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

# A STUDY OF REAL TIME INTRUSION DETECTION FRAMEWORK FOR NETWORK SECURITY USING MACHINE LEARNING TECHNIQUES

**[1]Asha Sisodiya , [2]Dr. Ganpat joshi**
1. Research Scholar, Department of Computer Science & Application, Madhav University, Abu Road, Sirohi, Rajasthan
2. Professor, Department of Computer Science & Application, Madhav University, Abu Road, Sirohi, Rajasthan

***Abstract :*** In today's world, where digital threats to network security are constantly changing, the need for advanced intrusion detection systems is more important than ever. Traditional systems often face challenges like high rates of false positives and sluggish response times, which can lead to inefficiencies that jeopardize sensitive information and the integrity of the entire network. Tackling these problems is crucial, especially in fields like healthcare, where safeguarding patient data is vital. Fortunately, recent breakthroughs in machine learning have brought forth some exciting solutions, enhancing detection capabilities by utilizing algorithms like Support Vector Machines and K-Nearest Neighbors. By weaving these techniques into a software-defined networking framework, the proposed model seeks to streamline real-time threat detection and response, ultimately boosting overall system performance.

***IndexTerms*** **- Network security, Machine learning and Intrusion detection.**

## 1. Introduction

In an era where digital threats to network security continue to evolve, the demand for sophisticated intrusion detection systems has never been more critical. Traditional systems often struggle with high false positive rates and slow response times, leading to inefficiencies that can compromise sensitive information and overall network integrity. Addressing these issues is paramount, particularly in sectors like healthcare, where protecting patient data is essential. Recent advancements in machine learning have introduced promising solutions, offering enhanced detection capabilities by leveraging algorithms such as Support Vector Machines and K-Nearest Neighbors. By integrating these techniques into a software-defined networking framework, the proposed model aims to optimize real-time threat identification and response mechanisms, thereby improving overall system performance. Moreover, the incorporation of explainable artificial intelligence principles fosters a deeper understanding of threat dynamics, facilitating better decision-making in security operations [(12)].

### *1.1. Overview of Network Security and the Importance of Intrusion Detection Systems*

As the digital landscape continually evolves, the stakes for network security rise correspondingly, necessitating robust defenses against an array of cyber threats. Intrusion Detection Systems play a pivotal role in this defensive strategy by enabling organizations to monitor network traffic for suspicious activities that could indicate a breach. These systems serve as a critical line of defense, employing various techniques to detect anomalies and potential threats within real-time data streams. Machine learning techniques have emerged as particularly effective for enhancing the capabilities of IDS, leveraging algorithms that can adaptively identify novel attack patterns [(6)]. Furthermore, the integration of a comprehensive approach to network security, as highlighted in programs like those at the Milwaukee School of Engineering, underscores the need for a holistic understanding of security principles that encompass network infrastructure, secure software development, and legal implications of cybersecurity practices [(5)].

## 2. Machine Learning Techniques in Intrusion Detection

The increasing sophistication of cyber threats necessitates the development of advanced methodologies for real-time threat detection. In this context, machine learning techniques have emerged as pivotal tools for enhancing intrusion detection systems. By leveraging algorithms like Support Vector Machines (SVM) and k-Nearest Neighbors (KNN), researchers can improve the accuracy and responsiveness of IDS in identifying malicious activities across networks. For instance, the proposed framework in [13] demonstrates a hybrid SVM-KNN model that significantly enhances detection rates while reducing false positives. Moreover, the integration of machine learning with network forensics allows for more effective threat identification by analyzing large datasets and balancing uneven traffic, as outlined in [14]. Ultimately, these advancements not only facilitate improved network security but also ensure efficient resource utilization, making machine learning an invaluable asset in contemporary cybersecurity strategies.

### *2.1 Types of Machine Learning Algorithms Used in Network Security*

The increasing sophistication of cyber threats necessitates robust solutions within network security frameworks. Among these, machine learning algorithms are pivotal in enhancing the efficacy of Intrusion Detection Systems (IDS). Techniques such as Bayesian networks enable adaptive learning and efficient classification of diverse network traffic, making them ideal for identifying a spectrum of attacks, including denial of service and user-specific threats [1]. Additionally, other machine learning methodologies, such as support vector machines and neural networks, contribute to accurate threat detection by learning from historical data and adapting to new patterns. With the ever-evolving nature of cybercrime, incorporating artificial intelligence lends the advantage of not only defending systems but also preemptively identifying potential vulnerabilities [2]. Thus, the synergy between machine learning algorithms and IDS plays a critical role in advancing network security.

## 3. Real-Time Intrusion Detection Frameworks

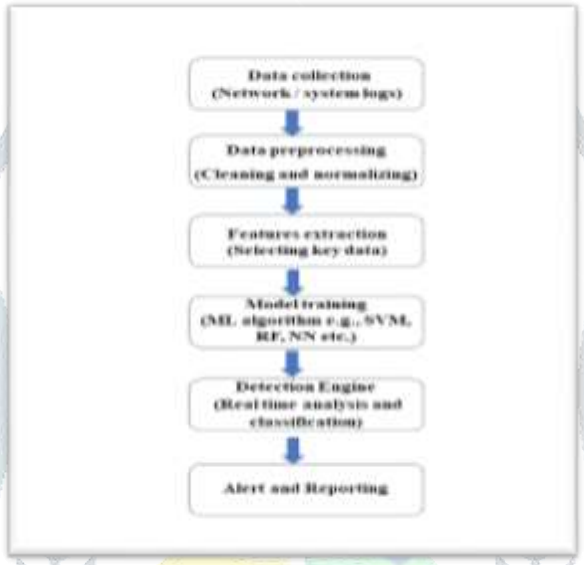
The increasing complexity of network environments necessitates sophisticated measures for safeguarding information integrity. Real-time intrusion detection frameworks leverage advanced machine learning techniques to enhance detection accuracy and response times. By employing models such as Random Forest and support vector machines, these frameworks can effectively process vast amounts of data to identify anomalous patterns indicative of security threats. In particular, the integration of a preprocessing pipeline—featuring data cleaning and feature selection—has proven essential for optimizing the performance of IDS. Studies reveal that a well-implemented framework can achieve impressive metrics, including accuracy rates exceeding 99% when utilizing comprehensive datasets like CIS-CICIDS2017 [15]. Furthermore, adapting these frameworks to unique challenges posed by Internet of Things (IoT) environments highlights the need for ongoing research and refinement in feature selection and algorithm efficiency to address emerging security concerns [16].

| Algorithm | Detection Accuracy | False Positive Rate | Training Time | Suitability for Real-Time IDS |
|---|---|---|---|---|
| Support Vector Machine (SVM) | High (~98%) | Moderate | Medium | Good |
| K-Nearest Neighbors (KNN) | Moderate (~93%) | High | Low | Fair |
| Random Forest | Very High (~99%) | Low | High | Excellent |
| Bayesian Network | Moderate (~90%) | Moderate | Low | Fair |
| Neural Networks | High (~97%) | Low | High | Good |

***Table no 1 showing the comparison of machine learning algorithms in IDS***

### *3.1 Key Components and Architecture of Effective Frameworks*

An effective framework for real-time intrusion detection encompasses several critical components that work synergistically to enhance network security. Central to this architecture is the integration of machine learning techniques, which allow for dynamic threat detection and response capabilities. By leveraging unsupervised learning for anomaly detection, systems can identify unusual patterns that may indicate an intrusion, thereby mitigating risks to data integrity and confidentiality. Furthermore, positioning cIDS within a cloud architecture is essential, as outlined in previous studies, to address vulnerabilities in existing technologies. The adaptability of frameworks can be further enhanced by employing AI-driven strategies that dynamically adjust security measures in response to emerging threats in distributed environments, as articulated in discussions about microservices. Ultimately, such an architecture not only strengthens defenses against potential attacks but also ensures overall system resilience and availability, reflecting the complex demands of contemporary network security [(3)(4)].




**Machine learning based intrusion detection system architecture**

## 4. CONCLUSION

The exploration of innovative strategies for real-time intrusion detection highlights the necessity of adapting to the evolving landscape of cyber threats. The integration of machine learning techniques has emerged as a pivotal factor that enhances the efficacy of these systems, demonstrating improved accuracy and reduced false positive rates. As illustrated through various assessments, reliance on signature-based detection alone is insufficient in counteracting the sophisticated tactics employed by modern attackers. By employing anomaly-based and heuristic detection methods, researchers reveal significant advancements in safeguarding digital infrastructures. Moreover, incorporating feature selection techniques not only augments detection capabilities but also optimizes computational resource allocation. The study underscores the critical importance of fostering adaptive security frameworks that not only respond dynamically to threats but also evolve alongside them, ultimately reinforcing the overarching goal of bolstering network security in an increasingly interconnected world [(9)(10)].

### *4.1 Future Directions and Challenges in Machine Learning for Intrusion Detection*

As the landscape of network security evolves, addressing the complexities of IDS becomes increasingly critical. Future research must confront the dual challenges of developing advanced machine learning (ML) algorithms while ensuring operational efficiency in heterogeneous environments, such as the Internet of Things (IoT). Strategies to enhance IDS efficacy include exploring ensemble methods and real-time adaptive learning algorithms, which can respond dynamically to emerging threats. Additionally, the integration of Explainable AI (XAI) techniques is paramount, enabling analysts to interpret model decisions and trust in their outputs, especially amidst intricate cyber threats like zero-day attacks. Moreover, establishing benchmark datasets and standardized evaluation frameworks is vital for assessing ML-based IDS effectively. By employing rich feature selection and anomaly detection

approaches, the field can advance significantly, improving security and integrity across various applications, as highlighted in and [8].

**References**


1. Abouzakhar, Nasser, Alocious, Chaminda, Christianson, B., Xiao, et al.. "Intrusion Detection System using Bayesian Network Modeling" ACPI (Academic Conference Publishing International), 2014, doi: https://core.ac.uk/download/29843350.pdf
2. Diep, Quoc Bao, Truong, Thanh Cong, Zelinka, Ivan. "Artificial intelligence in the cyber domain: Offense and defense" 'MDPI AG', 2020, doi: https://core.ac.uk/download/323112801.pdf
3. Arshad, Avi Patel, Beg, Bhavesh Borisaniya, Botha, Chen, Chen, et al.. "A survey of intrusion detection techniques in Cloud" 'Elsevier BV', 2013, doi: https://core.ac.uk/download/9559501.pdf
4. Ramamoorthi, Vijay. "Anomaly Detection and Automated Mitigation for Microservices Security with AI" ResearchBerg, 2024, doi: https://core.ac.uk/download/620852569.pdf
5. W. Schilling, E. Durant. "Teaching Software Security: A Multi-disciplinary Approach" 2012, doi: https://www.semanticscholar.org/paper/7a16c4e0593bc67fa1d4b6bdab8aa8b5be313f5b
6. A. Prodromidis, S. Stolfo. "Agent-Based Distributed Learning Applied to Fraud Detection" 1999, doi: https://www.semanticscholar.org/paper/df619024edc7c1cd297e7cc3a88858336332a758
7. Mohammed Naif Alatawi. "Enhancing Intrusion Detection Systems With Advanced Machine Learning Techniques: An Ensemble and Explainable Artificial Intelligence (AI) Approach" SECURITY AND PRIVACY, 2025, doi: https://www.semanticscholar.org/paper/103da0507237f769c60135db2d5d960d4b049c0b
8. Mazin S. Mohammed, H. A. Talib. "Using Machine Learning Algorithms in Intrusion Detection Systems: A Review" Tikrit Journal of Pure Science, 2024, doi: https://www.semanticscholar.org/paper/bac70ad4c0213ea69670c8265d308f9833c4bc71
9. Yaseen, Asad. "UNCOVERING EVIDENCE OF ATTACKER BEHAVIOR ON THE NETWORK" ResearchBerg, 2020, doi: https://core.ac.uk/download/603939725.pdf
10. Elfayq, Khalid, Idouglid, Lahcen, Tkatek, Said. "Boosting industrial internet of things intrusion detection: leveraging machine learning and feature selection techniques" Institute of Advanced Engineering and Science, 2025, doi: https://core.ac.uk/download/642649195.pdf
11. Muhammad Waseem Asif, Aqsa Aqdus, Rashid Amin, Shehzad Ashraf Chaudhry, Faisal S. Alsubaei, Sajid Iqbal. "An Efficient Intrusion Detection System using Advanced Machine Learning Techniques in Software-Defined Networks (SDN) for Healthcare System." IEEE journal of biomedical and health informatics, 2025, doi: https://www.semanticscholar.org/paper/27bcce30ec3df3ca5912784f66a296e31323dab0
12. Hyunwoo Lee, Taewoong Kwon, Jun Lee, Jung-suk Song. "Enhancing Decision-Making of Network Intrusion Analysis Assisted by Explainable AI for Real-Time Security Monitoring" 2024 IEEE Conference on Dependable and Secure Computing (DSC), 2024, 147-154. doi: https://www.semanticscholar.org/paper/06185c2ceb4e89da09c025d192b42c28e9f0d81c
13. Muhammad Waseem Asif, Aqsa Aqdus, Rashid Amin, Shehzad Ashraf Chaudhry, Faisal S. Alsubaei, Sajid Iqbal. "An Efficient Intrusion Detection System using Advanced Machine Learning Techniques

in Software-Defined Networks (SDN) for Healthcare System." IEEE journal of biomedical and health informatics, 2025, doi: https://www.semanticscholar.org/paper/27bcce30ec3df3ca5912784f66a296e31323dab0

14. Raisa Fabiha, Stein Joachim Reberio, Zubayer Farazi, Fernaz Narin Nur, Shaheena Sultana. "A Machine Learning Framework for Real-Time Intrusion Detection for Malicious Internet Activity" 2024 6th International Conference on Sustainable Technologies for Industry 5.0 (STI), 2024, 1-6. doi: https://www.semanticscholar.org/paper/470c698026511464360d2163c9e0eef8168c82a4
15. MD Shadman Soumik. "A comparative analysis of Network Intrusion Detection (NID) using Artificial Intelligence techniques for increase network security" International Journal of Science and Research Archive, 2024, doi: https://www.semanticscholar.org/paper/c71c3da8572a7c711633155b0f6214daad4c1269
16. Mazin S. Mohammed, H. A. Talib. "Using Machine Learning Algorithms in Intrusion Detection Systems: A Review" Tikrit Journal of Pure Science, 2024, doi: https://www.semanticscholar.org/paper/bac70ad4c0213ea69670c8265d308f9833c4bc71