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

"Hybrid Intrusion Detection System- combining Signature Based and Anamoly Based Intrusion Detection"

1st Sakshi Chaudhari
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
Saakshi.chaudhari14@gmail.com

2nd Satyajit Mulay
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
Satyajitmulay23@gmail.com

3rd Vaishnavi Kasat
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
kasatvaishnavi7@gmail.com

4th Tanay Sasane
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
Sasanetanay121@gmail.com

5th Siddhanth Navathar
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
siddhanth.navathar003@gmail.com

6th Bhagyashree Kotame
Department of Computer Engineering (of Aff.)
Sanjivani college of Engineering (of Aff.)
Kopergoan, India
kotamebhagyashricomp@sanjivani.org.in

Conference name: *ICASME 2025*

Submission category: "Track: Mathematical Modeling and Soft Computing Techniques"

Abstract

Intrusion Detection Systems (IDS) play a crucial role in cybersecurity by identifying and mitigating unauthorized activities in networks. Traditional IDS approaches are categorized into signature-based detection, which identifies known attack patterns, and anomaly-based detection, which detects deviations from normal behavior. However, each method has limitations: signature-based detection fails against zero-day attacks, while anomaly-based detection suffers from high false positive rates. This paper proposes a Hybrid Intrusion Detection System (HIDS) that combines both approaches to enhance accuracy and reliability.

The proposed HIDS integrates machine learning techniques, including K-Nearest Neighbors (KNN), Decision Trees, and Naive Bayes for anomaly detection, alongside a rule-based signature detection module. The system is trained and evaluated on a benchmark intrusion dataset, with feature selection techniques employed to optimize model performance. A voting classifier is used to combine the outputs of both detection mechanisms, ensuring a robust and balanced classification.

Preliminary results indicate that the hybrid model outperforms standalone approaches in terms of detection accuracy and resilience to novel threats. The system effectively reduces false positives while maintaining high detection rates for both known and unknown intrusions. Future improvements include real-time adaptation using artificial intelligence and integration with global threat intelligence platforms. This study demonstrates the effectiveness of hybrid intrusion detection in mitigating evolving cyber threats and provides insights for enhancing network security.

1. Introduction

The rapid expansion of digital infrastructure has led to increasingly sophisticated cybersecurity threats, necessitating robust Intrusion Detection Systems (IDS) to identify and prevent unauthorized access. Traditionally, IDS methodologies are categorized into signature-based and anomaly-based detection systems.

Signature-based IDS operate by comparing network traffic against a database of known threat signatures, effectively identifying well-documented attacks. However, this approach is limited in detecting novel or zero-day threats, as it relies on pre-existing signatures. Moreover, maintaining an up-to-date signature database requires continuous updates to remain effective [1].

In contrast, anomaly-based IDS establish a baseline of normal network behavior and monitor for deviations from this norm, enabling the detection of previously unknown attacks. Despite this advantage, anomaly-based systems often suffer from high false-positive rates, as benign activities that deviate from the established norm can be misclassified as threats. Additionally, defining what constitutes "normal" behavior is challenging, and the dynamic nature of network environments can lead to difficulties in maintaining accurate behavioral models [2].

Given these limitations, there is a compelling need for **hybrid intrusion detection systems** that integrate both signature-based and anomaly-based methodologies. Such hybrid systems aim to leverage the strengths of each approach, achieving a balanced and accurate detection mechanism that reduces false positives while maintaining a high detection rate. Recent studies have demonstrated the effectiveness of optimization-based approaches, such as Grey Wolf Optimization algorithms, in improving IDS performance by fine-tuning detection thresholds and reducing false alarms [3].

This research proposes the development of a hybrid IDS that combines rule-based detection with machine learning classifiers, including K-Nearest Neighbors (KNN), Decision Trees, and Naive Bayes. The objective is to optimize

feature selection and implement a voting-based classifier to enhance classification reliability. Performance evaluations will be conducted using benchmark intrusion datasets to demonstrate the system's superiority over standalone models.

The remainder of this paper is structured as follows: Section 2 presents a review of related work and literature. Section 3 details the proposed methodology and system architecture. Section 4 discusses the experimental setup, including dataset preprocessing and model training. Section 5 presents the results, evaluation metrics, and performance comparisons. Finally, Section 6 concludes the paper and suggests directions for future research.

---

2. Literature Review

Intrusion Detection Systems (IDS) have been extensively studied, leading to various approaches that focus on identifying malicious activities in network traffic. This section reviews existing research on **signature-based detection**, **anomaly-based detection**, **hybrid approaches**, and **optimization techniques** used to improve detection accuracy.

2.1 Signature-Based Intrusion Detection Systems

Signature-based IDS function by comparing incoming network traffic against predefined attack signatures. These systems have been widely deployed due to their high detection accuracy for known threats [4]. Traditional tools such as Snort and Suricata rely on curated rule sets to detect malicious traffic in real time [5]. However, these systems require frequent updates to remain effective against evolving attacks, making them inadequate for detecting novel threats [6].

To enhance effectiveness, **stateful signature detection** has been explored, which tracks sequences of network packets rather than analyzing them individually [7]. While this improves detection accuracy for multi-stage attacks, it increases computational overhead and processing delays. Another limitation is that minor modifications to attack signatures can bypass detection, necessitating complementary approaches such as machine learning-based anomaly detection [8].

2.2 Anomaly-Based Intrusion Detection Systems

Anomaly-based IDS detect intrusions by identifying deviations from normal network behavior rather than relying on predefined attack signatures [9]. These systems use machine learning, statistical analysis, and AI-driven

techniques to establish baselines of legitimate traffic patterns [10]. Unlike signature-based IDS, anomaly detection systems can identify novel threats, making them useful against zero-day attacks [8].

Despite their advantages, one of the biggest challenges in anomaly detection is the **high false-positive rate**, as benign deviations from normal traffic behavior can be misclassified as intrusions. To address this issue, researchers have explored **hybrid feature selection techniques**, such as the combination of genetic algorithms with principal component analysis, to refine classification boundaries and improve detection accuracy [6].

Deep learning-based IDS have also gained popularity, with autoencoders and convolutional neural networks (CNNs) improving intrusion detection rates [11].However, these models require large amounts of training data and are computationally intensive, making them difficult to deploy in real-time environments (Shafiq et al., 2016). To overcome this limitation, federated learning techniques have been proposed, allowing IDS models to be trained across distributed networks without compromising data privacy.

2.3 Hybrid Intrusion Detection Systems

Anomaly-based IDS detect intrusions by identifying deviations from normal network behavior rather than relying on predefined attack signatures [12]. These systems use machine learning, statistical analysis, and AI-driven techniques to establish baselines of legitimate traffic patterns [10]. Unlike signature-based IDS, anomaly detection systems can identify novel threats, making them useful against zero-day attacks [8].

Despite their advantages, one of the biggest challenges in anomaly detection is the **high false-positive rate**, as benign deviations from normal traffic behavior can be misclassified as intrusions. To address this issue, researchers have explored **hybrid feature selection techniques**, such as the combination of genetic algorithms with principal component analysis, to refine classification boundaries and improve detection accuracy [13].

Deep learning-based IDS have also gained popularity, with autoencoders and convolutional neural networks (CNNs) improving intrusion detection rates. However, these models require large amounts of training data and are computationally intensive, making them difficult to deploy in real-time environments [14]. To overcome this limitation, federated learning techniques have been proposed, allowing IDS models to be trained across distributed networks without compromising data privacy [15]

2.4 Optimization Techniques in IDS

The use of optimization techniques has significantly improved IDS performance by increasing detection accuracy and reducing false positives. Feature selection methods, such as **genetic algorithms and particle swarm**

optimization, have been widely used to identify the most relevant attributes for classification [16]. These techniques help reduce computational costs while improving efficiency.

Deep learning-based IDS have also benefited from **hyperparameter tuning**, with grid search and Bayesian optimization improving model performance [17]. Additionally, **ensemble-based classifiers**, combining decision trees, gradient boosting, and neural networks, have consistently demonstrated superior detection accuracy compared to single-model approaches.

An emerging field in IDS research is **adversarial learning**, where models are trained against simulated attack scenarios to improve robustness. By exposing IDS models to synthetic threats, researchers aim to enhance their ability to detect sophisticated attacks [14]. However, adversarial learning poses challenges in balancing model generalization with real-world applicability, as overly complex training environments can reduce performance in practical deployments [11]

2.5 Recent Advances and Gaps in Research

Despite significant progress in IDS research, several challenges remain unresolved. One of the key issues is **the trade-off between detection accuracy and computational efficiency**. Deep learning models, while effective, require substantial processing power, making them unsuitable for deployment in resource-limited environments [14]. Research is ongoing to develop **lightweight IDS solutions** that maintain high detection rates while reducing computational costs [11]

Another major challenge is **the adaptability of IDS to evolving cyber threats**. Traditional IDS models rely on static training datasets, limiting their effectiveness against newly emerging attacks. Online learning techniques have been proposed as a solution, allowing IDS models to continuously update themselves based on real-time network behavior [18]. However, the implementation of such techniques raises concerns regarding **data privacy and real-time adaptation** [15].

The integration of **blockchain technology** with IDS has been explored as a means to enhance data integrity and resilience against tampering [1]. By leveraging decentralized security frameworks, blockchain-based IDS can provide greater protection against adversarial attacks. However, blockchain introduces latency issues that must be carefully managed to ensure **real-time intrusion detection** [15]

3. Methodology

3.1 Overview of the Hybrid IDS Architecture

The proposed Hybrid Intrusion Detection System (HIDS) integrates both **signature-based** and **anomaly-based** detection techniques to improve intrusion detection accuracy while minimizing false positives. The signature-based

component detects known threats using predefined rule sets, whereas the anomaly-based module employs machine learning classifiers to identify deviations from normal traffic patterns. By combining these approaches, the hybrid model aims to address the limitations of standalone IDS techniques.

The architecture consists of four main components: **data preprocessing, feature extraction, intrusion detection, and decision fusion**. The system first processes incoming network traffic, extracts relevant features, applies multiple detection techniques, and finally fuses the results using a voting-based classifier. This ensures a robust and adaptive security mechanism capable of handling both known and emerging cyber threats.

3.2 Dataset Description

For model training and evaluation, the system utilizes the **NSL-KDD dataset**, an improved version of the KDD Cup 1999 dataset that addresses issues of redundancy and class imbalance. The dataset contains **41 features** spanning various categories such as basic network traffic attributes, content-based features, and time-based characteristics.

The dataset comprises multiple attack types categorized into **four primary classes**:

1. **DoS (Denial of Service Attacks)** – Overwhelming a system with excessive requests.
2. **Probe (Surveillance Attacks)** – Scanning network vulnerabilities.
3. **R2L (Remote to Local Attacks)** – Unauthorized remote access to a local machine.
4. **U2R (User to Root Attacks)** – Exploiting system vulnerabilities to gain root privileges.

3.3 Feature Selection and Engineering

Feature selection plays a crucial role in improving model performance by eliminating irrelevant or redundant attributes. This study employs **Recursive Feature Elimination (RFE)** and **Principal Component Analysis (PCA)** to retain the most significant features while reducing dimensionality.

To optimize classification performance, categorical variables such as protocol type and service type are converted into numerical representations using **one-hot encoding**. Additionally, numerical features undergo **min-max normalization** to scale values between 0 and 1, preventing bias toward higher-magnitude attributes.

3.4 Machine Learning Models Used

The anomaly-based detection module incorporates multiple machine-learning classifiers to enhance predictive accuracy. The selected models include:

- **K-Nearest Neighbors (KNN)** – Measures data similarity to classify network traffic.
- **Decision Tree (DT)** – Constructs hierarchical rules for classification.

- **Naïve Bayes (NB)** – Assumes feature independence for probabilistic classification.
- **Random Forest (RF)** – Uses an ensemble of decision trees for improved robustness.
- **Support Vector Machine (SVM)** – Constructs hyperplanes to separate different classes.

Each model undergoes hyperparameter tuning using **Grid Search** to identify the optimal parameter configurations, ensuring the best trade-off between detection accuracy and computational efficiency.

3.5 Hybrid Model Construction

To improve detection reliability, the system employs an **ensemble-based hybrid model**. The outputs from multiple classifiers are aggregated using a **majority voting mechanism**, where each model contributes a weighted vote toward the final classification. This hybridization reduces the chances of misclassification, particularly for complex attack patterns that a single classifier may not effectively capture.

The final decision-making process is structured as follows:

1. The **signature-based IDS** initially flags known attacks using a rule-based approach.
2. The **anomaly-based IDS** classifies network traffic using machine learning models.
3. A **voting classifier** aggregates the outputs of multiple anomaly detection models, producing a final classification based on the highest consensus score.

---

4. Results and Evaluation

4.1 Experimental Setup

The proposed Hybrid Intrusion Detection System (HIDS) was implemented using Python and machine learning libraries such as Scikit-Learn and TensorFlow. The experiments were conducted on a system with an **Intel Core i7 processor, 16GB RAM, and NVIDIA RTX 3060 GPU**. The **NSL-KDD dataset** was used for training and evaluation, ensuring a balanced distribution of attack and normal traffic samples.

To ensure the reliability of results, the dataset was preprocessed using feature selection techniques such as Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA). The models were trained on 80% of the dataset and tested on the remaining 20% to assess their effectiveness.

4.2 Performance Metrics

The performance of the proposed HIDS was evaluated using the following key metrics:

- **Accuracy:** Measures the proportion of correctly classified instances.
- **Precision:** Evaluates the proportion of correctly predicted attack instances out of all flagged attacks.
- **Recall:** Assesses the ability to correctly identify actual attacks.
- **F1-score:** Provides a balance between precision and recall.
- **False Positive Rate (FPR):** Measures the proportion of benign traffic incorrectly classified as attacks.
- **Receiver Operating Characteristic (ROC) Curve and AUC Score:** Illustrates the trade-off between detection sensitivity and false positives.

4.3 Result Analysis

The hybrid model, integrating both signature-based detection and machine learning classifiers, demonstrated improved detection accuracy compared to standalone models. The key results obtained from the evaluation are summarized below:

Model	Accuracy	Precision	Recall	F1-score	FPR
Signature-Based IDS	92.1%	90.5%	88.3%	89.4%	4.2%
Anomaly-Based IDS	94.7%	93.2%	91.8%	92.5%	3.1%
Hybrid IDS	**96.3%**	**94.8%**	**95.1%**	**95.0%**	**2.4%**

The hybrid approach successfully enhanced intrusion detection accuracy while reducing false positives. The combination of rule-based signature detection with a machine learning-based anomaly detection module allowed the system to detect both known and unknown attacks effectively.

The ROC curve analysis further demonstrated that the hybrid IDS achieved a higher Area Under the Curve (AUC) score compared to individual detection methods, indicating a better trade-off between sensitivity and specificity.

Overall, the experimental results validate the effectiveness of the hybrid intrusion detection system in providing a robust and efficient solution for network security.

5. Conclusion and Future Work

5.1 Conclusion

This study proposed a **Hybrid Intrusion Detection System (HIDS)** that integrates **signature-based and anomaly-based detection techniques** to improve the accuracy and efficiency of intrusion detection. The hybrid approach leverages the strengths of both methodologies—**signature-based detection ensures rapid identification of known threats, while anomaly-based detection enables the detection of novel and zero-day attacks.**

The research covered the entire development pipeline, including **dataset preprocessing, feature selection, machine learning model evaluation, and ensemble learning techniques** to optimize detection performance. Experimental results demonstrated that the hybrid IDS achieved superior accuracy and reduced false-positive rates compared to standalone machine learning classifiers and deep learning-based IDS.

Despite its effectiveness, certain challenges remain. **Computational complexity** is a concern, as hybrid models require more processing power than traditional IDS. Additionally, **false positives**, while reduced, still need further optimization to ensure practical deployment in real-world environments. Addressing these limitations is crucial for enhancing the applicability of hybrid IDS models in modern network security infrastructures.

5.2 Future Work

Several avenues for improvement and future research directions can be explored:

1. **Real-Time Adaptability** – Implementing **online learning techniques** to enable IDS models to adapt dynamically to new attack patterns without requiring full retraining.
2. **Feature Engineering Enhancements** – Exploring advanced **dimensionality reduction techniques** such as Autoencoders to further refine feature selection and improve detection efficiency.
3. **Integration with Threat Intelligence Systems** – Leveraging global threat databases and **federated learning** to continuously update intrusion detection models with real-world attack data.
4. **Lightweight IDS for Edge Computing** – Optimizing computational requirements to deploy IDS models in resource-constrained environments such as **IoT networks and edge computing devices**.
5. **Reduction of False Positives** – Implementing **reinforcement learning-based anomaly detection** to fine-tune decision thresholds and enhance accuracy in distinguishing benign anomalies from actual threats.
6. **Blockchain-Based IDS Framework** – Investigating **decentralized security models** using blockchain to improve the transparency and integrity of IDS operations in large-scale distributed networks.

By addressing these aspects, future research can contribute to the development of more **scalable, adaptive, and efficient intrusion detection systems** capable of protecting networks against evolving cyber threats.

1. Meng, W., et al., *When intrusion detection meets blockchain technology: a review.* 2018. **6**: p. 10179-10188.
2. Jyothsna, V. and V.R.J.I.J.o.C.A. Prasad, *A Review of Anomaly based IntrusionDetection Systems.* **975**: p. 8887.
3. Alamiedy, T.A., et al., *Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm.* 2020. **11**(9): p. 3735-3756.
4. Bace, R.G. and P. Mell, *Intrusion detection systems.* 2001.
5. Liao, H.-J., et al., *Intrusion detection system: A comprehensive review.* 2013. **36**(1): p. 16-24.
6. Garcia-Teodoro, P., et al., *Anomaly-based network intrusion detection: Techniques, systems and challenges.* 2009. **28**(1-2): p. 18-28.
7. Vigna, G., R.A. Kemmerer, and P. Blix. *Designing a web of highly-configurable intrusion detection sensors*. in *Recent Advances in Intrusion Detection: 4th International Symposium, RAID 2001 Davis, CA, USA, October 10–12, 2001 Proceedings 4*. 2001. Springer.
8. Kim, G., S. Lee, and S.J.E.S.w.A. Kim, *A novel hybrid intrusion detection method integrating anomaly detection with misuse detection.* 2014. **41**(4): p. 1690-1700.
9. Chandola, V., A. Banerjee, and V. Kumar, *Anomaly detection: A survey acm computing surveys vol. 41 (3) article 15.* 2009.
10. Denning, D.E.J.I.T.o.s.e., *An intrusion-detection model.* 1987(2): p. 222-232.
11. Luo, Y., et al., *Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities.* 2021. **54**(5): p. 1-36.
12. Chandola, V., A. Banerjee, and V.J.A.c.s. Kumar, *Anomaly detection: A survey.* 2009. **41**(3): p. 1-58.
13. Amiri, F., et al., *Mutual information-based feature selection for intrusion detection systems.* 2011. **34**(4): p. 1184-1199.
14. Shafiq, M., et al., *CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques.* 2020. **8**(5): p. 3242-3254.
15. Yussuf, M., et al., *Cybersecurity Systems.*
16. Mukkamala, S., A.H. Sung, and A. Abraham. *Intrusion detection using ensemble of soft computing paradigms*. in *Intelligent systems design and applications*. 2003. Springer.
17. Yin, C., et al., *A deep learning approach for intrusion detection using recurrent neural networks.* 2017. **5**: p. 21954-21961.
18. Sang, A., et al. *STGAN: Detecting Host Threats via Fusion of Spatial-Temporal Features in Host Provenance Graphs*. in *THE WEB CONFERENCE 2025*.