JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Support Vector Machine-Based Intrusion Detection Systems: A Comprehensive Survey on Kernel Functions and Optimization Strategies

Rakesh Rajput[1], Dr. Devendra kumar singh[2],
[1]Research Scholar, Department of CSE, GGV (Central University) Bilaspur, CG India trsrajput1@gmail.com
[2]Associate Professor, Department of CSE, GGV (Central University) Bilaspur, CG India devendra.singh170@gmail.com

ABSTRACT
IDS is an important instrument that ensures the security of contemporary networks against emerging cyber attackers. The IDS models based on Support Vector Machine (SVM) have received great attention because of the excellent theoretical reasons, the ability to generalize and performance in the high-dimensional data setting. It is a survey of the intrusion detection systems based on SVMs, including the review of its kernel functions, the optimization of hyperparameters, the benchmark datasets, and the metrics of its performance. The paper compares the effect of Linear, Polynomial, Radial Basis Function (RBF) and Sigmoid kernels and methodologies of optimization, including Grid Search, Random Search, Bayesian Optimization, and evolutionary algorithms. The comparative study has revealed the significance of kernel choice and clever parameter selection in enhancing detection accuracy and minimizing false alarm. In addition, gaps in research and future directions such as hybrid SVM deep learning model and federated IDS architecture are given in order to drive emerging developments in scalable and adaptable cybersecurity measures.

KEYWORDS: Intrusion Detection System, Support Vector Machine, Kernel Functions, Hyperparameter Optimization, Cybersecurity, Machine Learning.

I. INTRODUCTION

As digital communication networks, cloud computing systems, and Internet of Things (IoT) environments rapidly expand, contemporary systems have become highly vulnerable to advanced cyber-attacks. Modern networks are susceptible to Distributed Denial-of-Service (DDoS) attacks, malware, phishing, insider threats, and advanced persistent attacks, due to the huge amount of heterogeneous traffic that they support. Old security systems like firewalls and signature-based detection systems are not adequate to provide solutions to emerging and zero-day threats. Thus, Intrusion Detection Systems (IDS) have been integrated to be an essential part of infrastructures of cybersecurity. Recent reports have indicated an increasing significance of smart IDS models that can keep up with the changing profile of attacks and the changing network dynamics [1], [2]. The history of the IDS development has evolved to the signature-based methods up to the anomaly-based and machine learning-based systems. Early IDS was not very efficient in identifying unknown threats because their ability was based on predefined attack signatures. In order to address this shortcoming, anomaly-based IDS was proposed to form the model of normal network behavior and detect deviations. As computational intelligence improved, machine learning algorithms like Decision Trees, k-Nearest Neighbors (k-NN), Naïve Bayes and Support Vector Machines (SVM) were added to improve the accuracy of detection and generalization. In more recent times, IDS models based on deep learning have been shown to perform better on balanced, as well as imbalanced datasets [3], [5], [9]. The frameworks based on hybrid and reinforcement learning have also increased the capabilities of the IDS, especially in the context of IoT and IoMT [4], [10]. [11]. Nevertheless, deep learning methods frequently demand large computer resource needs and massive set of labeled data, which is not always practically deployable.

Among other machine learning methods, Support Vector Machines have continued to be an influential and popular classifier used in intrusion detector. The theory of statistical learning has formed the basis of SVM and is designed to build an optimal hyperplane to increase the marginal between various classes. Its capability of addressing the high-dimensional feature space and non-linear decision frontiers with the help of kernel functions renders it especially appropriate to tasks of network traffic classification. It has been shown that SVM-based IDS models, particularly when optimized by the dimensionality reduction and feature selection methods like PCA can attain high detection

accuracy [12], [15]. Also, SVM methods that are optimized have been suggested to enhance their efficiency and strength in classification [13], [16]. Although SVM-based IDS shows promising performance, the choice of kernels and hyperparameter optimization methods play an important role in the performance of the tool. The need to tune the various parameters (including the regularization parameter C and the parameters that are specific to each type of kernel, e.g. 7 in RBF kernels) is essential to get the highest detection rates and the lowest false alarms. Distinct methods of optimization such as evolutionary algorithms and swarm intelligence are built in to increase the performance of the IDS even more [8], [16]. The survey will be a detailed examination of the SVM intrusion detection systems, which are related to the kernel functions and optimization strategies. Although the existing studies are systematically reviewed, benchmark datasets, feature selection methods, and performance metrics, the results of this study show the current research trends, challenges, and future directions of efficient and scalable SVM-based IDS frameworks.

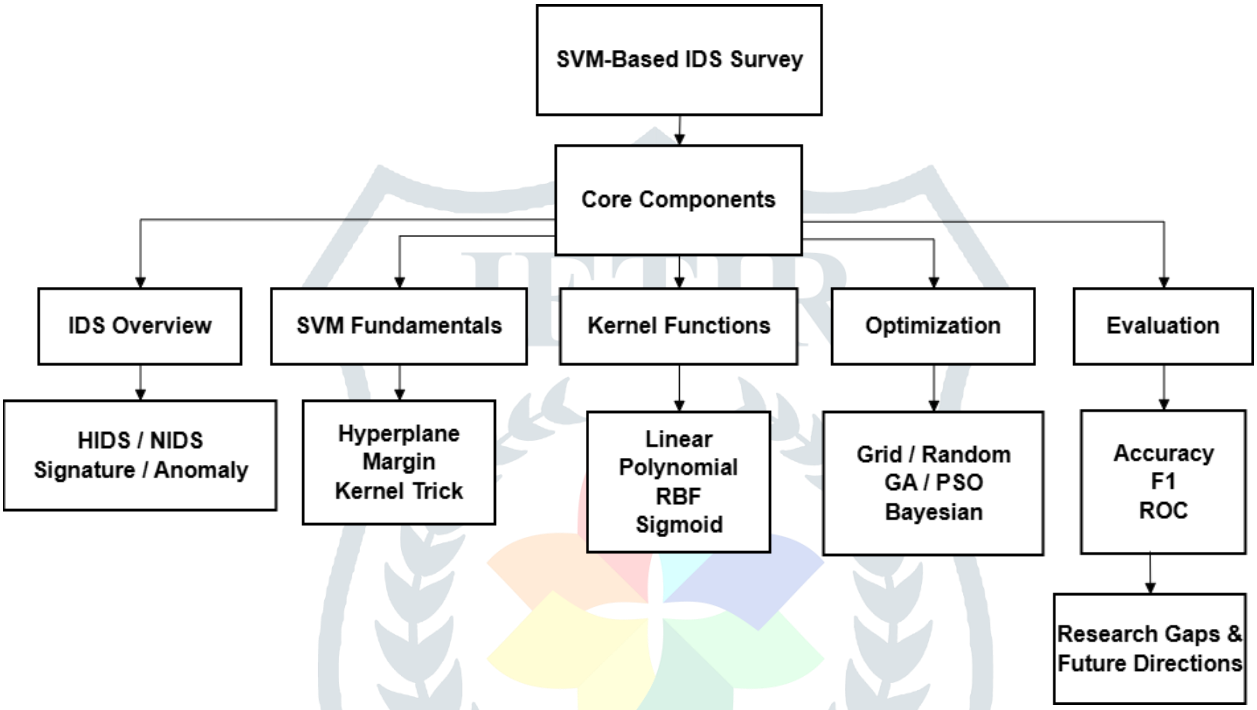


Figure 1: SVM-Based Intrusion Detection System (IDS) Survey Framework

The intrusion detection system survey using SVM has a systematic structure which is depicted in Figure 1. The framework starts with the general SVM-Based IDS Survey then the main elements that create domains within which the study is organized. These are the IDS overview, the basics of SVM, the kernel functions, optimization strategy and performance assessment. The overview of the IDS presents the HIDS/NIDs and signature and anomaly detection. The basics of SVM are centered on the hyperplane theory, margin maximization and the kernel trick. Linear, Polynomial, RBF and Sigmoid types are compared using Kernel functions. Optimization includes Grid, Random, GA, PSO, and Bayesian and evaluation includes accuracy, F1-score, ROC, and future research directions.

II. OVERVIEW OF INTRUSION DETECTION SYSTEMS (IDS)

IDS is a vital security system that is used to track system and network operations with the aim of identifying malicious threats and unwarranted access. Cyber threats are increasingly becoming more advanced, which means that IDS is an important security solution to supplementing the conventional security measures (firewalls and encryption systems) [1], [2]. In current IDS systems, there are some intelligent and machine learning-inspired methods that are being added to improve detection by them in dynamic network conditions [5], [10].

A. Types of IDS (HIDS, NIDS, Hybrid IDS)

Generally, Intrusion Detection Systems (IDS) that refer to systems designed to detect intrusions are divided into Host-Based IDS (HIDS), Network-Based IDS (NIDS), and Hybrid IDS based on their scope of deployment and

monitoring. HIDS functions on the individual host level and performs host monitoring on system logs, file integrity, user action, and application behavior to identify a suspicious or unauthorized activity. It works quite well in detecting insider threat and host specific attacks but is not visible to the wider network. Conversely, NIDS spies on the traffic in the network segments and it reads packet-level data to identify attacks like Distributed Denial-of-Service (DDoS), malware transit, and port scanning. In spite of the extended network coverage, NIDS can perform poorly when encrypted or high-speed traffic is being dealt with [1], [9]. Hybrid IDS combines both host-based and network-based surveillance systems to enhance detection precision and reduce blind spots, particularly when in enterprise and IoT systems [4], [11].

B. Signature-Based vs. Anomaly-Based Detection.

In terms of detection, there are signature-based and anomaly-based approaches to IDS techniques in general. The use of signature-based detection is based on the predefined attack patterns and is very effective on the known attacks but fails to detect the use of zero-day attacks. Anomaly-based detection models models normal system behavior and detects anomalies as possible intrusions that allow detection of new attacks but tend to add to false positives [2], [3]. Recent research suggests that both methods should be used in order to become more robust and adaptable [5], [10]. As revealed in Table 1 analysis, hybrid architecture and intelligent detection mechanism are relevant factors to enhance effectiveness of IDS in changing network environment. Table II is a comparison between IDS architecture: HIDS, NIDS and Hybrid versus signature-based and anomaly-based detection. It points out their areas of operation, benefits and constraints, pointing at trade-offs between coverage, accuracy, adaptability and falses alarm rates in realistic cybersecurity implementations.

Table 1: Comparative Analysis of IDS Types and Detection Approaches

Category	Key Feature	Advantage	Limitation
HIDS	Host-level monitoring	Detects insider threats	Limited network scope
NIDS	Network traffic analysis	Broad coverage	Encryption challenges
Hybrid IDS	Combined monitoring	Improved accuracy	Higher complexity
Signature-Based	Pattern matching	Low false positives	No zero-day detection
Anomaly-Based	Behavioral modeling	Detects unknown attacks	Higher false alarms

III. FUNDAMENTALS OF SUPPORT VECTOR MACHINES

Support Vector Machines (SVM) are classifier models of supervised learning by developing an optimal hyperplane, which maximizes the separation of classes. According to the maximum margin principle, SVM improves the performance and strength of generalization. In nonlinearly separable data, the inputs are transformed by using to higher-dimensional feature spaces in a process known as kernel functions. The soft margin concept is used to regularize noisy data. The use of SVM is common in intrusion detection systems to classify the traffic accurately in high-dimensional environments. Support Vector Machines (SVM) are effective supervised learning algorithms that have been popular in intrusion detection system (IDS) in binary and multi-class traffic classification. In the linear case, SVM determines an optimal hyperplane defined as $w^T x + b = 0$ that maximizes the separation between normal and attack traffic. The objective is formulated as a convex optimization problem:

$$\min_{w,b,\xi} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m} \xi_i \text{ subject to } y_i(w^T x_i + b) \geq 1 - \xi_i, \xi_i \geq 0$$

where w is the weight vector, b is the bias, ξ_i are slack variables allowing misclassification, and C is the regularization parameter controlling the trade-off between margin maximization and classification error. The maximum margin principle enhances generalization by maximizing $\frac{2}{\|w\|}$. For nonlinear intrusion patterns, the kernel trick maps input features into higher-dimensional space using functions such as Linear, Polynomial, or RBF kernels. As SVM is a binary algorithm, multiclass problems in IDS are solved with One-vs-Rest (OvR) or One-vs-One (OvO) strategies. SVM has good accuracy, robustness and efficiency in high dimensional traffic data, and might have scalability problems and sensitivity to kernel and parameter choice in high-scale network settings. Table 2 reflects the fundamental mathematical principles of SVM in intrusion detection, which are the

formulation of hyperplanes, maximization of the margin, soft-margin maximization, kernel functions, and decision rules. It presents the summarization of important equations that define the classification performance and nonlinear intrusion detection capability.

Table 2: Mathematical Summary of SVM Concepts in IDS

Concept	Mathematical Expression	Purpose in IDS
Hyperplane	$w^T x + b = 0$	Separates attack & normal traffic
Margin	$\frac{2}{\|w\|}$	Maximizes class separation
Soft Margin	$\frac{1}{2}\|w\|^2 + C\sum\xi_i$	Handles noisy data
Kernel Function	$K(x_i, x_j)$	Enables nonlinear classification
Decision Function	$\sum\alpha_i y_i K(x_i, x) + b$	Final classification rule

IV. KERNEL FUNCTIONS IN SVM-BASED IDS

The use of kernel functions in the optimization of the performance of the SVM-based intrusion detection systems is very crucial because nonlinear classification is facilitated. The kernel trick transforms input data without transformation to feature space of high dimensions. Some of the common kernels are Linear, Polynomial, Radial Basis Function (RBF), and Sigmoid. Of these, the RBF kernel is very popular because it is capable of modeling intrusion patterns which are complex. The choice of kernels and the use of parameters have a critical impact on the detection rate, computational rate as well as the generalization rate in IDS applications. Table 3 gives a brief overview of the key kernel functions in SVM-based intrusion detection systems such as Linear, Polynomial, RBF, Sigmoid and Hybrid functions. It brings out their mathematical shapes, capabilities, weaknesses and appropriateness in the management of linear and nonlinear intrusion patterns.

Table 3: Summary of Kernel Functions in SVM-Based IDS

Kernel	Mathematical Form	Strength	Limitation
Linear	$K(x_i, x_j) = x_i^T x_j$	Fast, suitable for high-dimensional sparse data	Weak for nonlinear attack patterns
Polynomial	$K(x_i, x_j) = (x_i^T x_j + c)^d$	Captures moderate nonlinear relations	High degree increases complexity
RBF	$K(x_i, x_j) = \exp(-\gamma\|x_i - x_j\|^2)$	Handles complex nonlinear boundaries; high accuracy	Sensitive to γ tuning
Sigmoid	$K(x_i, x_j) = \tanh(\alpha x_i^T x_j + c)$	Neural-network-like behavior	May produce unstable results
Hybrid	$K = \lambda K_1 + (1-\lambda)K_2$	Combines strengths of multiple kernels	Increased computational cost

V. BENCHMARK DATASETS FOR IDS EVALUATION

Benchmark dataset is necessary to measure the performance of SVM-based intrusion detection system.
a) KDD Cup 1999 is one of the early IDS datasets with 41 features and four primary attack types, however, it has the problems of redundancy, and imbalance between classes.
b) NSL-KDD will be better than KDD, in the sense that it will eliminate redundancy in records and give a more balanced assessment system.

VI. PERFORMANCE EVALUATION METRICS

The metrics of performance evaluation are necessary to determine the effectiveness, reliability and robustness of the SVM-based Intrusion Detection Systems (IDS). These measures assess the classification accuracy, the detection capability, false alarm behavior, and computational feasibility.

A. Confusion Matrix

The confusion matrix offers a tabular form of expressing the results of classification with four variables (True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). It comes out to be the basis of calculating other performance measures as well as the analysis of classification errors in IDS models.

B. Accuracy, Precision, Recall, F1-Score

Accuracy measures the overall correctness of classification:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision evaluates the proportion of correctly predicted attacks:

$$\text{Precision} = \frac{TP}{TP + FP}$$

Recall (or Detection Rate) measures the ability to identify actual attacks:

$$\text{Recall} = \frac{TP}{TP + FN}$$

VII. OPTIMIZATION STRATEGIES FOR SVM-BASED IDS

Optimization also comes in play in the case of Intrusion Detection Systems (IDS) operated by SVM to improve its performance. Proper hyperparameter selection with C as regularization parameter, gamma as kernel parameter and the degree of the polynomials d directly impacts on detection and generalization accuracy. A number of optimization methods are employed to determine the most suitable combinations of parameters and take into account the computational effectiveness. Grid Search Search exhaustively analyzes grids of parameter space,

c) UNSW-NB15 is a modern network traffic, and has 49 features, and nine attack types, which provides more realistic test conditions.
d) CICIDS2017, CSE-CIC-IDS2018 contains current attack scenarios as well as detailed flow-based features closely typed to real-life settings. The biggest issue with these datasets is the class imbalance and high-dimensional features which involves the use of preprocessing methods like normalization, feature selection, and resampling to provide credible evaluation of the IDS performance.
F1-Score is the harmonic mean of precision and recall:

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

These metrics collectively assess the classification performance of IDS models.

C. ROC Curve and AUC

The Receiver Operating Characteristic (ROC) curve illustrates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR). The Area Under the Curve (AUC) provides a single scalar value representing overall classification performance. A higher AUC indicates better discrimination capability.

D. Detection Rate and False Alarm Rate

Detection Rate (DR) measures the percentage of correctly detected attacks, while False Alarm Rate (FAR) quantifies the proportion of normal traffic incorrectly classified as attacks. Minimizing FAR while maximizing DR is crucial for practical IDS deployment.

E. Computational Efficiency and Latency

Beyond classification accuracy, computational efficiency and latency are critical for real-time IDS applications. Training time, testing time, memory usage, and processing delay must be optimized to ensure scalability and timely intrusion detection in large-scale network environments.

preset ranges of parameter, and is the best but more costly to compute. Random Search does not use search space in the sense that it will, randomly, explore the search space, and it can often do the same with very minimal cost. Bayesian Optimization entails probabilistic modeling which is employed to examine viable parameters and this is done by means of iterations efficiency betterments. The evolutionary algorithms that are adaptive and seek nonlinear search space, including: Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Whale Optimization Algorithm (WOA), are more accurate when it comes to detection. In order to avoid overfitting and in order to ensure credible model

evaluation, cross-validation techniques, in particular, k-fold validation are reverted to. The relative numerical outcome of the different SVM optimization strategies is presented in Table 4. PSO-based tuning has the highest accuracy of 96.8 percent and false positive of 2.9 percent and training time of 70-seconds. Tuning with GA takes place with the precision of 96.5 and FPR of 3.0. The accuracy of the Bayesian optimization is the most precise (96.1% with least training time (60 seconds)) and the least training time is also the lowest, the most accurate search of Grida Search (95.2% with maximum cost of computation (120 seconds)) is the least accurate but with the largest cost.

Table 4: Numerical Performance Comparison of Optimization Techniques (Example on NSL-KDD Dataset)

Optimization Method	Accuracy (%)	F1-Score	Training Time (sec)	False Positive Rate (%)
Grid Search	95.2	0.94	120	3.8
Random Search	94.8	0.93	75	4.1
Bayesian Opt.	96.1	0.95	60	3.2
GA-Based Tuning	96.5	0.96	85	3.0
PSO-Based Tuning	96.8	0.96	70	2.9

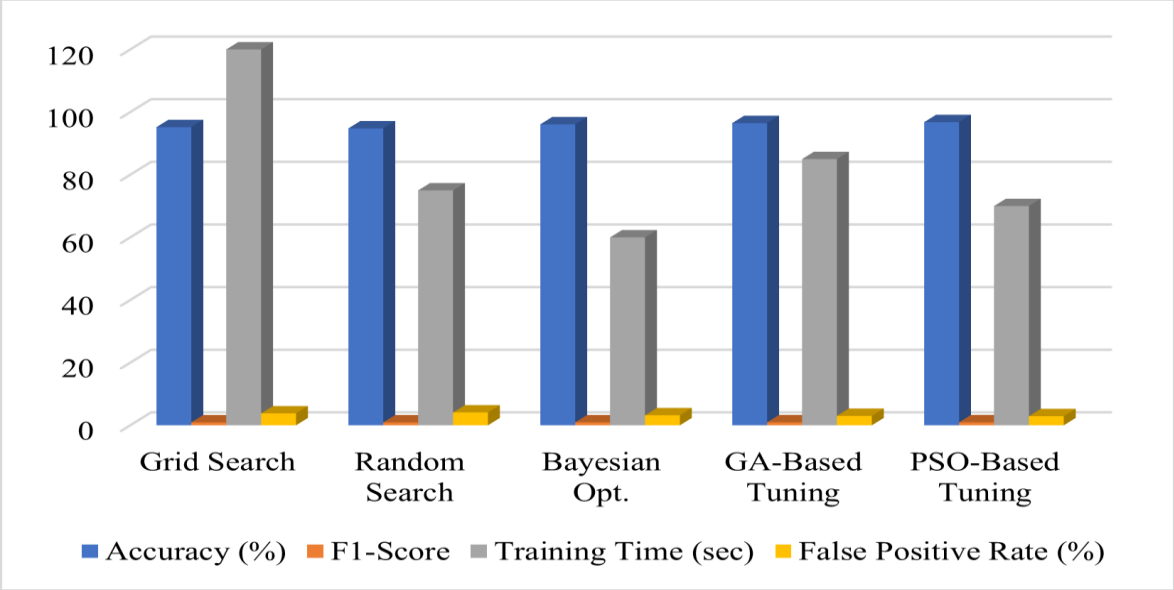


Figure 2: Performance Comparison of Optimization Techniques for SVM-Based IDS

Figure 2 shows the relative performance of various optimization strategies within the intrusion detection systems of the SVM-based systems. GA-based and PSO-based tuning are evolutionary methods that are more accurate, and have lower false positive rates than grid and random search. Bayesian optimization is seen to have a moderate performance with shorter training time and the effectiveness of intelligent parameter tuning showed by high efficiency and robustness of the IDS performance.

X. RESEARCH GAPS AND OPEN CHALLENGES

Although the SVM-based Intrusion Detection Systems (IDS) have made tremendous progress, there are still a number of research gaps and unresolved challenges, which restrict the large-scale deployment and real-life adaptability. These problems need to be addressed to enhance the resilience, scalability, and efficiency of operations in the current cybersecurity context. In Table 6, the main research gaps in SVM-based intrusion detection systems are provided, such as scaling, real-time deployment, high-dimensional and imbalanced data processing, encrypted traffic processing, interpretability, and integration with the emerging AI methods to enhance adaptability.

Table 6: Research Gaps and Open Challenges in SVM-Based IDS

Research Gap	Problem Description	Impact on IDS	Possible Research Direction
Scalability & Real-Time Deployment	High computational cost of SVM training and large traffic volumes	Delayed detection and reduced real-time performance	Parallel processing, distributed SVM, lightweight optimization methods
High-Dimensional & Imbalanced Data	Large feature space and minority attack classes	Bias toward normal traffic; reduced rare attack detection	Feature selection, dimensionality reduction, resampling (SMOTE), cost-sensitive learning
Encrypted Traffic Detection	Limited visibility of packet payloads due to encryption	Reduced effectiveness of content-based detection	Flow-based analysis, statistical feature modeling, metadata-driven detection
Explainability & Interpretability	Complex decision boundaries in nonlinear SVM models	Reduced transparency and trust in IDS decisions	Explainable AI (XAI) methods, feature importance analysis
Integration with Emerging AI	Limited adaptability to dynamic threat landscapes	Lower resilience against evolving attacks	Hybrid SVM–Deep Learning, Federated Learning, Reinforcement Learning

XI. FUTURE RESEARCH DIRECTIONS

Future studies on intrusion detection systems using SVMs should be directed towards the hybrid SVM-deep learning networks to improve the representation of features and detection rates. Real time flexibility to changing threats can be facilitated by online and incremental learning procedures. The frameworks of federated IDS can enhance privacy-sensitive collaborative detection, whereas adaptive AI-driven security frameworks have the potential to boost the resilience to evolving and advanced cyberattacks in contemporary network settings. Table 7 reflects the current research directions such as hybrid SVM deep learning systems, online and incremental learning systems, federated intrusion detection systems, and adaptive AI-based security framework. Such guidelines are expected to maximize scalability, privacy, dynamism in real-time, and intelligent response to threats in contemporary cybersecurity contexts.

Table 7: Future Research Directions in SVM-Based Intrusion Detection Systems

Research Direction	Concept	Expected Benefit	Key Challenges
Hybrid SVM–Deep Learning Architectures	Combine deep learning for feature extraction with SVM for classification	Improved detection accuracy and better nonlinear modeling	Increased computational complexity and training cost
Online & Incremental Learning SVM	Continuously update SVM model with streaming network data	Real-time adaptability to evolving threats	Model stability and drift handling
Federated Intrusion Detection Systems	Distributed IDS training without centralized data sharing	Enhanced privacy and collaborative threat intelligence	Communication overhead and model synchronization
Adaptive & Intelligent Security Frameworks	Integrate SVM with AI-driven decision systems for dynamic response	Self-learning and proactive threat mitigation	Complexity in system integration and scalability

XII. CONCLUSION

This survey has presented comprehensive research on Support Vector Machine (SVM)-based Intrusion Detection Systems (as much as kernel functions and optimization approaches are involved). A large variety of algorithms of the kernel, hyperparameter optimization, benchmark datasets, and performance measurement metrics that had an influence on the efficiency of IDS were discussed in the paper. Analysis on comparison showed that an appropriate selection of

kernel and smart optimization are quite effective in improving detection and reduction of false alarm. Besides, the emerging directions in research such as hybrid SVM-deep learning systems, federated learning, and adaptive security frameworks state about the potential breakthroughs in scalable and real-time intrusion detection. Despite the considerable gains, scalability, imbalance of data, analysis of encrypted traffic, and interpretability remain some of the issues in research. Such issues will play a crucial role in the development of strong, efficient and smart SVM-based IDS systems that would be capable of dealing with the evolving cybersecurity issues in the modern network environments.

REFERENCES

[1] S. Allah Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered intrusion detection system," *Internet of Things*, vol. 24, p. 100936, 2023. doi: 10.1016/j.iot.2023.100936.

[2] O. M. A. Alsyaibani, E. Utami, and A. D. Hartanto, "Survey on deep learning based intrusion detection system," *Telematika*, vol. 14, no. 2, pp. 86–100, Aug. 2021. doi: 10.35671/telematika.v14i2.1317.

[3] A. Meliboev, J. Alikhanov, and W. Kim, "Performance evaluation of deep learning-based network intrusion detection system across multiple balanced and imbalanced datasets," *Electronics*, vol. 11, no. 4, p. 515, 2022. doi: 10.3390/electronics11040515.

[4] J. A. Shaikh et al., "A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks," *Frontiers in Medicine*, vol. 12, p. 1524286, 2025. doi: 10.3389/fmed.2025.1524286.

[5] Y. Wu, B. Zou, and Y. Cao, "Current status and challenges and future trends of deep learning-based intrusion detection models," *Journal of Imaging*, vol. 10, no. 10, p. 254, 2024. doi: 10.3390/jimaging10100254.

[6] C. E. L. Asry, I. Benchaji, S. Douzi, and B. E. L. Ouahidi, "A robust intrusion detection system based on a shallow learning model and feature extraction techniques," *PLoS ONE*, vol. 19, no. 1, p. e0295801, 2024. doi: 10.1371/journal.pone.0295801.

[7] A. Hashmi, O. M. Barukab, and A. H. Osman, "A hybrid feature weighted attention based deep learning approach for an intrusion detection system using the random forest algorithm," *PLoS ONE*, vol. 19, no. 5, p. e0302294, 2024. doi: 10.1371/journal.pone.0302294.

[8] A. A. Yılmaz, "A novel deep learning-based framework with particle swarm optimisation for intrusion detection in computer networks," *PLoS ONE*, vol. 20, no. 2, p. e0316253, 2025. doi: 10.1371/journal.pone.0316253.

[9] K. Bella et al., "An efficient intrusion detection system for IoT security using CNN decision forest," *PeerJ Computer Science*, vol. 10, p. e2290, 2024. doi: 10.7717/peerj-cs.2290.

[10] A. R. Khan et al., "Deep learning for intrusion detection and security of Internet of Things (IoT): Current analysis, challenges, and possible solutions," *Security and Communication Networks*, vol. 2022, Article ID 4016073, 2022. doi: 10.1155/2022/4016073.

[11] A. Deshmukh and K. Ravulakollu, "An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity," *Technologies*, vol. 12, no. 10, p. 203, 2024. doi: 10.3390/technologies12100203.

[12] S. T. Ikram and A. K. Cherukuri, "Improving accuracy of intrusion detection model using PCA and optimized SVM," *Journal of Computing and Information Technology (CIT)*, vol. 24, no. 2, pp. 133–148, 2016. doi: 10.20532/cit.2016.1002701.

[13] D. Wang and G. Xu, "Research on the detection of network intrusion prevention with SVM based optimization algorithm," *Informatica*, vol. 44, no. 2, pp. 269–273, 2020. doi: 10.31449/inf.v44i2.3195.

[14] O. A. Ojoje, G. I. O. Aimufua, S. I. Bassey, and U. Musa, "Performance evaluation and benchmarking of machine learning algorithms for network intrusion detection: An ensemble approach," *SSR Journal of Engineering and Technology*, vol. 2, no. 5, 2025. doi: 10.5281/zenodo.17399805.

[15] R. A. R. Mahmood, A. H. Abdi, and M. Hussin, "Performance evaluation of intrusion detection system using selected features and machine learning classifiers," *Baghdad Science Journal*, vol. 18, no. 2 (Suppl.), pp. 884–??, 2021. doi: 10.21123/bsj.2021.18.2(Suppl.).0884.

[16] R. AlGhamdi, "Design of network intrusion detection system using lion optimization-based feature selection with deep learning model," *Mathematics*, vol. 11, no. 22, p. 4607, 2023. doi: 10.3390/math11224607.