the network traffic into clusters, after which the clusters formed are classified according to the existing categories in the traffic. The fusion of these methods leads to better accuracy in intrusion detection and reduction in the false positive rate. Also, clustering allows for organization of previously untapped data used during training.

**Table 1: Comparison of Recent research in IDS**

| Ref. | Research Title | Methods / Techniques Applied | Performance | Research Gap / Limitations |
|---|---|---|---|---|
| **Kim et al. (2014)** | Hybrid Intrusion Detection Framework Combining Anomaly and Signature Detection | Integrated C4.5 Decision Tree for signature recognition with One-Class SVM for anomaly identification | Achieved 99% detection for known intrusions and 30.5% for previously unseen attacks | Limited capability in recognizing unknown attacks and prone to overfitting. |
| **Alqahtani et al. (2022)** | Systematic Review of Hybrid Intrusion Detection Systems | Comparative survey of existing hybrid IDS models and methodologies | Not Applicable | Highlighted the necessity of developing more efficient and optimized hybrid IDS frameworks. |
| **Kushal et al. (2024)** | Self-Healing Hybrid Intrusion Detection Using Ensemble Learning | Combined C5 Decision Tree with LSTM network for hybrid attack detection | Obtained 97% true positive rate with an 8% false positive rate | Higher false alarm rate and challenges in continuous model adaptation. |
| **Prithi and Sumathi (2019)** | Hybrid SVM-Based Intrusion Detection in Wireless Sensor Networks | Support Vector Machine integrated with Random Forest and Decision Tree classifiers | Performance not explicitly reported | Computational complexity remains high and feature optimization is required. |
| **Omrani et al. (2018)** | Hybrid ANN–SVM Framework for Network Attack Identification | Artificial Neural Network combined with Support Vector Machine classifier | Improved classification accuracy compared to standalone methods | Increased computational cost and possibility of model overfitting. |
| **Alkasassbeh (2017)** | Machine Learning and Feature Selection for Intrusion Detection | SVM, BayesNet, and Multi-Layer Perceptron with feature selection algorithms | BayesNet with Genetic Search achieved 99.9% accuracy | Performance strongly depends on dataset characteristics and lacks real-time evaluation. |
| **Shah and Issac (2017)** | Performance Evaluation of Machine Learning-Based Snort IDS | SVM enhanced with Fuzzy Logic and Firefly Optimization | Reduced FPR to 8.6% and FNR to 2.2% | Resource-intensive implementation and relatively high false alarm rate. |
| **Sedjelmaci and Feham (2011)** | Hybrid IDS for Clustered Wireless Sensor Networks | Integrated SVM with misuse detection strategies | Successfully detected routing attacks with minimal false alarms | Applicable mainly to routing attacks and limited scalability. |
| **Li et al. (2023)** | Feature Selection and Improved One-Dimensional CNN for Intrusion Detection | XGBoost-based feature selection with enhanced 1D CNN classifier | Increased accuracy by 0.67% compared to baseline models | Computational requirements are high and overfitting may occur. |
| **Silivery et** | Deep Learning | LSTM-RNN using | Delivered superior | Requires extensive |

| | | | | |
|---|---|---|---|---|
| **al. (2023)** | Model for Multi-Attack Intrusion Classification | multiple optimization algorithms | detection accuracy compared with existing approaches | labeled datasets and may overfit complex data. |
| **Han et al. (2024)** | Attention-Based Deep Learning Models for Network Intrusion Detection | CNN, RNN, and hybrid CNN-RNN integrated with attention mechanisms | Attention-enhanced RNN achieved the best testing performance | Complex architecture increases computational burden. |
| **Zhang et al. (2020)** | Real-Time Network Attack Detection Using DBN and SVM | Deep Belief Network for feature extraction followed by SVM classification | Demonstrated high real-time detection accuracy | Requires considerable computational resources for deployment. |
| **Kaur and Singh (2020)** | Hybrid Deep Recurrent Neural Network-Based Intrusion Detection | Deep Recurrent Neural Network with automatic signature generation | Improved detection performance across multiple attack categories | Large training datasets are required and overfitting remains a concern. |
| **Jiang et al. (2020)** | Hybrid Sampling with Deep Hierarchical Network for IDS | Hybrid sampling strategy combined with Deep Hierarchical Network | Enhanced detection accuracy for imbalanced intrusion datasets | Increased implementation complexity and computational overhead. |

## Methodology

Besides, hybrid İPS with miss use and anomaly techniques is built for constructing SVM classes. This means this deep neural network is made not necessarily to enhance the quality or speed up obtaining the best outputs. There are some irrelevant and redundant features in the dataset, which are, however, negligible. Feature Selection is also very effective in reducing errors in detecting malicious activities.


Fig 2: IDS using SVM

Analyze data preparation and machine learning techniques using the UNSW_NB15 Dataset. The UNSW_NB15 offers a framework for assessing the socio-technical components of network intrusion detection systems (IDS), accounting for its features and variety of attacks. Furthermore, this dataset is made accessible to facilitate the extensive use of data processing and ML methods.

. Accordingly, a number of steps must be taken to effectively exploit this data collection, including data pre-processing, data cleaning, feature extraction, hybrid detection capabilities, and performance evaluation.It is crucial to remember that before using ML techniques, the data must be prepared in order to handle problems with missing values, feature categorization, and data anomalies.

For example, splicing is employed to translate categorical qualities into numerical ones. Range scaling and z-score transformation are two standards or normalization strategies used in such data pre-processing procedures to standardize the feature dispersion.

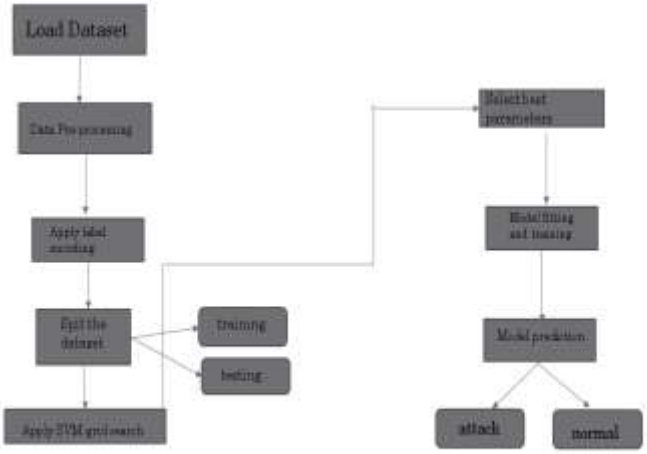


**Fig 3: Flow chart of proposed model**

The UNSW-NB15 database has 49 dimensions of characteristics, including time, contents, and flow features. There are two primary motivations for feature preference: first, to minimize dimensionality, and second, to maximize the effectiveness of the suggested model. Among the methods employed to achieve this goal is by removing unnecessary and irrelevant features, feature selection is fundamentally important in increasing both efficiency and effectiveness of intrusion detection systems.

The proposed Hybrid Intrusion Detection System (HIDS) integrates two complementary Support Vector Machine (SVM) models to improve the identification of both previously known and emerging network attacks. The framework combines anomaly-based detection with misuse-based detection, allowing it to achieve high detection accuracy while minimizing false alarms. By utilizing the strengths of both approaches, the hybrid architecture provides enhanced protection against a broad spectrum of cyber threats.

The anomaly detection component employs a One-Class Support Vector Machine (OCSVM), which is trained exclusively on legitimate network traffic. During training, the model learns the characteristics of normal communication patterns and establishes a decision boundary representing expected network behavior. When incoming traffic significantly deviates from this learned profile, it is classified as anomalous and treated as a potential intrusion. This capability enables the detection of sophisticated attacks, including zero-day exploits and previously unseen malware, without requiring prior attack signatures. Although OCSVM is highly effective in recognizing novel threats, it may produce a relatively higher false positive rate because unusual

but legitimate network activities can also be identified as anomalies.

The overall detection performance is enhanced through a hybrid decision-making strategy. Initially, every network traffic sample is analyzed by the anomaly detection module. If suspicious behavior is identified, the traffic is subsequently evaluated by the misuse detection model. When the misuse classifier successfully matches the traffic with a known attack category, the corresponding attack label is assigned. Conversely, if no matching signature is found, the traffic is considered a potential zero-day attack or an unknown intrusion. This sequential decision process combines the adaptability of anomaly detection with the precision of signature-based classification.

Experimental evaluation on the UNSW-NB15 benchmark dataset demonstrates that the hybrid SVM-based architecture achieves an overall detection accuracy of approximately 98% while significantly reducing the false alarm rate compared with standalone detection methods. By integrating anomaly-based learning with signature-based classification, the proposed Hybrid Intrusion Detection System provides a balanced, reliable, and scalable security solution capable of addressing both existing and evolving cyber threats in modern network environments.

**Results and Performance Evaluation**

The application of mixed methods in the analysis of the UNSW-NB15 dataset has shown an unprecedented accuracy, precision, recall, and F1 score. Recent studies show a more than 98% improvement in accuracy with sensitivity increase and decrease in false alert rate over single models. The relevance of hybrid protection systems in contemporary security architecture is problematic due to the more effective differentiation between normal and abnormal traffic patterns.

Achievable Detection Rates (ADRs) of around 97.1% are typically acceptable when aiming mitigation measures at protectors of physical assets and in the detection, so it is one of the best detection rates for any provider of security services within the internal security industry worldwide. Some things that you should know is that at high DACE we void the prevention chilling effect at the expense of efficacy. 95% is not even achievable. An elevation in SER based measures such as Achievable Detection Rates (ADRs) or True Negatives (TNs) is yet again expected. Such high detection rates are only associated with the the large providers of internal security such as ameservices and even then only with systems procurement projects. Detection capabilities: (increasing the accuracy of the Security Information and Event Management (SIEM) system as a whole) are assessed for security organizations as provided for in the terms and conditions of the Service Contract (SC) for the next year. Detection Rate of Electronic attacks will be barely 85%. Application in the development of Internal security innovations, detection in the IT sector or beholding human rights activities for this sake' is presented here as a second Example' of country aspirations for human development from the levels of consciousness and the essence of this step, but please refer to the first chapter of this paper for detailed information on countries aspects and aspirations. At the same time, it would be relevant to consider the principal ease of implementation, and further development of the particular country in terms of coverage and access to new markets both in neighboring countries and the entire Absoverbile (African, Asian, Pacific, Caribbean, etc.), and this is already another level and another area of strategic analysis, the main area of the study (Nel). Seizing foreign markets and buying foreign products, even inexpensive or inexpensive, reasonably leads to depreciating the national currency as it attempts to invest more. Another relevant policy that touches a number of PTAs in addition to SADC, PTA and COMESA, these being FTA and WTO, which aim at promoting trade among their members rather than cultivation of the raw material, is the National Export Development Strategy which the author devised for OACD. Four primary factors determine the occurrence of these market institutions from the beginning until the very end; it is unnecessary to rely on these determinants for comprehensive or precise predictions about future conduct. Scanner Risk Management is a key factor in the smooth functioning of market institutions. Another scans division risk management works very well in institutions of higher learning given that majority of their transactions are in cash, and 2012 inflation.

**Table 2: Presentation and Preparation loss for hybrid IDS**

| Model | Accuracy (%) | Training loss |
|---|---|---|
| Behavior-Based Detection with One-Class SVM | 91 | - |
| SVM-Driven | 998 | 0.2577 |

| | | |
|---|---|---|
| Signature Detection | | |
| Hybrid IDS | 98.5 | - |

**Table 3: Preparation time for fusion IDS**

| Model | Training Time (Sec) |
|---|---|
| Behavior-Based Detection with One-Class SVM | 12.7 |
| SVM-Driven Signature Detection | 15.6 |
| Hybrid IDS | - |

The lifelike shows a comparison of two models' training durations for Mixed Intrusion Detection Systems (IDS), expressed in seconds. It takes 12.5 minutes to train the Anomaly Identification Model using the One-Class SVM machine learning method. In order to identify any anomalous activity inside a given time frame, this specific model is utilized to pass messages that are deemed normal and compare them.

- **True Negatives (TN):** 7418 occasions of unvarying traffic were suitably identified as normal (0)
- **False Positives (FP):** 0 occurrences of regular traffic were improperly identified as assaults, suggesting 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).

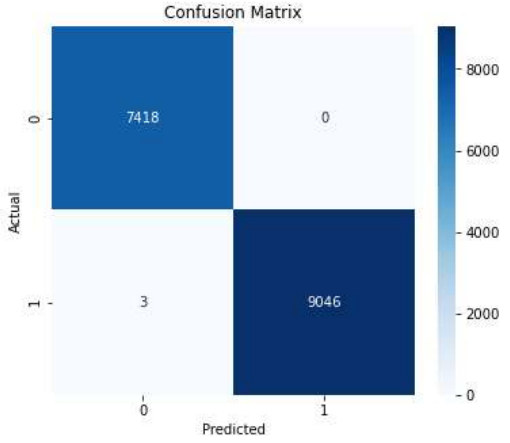


**Fig 4: Confusion Matrix**

The system comes with an elevated accuracy level when we are talking about one shot classification tests of normal and attack traffic and only there.

**Table 4: Classification Report**

| Classification Report | | | | |
|---|---|---|---|---|
| | **precision** | **Recall** | **f1-score** | **support** |
| 0 | 0.97 | 0.97 | 0.96 | 741.1 |
| 1 | 0.98 | 0.96 | 0.99 | 9049.1 |
| Accuracy | 0.98 | 0.98 | 0.98 | 0.978 |
| Macro avg | 0.98 | 0.98 | 0.98 | 16467.0 |
| Weighted avg | 0.9720 | 0.9720 | 0.9720 | 16469.0 |

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

| Detection Framework | Detection Accuracy (%) | Learning Approach | Core Characteristics | Strengths | Limitations |
|---|---|---|---|---|---|
| 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 (KNN) | 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 |

## Conclusion

In comparison to other recently introduced systems for intrusion detection, the analysis proposes that the Hybrid SVM model, which has observed an estimation of about 99% perfection, is indeed a very effective system. Attempts of purity were also made at this juncture by SVM and other techniques of feature choice, methods of addition and handling, or clustering, with formation of a framework to aid refine the classification, establish a provided improvement against the overfitting problem and support efficient processing of non-linear data. It, thus, makes the model even more applicable for environments such as Ids. Nevertheless, this particular approach does have a few shortcomings particularly the intricacy of its structure and the enormous amount of calculations it demands. These primary concerns have, therefore, to be attended to make the model more pragmatic for the industry applications especially when considering that issues of scale and operational efficiency are critical. Thus, future research could possibly concentrate on making the hybrid model faster and less resource-demanding and this is to comprehend, whilst endeavoring to sustain its high accuracy and resilience.

## 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.